



Questo manuale d'istruzione è fornito da trovaprezzi.it. Scopri tutte le offerte per [Netgear SXR50](#) o cerca il tuo prodotto tra le [migliori offerte di Altri dispositivi di rete](#)



Questo manuale d'istruzione è fornito da trovaprezzi.it. Scopri tutte le offerte per [Netgear SXR50](#) o cerca il tuo prodotto tra le [migliori offerte di Wireless e Bluetooth](#)

# NETGEAR®

## User Manual

---

## Orbi Pro WiFi 6 AX5400 Tri-band WiFi System (SXX50)

### Models

Orbi Pro WiFi 6 AX5400 Router Model SXR50

Orbi Pro WiFi 6 AX5400 Satellite Model SXS50

April 2022  
202-12551-03

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

## **Support and Community**

Visit [netgear.com/support](https://www.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.

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

## **Trademarks**

© 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   |
|-------------------------|---------------|--|
| 202-12551-03            | April 2022    | We added <a href="#">NETGEAR Insight Business VPN</a> on page 22.  |
| 202-12551-02            | March 2022    | We made minor corrections to <a href="#">Technical specifications for Orbi Pro WiFi 6 AX5400 router model SXR50</a> on page 226 and <a href="#">Technical specifications for Orbi Pro WiFi 6 AX5400 satellite model SXS50</a> on page 228. |
| 202-12551-01            | February 2022 | First publication.   |

# Contents

## Chapter 1 Overview and Setup

- Supported Orbi Pro WiFi 6 AX5400 models.....11
- Orbi Pro WiFi 6 AX5400 router and satellite hardware overviews.11
  - Orbi Pro WiFi 6 AX5400 router model SXR50 hardware.....11
  - Orbi Pro WiFi 6 AX5400 satellite model SXS50 hardware.....12
- LED behavior.....13
  - Orbi Pro WiFi 6 AX5400 System LEDs.....13
  - Add-on Orbi Pro WiFi 6 AX5400 satellite LEDs.....14
- Orbi Pro WiFi 6 AX5400 router and satellite labels.....14
- Connect your Orbi Pro WiFi 6 AX5400 router.....15
- Place your Orbi Pro WiFi 6 AX5400 satellite.....16
- Sync your Orbi Pro WiFi 6 AX5400 satellite.....17
  - Sync a satellite from an Orbi Pro WiFi 6 AX5400 system.....17
  - Sync an add-on Orbi Pro WiFi 6 AX5400 satellite.....18
- Add satellites to your network using the router web interface.19
- Set up your satellite with a wired connection to your router.....20
  - Set up and sync an Orbi Pro satellite over a wired connection.20
  - Ethernet backhaul connections for multiple satellites.....21
- Manage and monitor your Orbi network with NETGEAR Insight..22
- NETGEAR Insight Business VPN.....22

## Chapter 2 Connect to the Orbi Pro WiFi 6 AX5400 Network and Access the Router

- Connect to the network for initial configuration.....25
  - Wired connection.....25
  - WiFi connection.....25
  - WiFi connection using WPS.....26
- Types of logins.....26
- Use a web browser to access the router.....26
  - Use the interactive Internet setup process.....27
  - Log in to the Orbi router web interface.....28
- Change the language.....29
- What to do if you get a browser security warning.....29

## Chapter 3 Specify Your Internet Settings

- Setup Wizard.....32

|   |    |
|---|----|
| Manually set up the Internet connection.....                | 32 |
| Set up an Internet connection without a login.....          | 33 |
| Set up an Internet connection with a login.....             | 34 |
| IPv6 Internet connections.....                              | 36 |
| Requirements for entering IPv6 addresses.....               | 36 |
| Set up IPv6 Internet connections.....                       | 36 |
| Use auto detection for an IPv6 Internet connection.....     | 37 |
| Use auto configuration for an IPv6 Internet connection..... | 39 |
| Set up an IPv6 6to4 tunnel Internet connection.....         | 40 |
| Set up an IPv6 6rd tunnel Internet connection.....          | 42 |
| Set up an IPv6 pass-through Internet connection.....        | 44 |
| Set up an IPv6 fixed Internet connection.....               | 45 |
| Set up an IPv6 DHCP Internet connection.....                | 46 |
| Set up an IPv6 PPPoE Internet connection.....               | 48 |
| MTU size.....   | 50 |

## **Chapter 4 Control Access to the Internet**

|   |    |
|---|----|
| MAC access control lists.....   | 53 |
| Enable a MAC ACL for a specific network.....                                      | 54 |
| Add automatically detected devices to a MAC ACL.....                              | 55 |
| Manually add, remove, or change the information for a device<br>on a MAC ACL..... | 56 |
| Disable a MAC ACL for a specific network.....                                     | 57 |
| Network access control list.....  | 58 |
| Enable the network access control list and specify the access<br>rule.....        | 59 |
| Manage the allowed devices on the network access control<br>list.....             | 61 |
| Manage the blocked devices on the network access control<br>list.....             | 62 |
| Block Internet sites by using keywords.....                                       | 63 |
| Delete keywords that are used to block Internet sites.....                        | 65 |
| Trusted computer.....   | 65 |
| Block services from the Internet.....   | 66 |
| Schedule when to block Internet sites and services.....                           | 68 |
| Email notifications for security events.....                                      | 69 |

## **Chapter 5 Manage the VLANs**

|  |    |
|--|----|
| About VLANs in general.....                          | 72 |
| About VLANs on the router.....                       | 72 |
| How the router organizes LANs, VLANs, and WLANs..... | 73 |
| VLAN profiles.....                                   | 74 |
| Add a new VLAN profile.....                          | 74 |
| Add a new VLAN profile directly to a LAN.....        | 76 |

- Change the client isolation or network isolation for a VLAN profile.....78
- Delete a VLAN profile.....79
- VLAN membership for a LAN, WiFi network, or port.....80
  - Change the VLAN profile for a LAN.....80
  - Enable, change, or disable the VLAN profile for a WiFi network.....81
  - Change the VLAN profile for an Ethernet port.....82
- Port mode: Trunk mode or Access mode.....83

**Chapter 6 Manage the WiFi Networks**

- About the WiFi networks.....86
- admin (default) WiFi network.....87
  - Change the admin WiFi network name, channel, or VLAN.....87
  - Change the admin WiFi password or security level.....89
- Employee WiFi network.....91
  - Enable the employee WiFi network and manage the settings.91
  - Change the employee WiFi password or security level.....93
- Internet of things WiFi network.....96
  - Enable the IoT WiFi network and manage the settings.....96
  - Change the IoT WiFi password or security level.....97
- Guest WiFi network and captive portal.....100
  - Set up a guest WiFi network with open access or password authentication.....101
  - Set up Facebook Wi-Fi for the guest WiFi network.....102
  - Set up a guest WiFi network with a captive portal.....104

**Chapter 7 Manage the LANs**

- About the LANs.....108
- LAN settings.....109
  - Change the default LAN 1 settings.....109
  - Change the employee LAN 2 settings.....111
  - Change the IoT LAN 3 settings.....112
  - Change the guest LAN 4 settings.....113
  - Set custom settings for LAN 5.....114
- DHCP servers.....115
  - Set up a DHCP server for the default LAN 1.....116
  - Set up a DHCP server for the employee LAN 2.....117
  - Set up a DHCP server for the IoT LAN 3.....118
  - Set up a DHCP server for the guest LAN 4.....119
  - Set up a DHCP server for the custom LAN 5.....120
  - Disable the DHCP server for a LAN.....122
- Reserved LAN IP addresses.....122
  - Reserve a LAN IP address.....123

Edit a reserved LAN IP address.....124  
Delete a reserved LAN IP address entry.....124

**Chapter 8 Manage the WAN and other Network Settings**

WAN settings.....127  
Dynamic DNS.....128  
    Set up a new Dynamic DNS account.....129  
    Specify a DNS account that you already created.....130  
    Change the Dynamic DNS settings.....131  
DMZ server.....131  
Static routes.....132  
    Set up a static route.....133  
    Change a static route.....135  
    Delete a static route.....135  
Universal Plug and Play.....136  
Link aggregation.....137  
    Add a link aggregation group.....138  
    Remove a link aggregation group.....139  
    Set up a LAG connection between an Orbi Pro WiFi 6 AX5400  
    satellite and router.....140

**Chapter 9 Manage and Monitor Your Orbi Pro System**

Firmware for the router and satellite.....143  
    Enable the automatic firmware update feature.....143  
    Check for firmware updates.....143  
    Manually update firmware.....144  
    Manually update satellite firmware.....145  
    Manually update router firmware.....146  
admin password.....147  
    Change the admin password.....147  
    Enable admin password reset.....148  
    Reset the admin password.....149  
Monitor the router, satellite, and Orbi network.....150  
    View router status and usage information.....150  
    View the satellite status in the satellite web interface.....150  
    View satellites, WiFi devices, and wired devices connected to the  
    Orbi network.....151  
    Check the Internet connection status or renew the  
    connection.....153  
    Display port and radio statistics.....154  
    View and manage logs of router activity.....155  
Syslog server.....156  
Traffic meter.....157  
    Start the traffic meter without traffic restrictions.....157

- Restrict Internet traffic by volume.....158
- Restrict Internet traffic by connection time.....159
- View the Internet traffic volume and statistics.....161
- Unblock the traffic meter after the traffic limit is reached.....161
- NTP server.....162
- Time zone.....163
- Configuration file.....163
  - Back up settings.....164
  - Manage the automatic backup options.....164
  - Erase the current configuration settings.....165
  - Restore configuration settings.....166
- Remote management.....166
- Remote access.....168
- AP mode.....168
- Router mode.....169
- Sync button security.....170
  - Manage the Sync button on the router.....170
  - Manage the Sync button on the satellite.....171

**Chapter 10 Manage the Advanced WiFi Settings**

- Download bandwidth per SSID.....174
- Region of operation.....175
- SSID broadcast for a radio.....176
- 20/40 MHz coexistence for the 2.4 GHz radio.....177
- Wi-Fi multimedia for a radio.....178
- CTS/RTS threshold and preamble mode for a radio.....179
- Transmission output power for a radio.....180
- Backhaul password.....181
- MU-MIMO.....182
- Protected Management Frames.....183

**Chapter 11 Customize Internet Traffic Rules for Ports**

- Port forwarding to a local server.....186
  - Set up port forwarding to a local server.....186
  - Add a custom port forwarding service.....187
  - Edit a port forwarding service.....188
  - Delete a port forwarding entry.....189
  - Application example: Make a local web server public.....189
  - How the router implements the port forwarding rule.....190
- Port triggering.....191
  - Add a port triggering service.....191
  - Enable port triggering.....192
  - Application example: Port triggering for Internet Relay Chat.193

## Chapter 12 Use OpenVPN to Access Your Network

|   |     |
|---|-----|
| About VPN connections.....                                    | 196 |
| LAN IP addressing in VPN networks.....                        | 196 |
| Enable OpenVPN service in the router.....                     | 197 |
| Install OpenVPN software on a VPN client.....                 | 198 |
| Install OpenVPN software on a Windows-based computer....      | 199 |
| Install OpenVPN software on a Mac computer.....               | 200 |
| Install OpenVPN software on an iOS device.....                | 201 |
| Install OpenVPN software on an Android device.....            | 202 |
| Use VPN to access your Internet service at your business..... | 203 |
| Allow VPN client Internet access in the router.....           | 204 |
| Block VPN client Internet access in the router.....           | 204 |

## Chapter 13 Troubleshooting

|  |     |
|--|-----|
| Quick tips.....  | 207 |
| Sequence to restart your network.....                    | 207 |
| WiFi settings.....                                       | 207 |
| Network settings.....                                    | 207 |
| The router and satellite do not sync.....                | 207 |
| You cannot log in to the router.....                     | 209 |
| You cannot access the Internet.....                      | 209 |
| Troubleshoot Internet browsing.....                      | 210 |
| Troubleshoot PPPoE.....                                  | 211 |
| Troubleshoot WiFi connectivity.....                      | 212 |
| Troubleshoot your network using the ping utility.....    | 212 |
| Test the LAN path to your router.....                    | 213 |
| Test the path from your computer to a remote device..... | 213 |

## Appendix A How to Use VLANs in Your Network

|  |     |
|--|-----|
| VLAN use case 1: Orbi Pro WiFi 6 router in a home environment.         | 216 |
| VLAN use case 2: Orbi Pro WiFi 6 router in a business environment..... | 218 |

## Appendix B Supplemental Information

|   |     |
|---|-----|
| Factory settings.....   | 223 |
| Factory settings for Orbi Pro WiFi 6 AX5400 router model SXR50.....         | 223 |
| Factory settings for Orbi Pro WiFi 6 AX5400 satellite model SXS50.....      | 226 |
| Technical specifications.....   | 226 |
| Technical specifications for Orbi Pro WiFi 6 AX5400 router model SXR50..... | 226 |

Technical specifications for Orbi Pro WiFi 6 AX5400 satellite  
model SXS50.....228

# 1

## Overview and Setup

---

The Orbi Pro WiFi 6 AX5400 Tri-band Mesh System (SXX50) creates dedicated high-speed WiFi connections to your Internet service. The Orbi Pro WiFi 6 AX5400 router (model SXR50) connects to your modem or gateway. You can use the router alone or let it support up to six Orbi Pro WiFi 6 AX5400 satellites (model SXS50), which can extend the WiFi signal throughout your business, office, or home.

This chapter contains the following sections:

- [Supported Orbi Pro WiFi 6 AX5400 models](#)
- [Orbi Pro WiFi 6 AX5400 router and satellite hardware overviews](#)
- [LED behavior](#)
- [Orbi Pro WiFi 6 AX5400 router and satellite labels](#)
- [Connect your Orbi Pro WiFi 6 AX5400 router](#)
- [Place your Orbi Pro WiFi 6 AX5400 satellite](#)
- [Sync your Orbi Pro WiFi 6 AX5400 satellite](#)
- [Set up your satellite with a wired connection to your router](#)
- [Manage and monitor your Orbi network with NETGEAR Insight](#)
- [NETGEAR Insight Business VPN](#)

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

**Note:** This manual refers to the Orbi Pro WiFi 6 AX5400 router as the *router* and refers to the Orbi Pro WiFi 6 AX5400 satellite as the *satellite*.

**Note:** The Orbi Pro WiFi 6 AX5400 router does not pair with satellites from any other Orbi and Orbi Pro systems. The Orbi Pro WiFi 6 AX5400 satellite does not pair with a router from any other Orbi and Orbi Pro system.

# Supported Orbi Pro WiFi 6 AX5400 models

This user manual describes the following Orbi Pro WiFi 6 AX5400 models:

- Orbi Pro WiFi 6 AX5400 Router (Model SXR50)
- Orbi Pro WiFi 6 AX5400 Satellite (Model SXS50)

**Note:** To manage your Orbi Pro WiFi 6 AX5400 router and any Orbi Pro WiFi 6 AX5400 satellites that are connected to your Orbi Pro WiFi 6 network, you must manage them from your Orbi Pro WiFi 6 AX5400 router web interface.

## Orbi Pro WiFi 6 AX5400 router and satellite hardware overviews

The following sections display and describe the hardware features of the Orbi Pro WiFi 6 AX5400 router (model SXR50) and Orbi Pro WiFi 6 AX5400 satellite (model SXS50).

### Orbi Pro WiFi 6 AX5400 router model SXR50 hardware

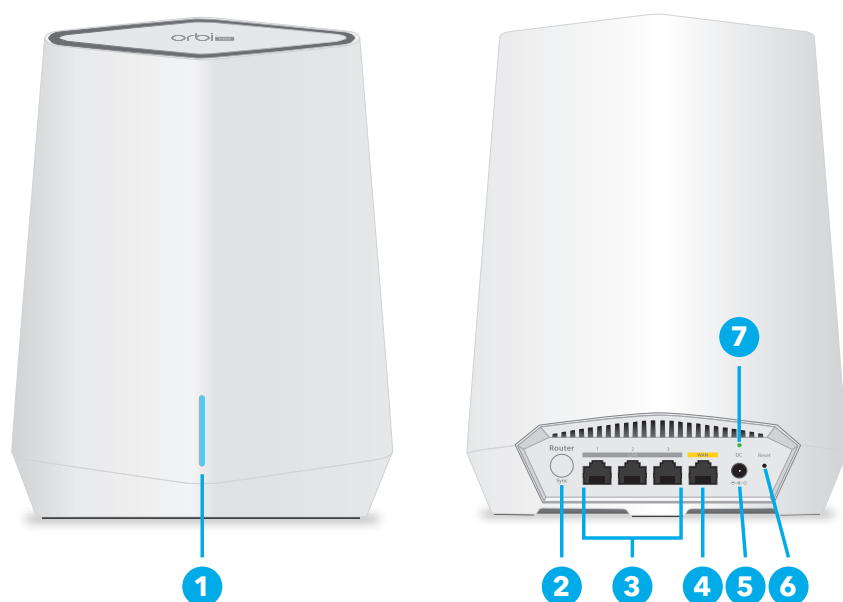


Figure 1. Orbi Pro WiFi 6 AX5400 router model SXR50, front and back views

1. Bar LED
2. Sync button (also used for WPS connection)

3. LAN Gigabit Ethernet ports 1-3. LAN ports 1 and 2 support link aggregation.
4. WAN Gigabit Ethernet port (with a yellow label). Use this port for your Internet connection.
5. DC Power connector
6. Reset button
7. Power LED

## Orbi Pro WiFi 6 AX5400 satellite model SXS50 hardware

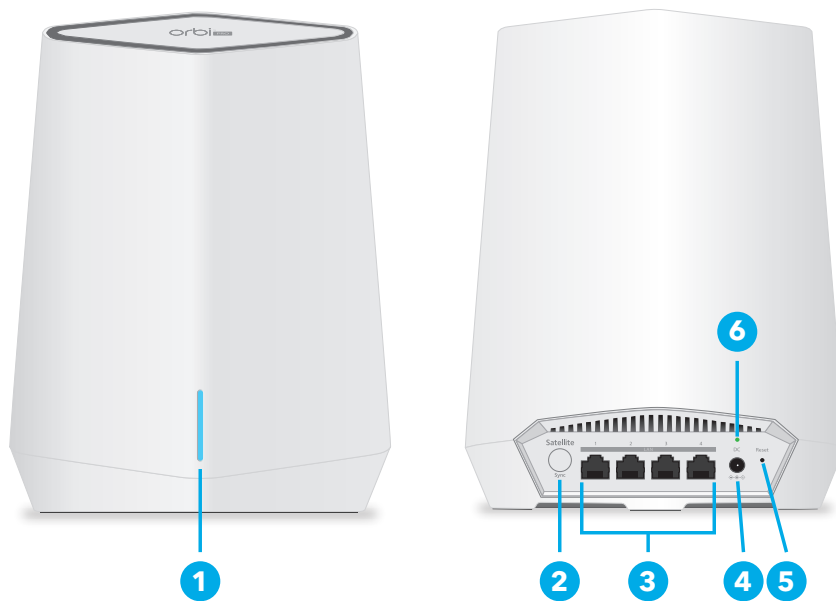


Figure 2. Orbi Pro WiFi 6 AX5400 satellite model SXS50, front and back views

1. Bar LED
2. Sync button (also used for WPS connection)
3. LAN Gigabit Ethernet ports 1-4. LAN ports 1 and 2 support link aggregation.
4. DC Power connector
5. Reset button
6. Power LED

# LED behavior

When you sync an Orbi Pro WiFi 6 AX5400 satellite to the Orbi Pro WiFi 6 AX5400 router, the LED behavior for a satellite that comes in an Orbi Pro WiFi 6 AX5400 system is different from the LED behavior for add-on Orbi Pro WiFi 6 AX5400 satellites.

## Orbi Pro WiFi 6 AX5400 System LEDs

The following table describes the LED behavior for an Orbi Pro WiFi 6 AX5400 router (model SXR50) and Orbi Pro WiFi 6 AX5400 satellite (model SXS50) that are purchased together and come in the same package.

Table 1. Orbi Pro WiFi 6 AX5400 System router and satellite LED descriptions

| LED               | LED Behavior   |
|-------------------|--|
| Power LED         | <p>The Power LED is located adjacent to the power connector on the rear panel.</p> <ul style="list-style-type: none"> <li>• <b>Solid green:</b> Power is on.</li> <li>• <b>Solid amber:</b> The router or satellite is booting.</li> <li>• <b>Blinking amber:</b> The router or satellite is resetting to factory default settings.</li> <li>• <b>Blinking red:</b> The firmware is corrupted.</li> <li>• <b>Off:</b> Power is not supplied.</li> </ul>  |
| Router bar LED    | <p>The bar LED is located on the front.</p> <ul style="list-style-type: none"> <li>• <b>Pulsing white:</b> The router is booting or someone pressed the <b>Sync</b> button.</li> <li>• <b>Off:</b> The router finished booting and is working normally.</li> <li>• <b>Solid white:</b> The router is resetting to factory default settings.</li> <li>• <b>Solid magenta:</b> The router cannot connect to the Internet. See <a href="#">You cannot access the Internet</a> on page 209.</li> </ul>   |
| Satellite bar LED | <p>This satellite is included when you buy an Orbi router. The bar LED is located on the front.</p> <ul style="list-style-type: none"> <li>• <b>Pulsing white:</b> The satellite is booting.</li> <li>• <b>Blue for three minutes:</b> The connection between the satellite and the router is good.</li> <li>• <b>Amber for three minutes:</b> The connection between the satellite and the router is fair.</li> <li>• <b>Magenta:</b> The satellite failed to sync to the router. See <a href="#">The router and satellite do not sync</a> on page 207.</li> <li>• <b>Off:</b> The satellite synced to the router and is working normally.</li> </ul> |

## Add-on Orbi Pro WiFi 6 AX5400 satellite LEDs

The following table describes the LED behavior for an add-on Orbi Pro WiFi 6 AX5400 satellite (model SXS50) that was purchased separately from the Orbi Pro WiFi 6 AX5400 System kit.

Table 2. Orbi Pro WiFi 6 AX5400 add-on satellite (model SXS50) LED description

| LED                      | LED Behavior   |
|--------------------------|--|
| Power LED                | <p>The Power LED is located adjacent to the power port on the rear panel.</p> <ul style="list-style-type: none"> <li>• <b>Solid green:</b> Power is on.</li> <li>• <b>Solid amber:</b> The satellite is rebooting.</li> <li>• <b>Blinking amber:</b> The satellite is resetting to factory default settings.</li> <li>• <b>Blinking red:</b> The firmware is corrupted.</li> <li>• <b>Off:</b> Power is not supplied.</li> </ul>   |
| Add-on satellite bar LED | <p>Optional add-on satellites are sold separately and can be added to your Orbi network. The bar LED is located on the front.</p> <ul style="list-style-type: none"> <li>• <b>Pulsing white:</b> The satellite is booting.</li> <li>• <b>Solid white:</b> The satellite is ready to sync to the router (press the <b>Sync</b> button).</li> <li>• <b>Blue for three minutes:</b> The connection between the satellite and the router is good.</li> <li>• <b>Amber for three minutes:</b> The connection between the satellite and the router is fair.</li> <li>• <b>Magenta:</b> The satellite is not connected to the router or is not getting an IP address.</li> <li>• <b>Off:</b> The satellite synced to the router and is working normally.</li> </ul> |

## Orbi Pro WiFi 6 AX5400 router and satellite labels

The Orbi Pro WiFi 6 AX5400 router label shows the login information, the WiFi network name and password, the router's MAC address, and the router's serial number. The following is an example of what the router label might look like:



Figure 3. Orbi Pro WiFi 6 AX5400 Model SXR50 router label

The Orbi Pro WiFi 6 AX5400 satellite label shows the WiFi network name and password, the satellite's MAC address, and the satellite's serial number. The following is an example of what the satellite label might look like:



Figure 4. Orbi Pro WiFi 6 AX5400 SXS50 satellite label

## Connect your Orbi Pro WiFi 6 AX5400 router

The back of the router has one yellow WAN port and three LAN ports. The label on the router displays model SXR50, and the preset WiFi network name (SSID) and password.

### **To cable your Orbi Pro router:**

1. Connect your Orbi Pro router to a modem or gateway that provides Internet.
  - If you use a modem, unplug the modem, remove and then reinsert the backup battery if it uses one, and plug the modem back in.
  - If you use a WiFi gateway, we recommend that you turn off your gateway's WiFi.
2. Use an Ethernet cable to connect your modem or gateway to the yellow WAN port on the back of your router.
3. Connect the power adapter to your router and plug the power adapter into an outlet. The Power LED on the back of the router lights green.

When the bar LED on the front of the router lights solid white, the router's preset WiFi network is ready for setup.

The router's bar LED turns off after about three minutes.



## Place your Orbi Pro WiFi 6 AX5400 satellite

Your satellite must be within range of your router's WiFi signal in order for it to sync with the router.

For the sync process, we recommend that you place the satellite approximately 10 ft. away from the router, facing the router, with a direct line of sight.

Use the satellite's bar LED to help you determine where to place your satellite.

# Sync your Orbi Pro WiFi 6 AX5400 satellite

The sync process for your Orbi Pro WiFi 6 AX5400 satellite depends on whether your satellite came with your Orbi Pro WiFi 6 AX5400 system, or if your satellite is an add-on satellite.

## Sync a satellite from an Orbi Pro WiFi 6 AX5400 system

The Orbi Pro WiFi 6 AX5400 system includes an Orbi Pro WiFi 6 AX5400 router and a Orbi Pro WiFi 6 AX5400 satellite. The Orbi Pro WiFi 6 AX5400 satellite that is packaged with an Orbi Pro WiFi 6 AX5400 router is preset to automatically find and sync to the router's WiFi signal.

### To sync your Orbi Pro WiFi 6 AX5400 satellite:

1. Place your satellite.

For more information, see [Place your Orbi Pro WiFi 6 AX5400 satellite](#) on page 16.

2. Connect the satellite to a power source.

The Power LED on the back of the satellite lights green.

The satellite bar LED pulses white. The satellite automatically finds the router's WiFi signal and attempts to sync to the Orbi Pro WiFi 6 AX5400 router.

**Note:** The first time that you sync the satellite and the router, the sync process can take up to five minutes because the router might automatically update the satellite's firmware.

The satellite bar LED lights one of the following colors for about three minutes and then turns off:

- **Blue:** The router and satellite successfully synced, and the connection between the router and satellite is good.
- **Amber:** The router and satellite successfully synced, and the connection between the router and satellite is fair. Consider moving the satellite closer to the router.
- **Magenta:** The router and satellite failed to sync.

3. If the satellite bar LED is magenta, move the satellite closer to the router and then sync the satellite to the router:

- a. Press the **Sync** button on the back of the router.

- b. Within two minutes, press the **Sync** button on the back of the satellite.

The satellite attempts to sync to the router. The satellite bar LED lights blue, amber, or magenta as described in [Step 2](#) of this procedure and then turns off.

## Sync an add-on Orbi Pro WiFi 6 AX5400 satellite

If you already set up an Orbi Pro WiFi 6 AX5400 router and satellite and you are adding an optional add-on Orbi Pro WiFi 6 AX5400 satellite (sold separately), follow the steps in this section.

**Note:** When you purchase an Orbi Pro WiFi 6 AX5400 satellite separately from the Orbi Pro WiFi 6 AX5400 router, the satellite has a different WiFi network name and password. However, after syncing the add-on satellite with the router, the satellite uses the same WiFi network name and password as the router.

### To sync your add-on Orbi Pro WiFi 6 AX5400 satellite:

1. Place your satellite.  
For more information, see [Place your Orbi Pro WiFi 6 AX5400 satellite](#) on page 16.
2. Connect the satellite to a power source.  
The power LED on the back of the satellite lights green.
3. Wait about two minutes for the satellite bar LED to light solid white.
4. Press the **Sync** button on the back of the satellite and within two minutes, press the **Sync** button on the back of your Orbi WiFi 6 AX5400 router.  
The satellite bar LED pulses white, then lights one of the following colors for about three minutes, and then turns off:
  - **Blue:** The router and satellite successfully synced, and the connection between the router and satellite is good.
  - **Amber:** The router and satellite successfully synced, and the connection between the router and satellite is fair. Consider moving the satellite closer to the router.
  - **Magenta:** The router and satellite failed to sync. Move the satellite closer to the router and try again.

**Note:** The first time that you sync the satellite and the router, the sync process can take up to five minutes because the router might automatically update the satellite's firmware.

## Add satellites to your network using the router web interface

You can use the Orbi Pro WiFi 6 AX5400 router web interface to add a satellite to your Orbi network.

### To add a satellite to your Orbi network using the router web interface:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **Add Orbi Pro Satellite**.

The Place Your Satellite page displays.

5. Follow the instructions about where to place your satellite at your location.

6. Connect the satellite to a power source.

7. Click the **NEXT** button.

8. Wait about two minutes for the satellite's bar LED to light solid white.

9. Press the **Sync** button on the satellite.

The satellite's bar LED pulses white.

10. Click the **SYNC** button in the router web interface.

The router attempts to sync with the satellite.

The satellite's bar LED lights one of the following colors for about three minutes and then turns off:

- **Blue:** The router and satellite successfully synced, and the connection between the router and satellite is good.
- **Amber:** The router and satellite successfully synced, and the connection between the router and satellite is fair. Consider moving the satellite closer to the router.
- **Magenta:** The router and satellite failed to sync. Move the satellite closer to the router and try again.

**Note:** The first time that you sync the satellite and the router, the sync process can take up to five minutes because the router might automatically update the satellite's firmware.

## Set up your satellite with a wired connection to your router

Instead of using a WiFi backhaul connection between the router and the satellite, you can use a wired connection.

### Set up and sync an Orbi Pro satellite over a wired connection

In some situations, you might prefer to set up your Orbi Pro satellite with an Ethernet cable directly connected to your Orbi Pro router.

If your business has built-in Ethernet outlets in the office rooms and the cables lead into the same physical network, you can also connect both your Orbi Pro router and Orbi Pro satellite to the Ethernet outlets and let them sync.

#### **To set up and sync your Orbi Pro satellite over a wired connection:**

1. Place your satellite in the room where you want WiFi service.
2. Connect an Ethernet cable to one of the LAN ports.
3. Connect the other end of the Ethernet cable to a LAN port on the router.
4. Connect the satellite to a power source.

The Power LED on the back of the satellite lights green.

The satellite bar LED pulses white. The satellite automatically syncs to the Orbi Pro router.

**Note:** The first time that you sync the satellite and the router, the sync process can take up to five minutes because the router might automatically update the satellite's firmware.

After the sync process is complete, the satellite bar LED lights blue for about three minutes and then turns off. Blue indicates that the router and satellite successfully synced, and the wired connection between the router and satellite is good.

## Ethernet backhaul connections for multiple satellites

Your Orbi Pro WiFi 6 satellite automatically connects over WiFi to your Orbi Pro router or another Orbi Pro satellite to create a WiFi backhaul connection, or you can use an Ethernet cable to connect your satellite to your router or another satellite to create a wired backhaul connection.

Before you set up an Ethernet backhaul connection, make sure that you update the firmware on all your Orbi Pro WiFi 6 devices.

**Note:** The products shown in the following diagrams do not represent any particular Orbi Pro models, but the topologies and setups in the diagrams do apply to your models.

The following figure shows how to connect your Orbi Pro WiFi 6 satellites to your Orbi Pro WiFi 6 router using a star topology to create an Ethernet backhaul connection.

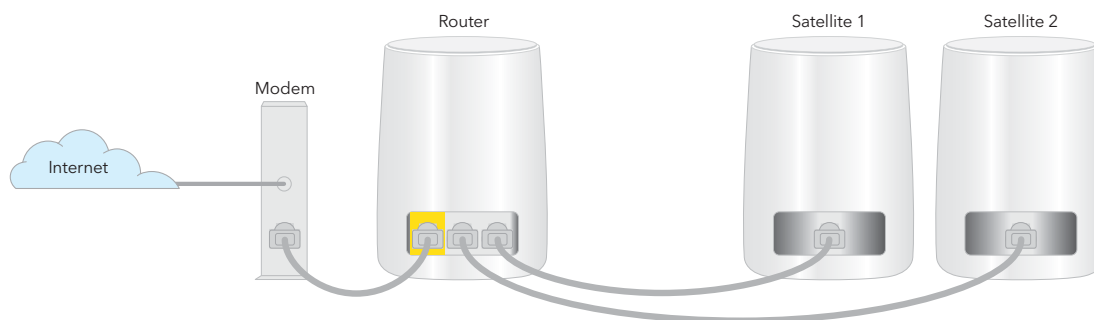


Figure 5. Star topology: Satellites connected to the router's Ethernet ports

The following figure shows another way to connect your Orbi Pro WiFi 6 satellites to your Orbi Pro WiFi 6 router using a daisy chain topology to create an Ethernet backhaul connection.

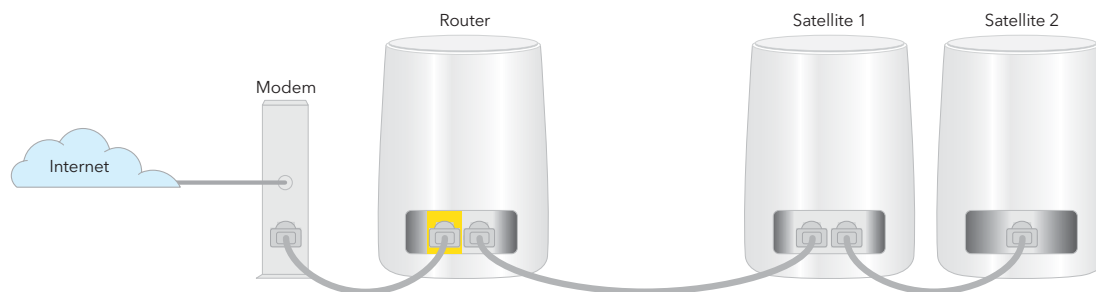


Figure 6. Daisy chain topology: Satellite 1 connected to router and satellite 2 connected to satellite 1

The following figure shows how to connect your Orbi Pro WiFi 6 satellites to your Orbi Pro WiFi 6 router through an Ethernet switch.

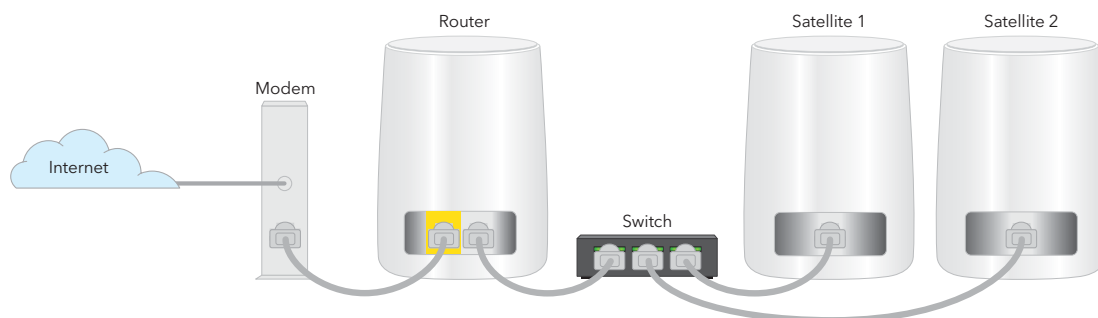


Figure 7. Ethernet backhaul connection using a switch

## Manage and monitor your Orbi network with NETGEAR Insight

If you are a NETGEAR Insight Premium or Pro subscriber, after you use the router web interface to set up your Orbi system, you can use NETGEAR Insight to manage and monitor your Orbi network remotely.

For more information about NETGEAR Insight, visit <https://www.netgear.com/insight/>.



## NETGEAR Insight Business VPN

NETGEAR Insight Business VPN enables Orbi Pro routers to support a virtual private network (VPN) tunnel between a main site and remote sites. A VPN tunnel allows secure data traffic with encryption for work-from-home employees or between business branches. Insight Business VPN requires an Orbi Pro router at each end of the VPN tunnel.

After Insight Business VPN is configured, the end user does not need to use a VPN client, log in, or use two-factor authentication (2FA): They connect to the existing office SSID and they are on the VPN. VPN access is also supported for wired clients and network devices that are cabled to the LAN ports of a router at a remote site.

Insight Business VPN features include site-to-site VPN connectivity, creating and deleting VPN groups for easy group management per main site, user management to control authentication and manage VPN access for users, business sites, information and systems and many more features.

**Note:** You cannot configure Insight Business VPN with the router web interface. You must use NETGEAR Insight.

If you are a NETGEAR Insight Premium or Pro subscriber, you can purchase a Business VPN subscription. Each remote site requires a subscription. A main site does not require a subscription. For more information about subscriptions, visit [netgear.com/business/services/insight/services/](https://netgear.com/business/services/insight/services/).

For more information about Insight Business VPN, visit <https://kb.netgear.com/000063726>.

# 2

## Connect to the Orbi Pro WiFi 6 AX5400 Network and Access the Router

---

To manage your Orbi Pro WiFi 6 AX5400 router and any Orbi Pro WiFi 6 AX5400 satellites that are connected to your Orbi Pro WiFi 6 network, you must manage them from your Orbi Pro WiFi 6 AX5400 router web interface.

This chapter contains the following sections:

- [Connect to the network for initial configuration](#)
- [Types of logins](#)
- [Use a web browser to access the router](#)
- [Change the language](#)
- [What to do if you get a browser security warning](#)

# Connect to the network for initial configuration

You can connect to the Orbi network through a wired or WiFi connection.

**Note:** If you set up your computer to use a static IP address, change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

## Wired connection

You can connect your computer to the router using an Ethernet cable and join the router's local area network (LAN).

### **To connect your computer to the router with an Ethernet cable:**

1. Make sure that the router is receiving power (its Power LED is lit).
2. Connect an Ethernet cable to an Ethernet port on your computer.
3. Connect the other end of the Ethernet cable to one of the router's Ethernet ports.  
Your computer connects to the LAN.

## WiFi connection

When you install your Orbi router for the first time, you can connect to the router's WiFi network by scanning the QR code on your router with the camera app on your mobile device. To scan the QR code with your camera app, your mobile device must have iOS version 11 or later, or Android version 10 or later.

You can also manually find and select the Orbi router's WiFi network from your WiFi-enabled computer or mobile device.

### **To find and select the WiFi network:**

1. Make sure that the router is receiving power (its Power LED is lit).
2. On your WiFi-enabled computer or mobile device, find and select the WiFi network.  
The WiFi network name is on the router label.
3. Join the WiFi network and enter the WiFi password.  
The password is on the router or satellite label.  
Your WiFi-enabled computer or mobile device connects to the WiFi network.

## WiFi connection using WPS

You can connect to the router's WiFi network with Wi-Fi Protected Setup (WPS) or you can find and select the WiFi network.

### To use WPS to connect to the WiFi network:

1. Make sure that the router is receiving power (its Power LED is lit).
2. Check the WPS instructions for your computer or WiFi device.
3. Press the **Sync** button on the router.
4. Within two minutes, on your WiFi-enabled computer or mobile device, press its **WPS** button or follow its instructions for WPS connections.

Your computer or mobile device connects to the WiFi network.

## Types of logins

You must use different logins for different types of tasks:

- **Internet service login:** The login information that your Internet service provider (ISP) gave you lets your router connect to your Internet service. Your service provider gave you this login information in a letter or some other way. If you cannot find this login information, contact your ISP.
- **WiFi network login:** Your router uses a preset WiFi network name (SSID) and password for WiFi access. This information is on the router label. During setup, you can change the WiFi network name (SSID) and password for increased security.
- **Orbi Pro router login:** The password that logs you in to the router interface from a web browser as the admin. The default password for initial login is **password**. During setup or at initial login, you must specify a new password for increased security.

## Use a web browser to access the router

When you connect to the network (either through WiFi or through an Ethernet cable), you can use a web browser to access the router to view or change the settings for the router and the satellites that you synced with the router.

The first time you log in to the router web interface, use the interactive Internet setup process to connect your router to your Internet service. You can also set up your router manually.

## Use the interactive Internet setup process

Before you start the interactive Internet setup process, get your ISP information and make sure that the computers and devices in the network use the settings described here.

When your Internet service starts, your Internet service provider (ISP) typically gives you all the information needed to connect to the Internet.

For DSL service, you might need the following information to set up your router:

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

If you cannot locate this information, ask your ISP to provide it.

The interactive Internet setup process takes about 10 minutes to complete.

### **To use the interactive Internet setup process:**

1. Power on your router.
2. Make sure that your WiFi-enabled computer or mobile device is connected to the router with an Ethernet cable (wired) or wirelessly with the preset security settings listed on the label.

**Note:** If you want to change the router's WiFi settings, use a wired connection so the WiFi device that you are using for setup is not disconnected when the new WiFi settings take effect.

3. Launch a web browser.

If your browser displays a security message, see [What to do if you get a browser security warning](#) on page 29.

The page that displays depends on whether you accessed the router before:

- The first time that you set up the Internet connection for your router, the browser goes to **orbilogin.com**, and the Orbi login page displays.
- If you already set up the Internet connection, enter **orbilogin.com** in the address field for your browser to start the installation process.

4. Follow the onscreen instructions.

The router connects to the Internet.

If your browser does not display the web page or your router does not connect to the Internet, see the following troubleshooting suggestions.

|  |   |
|--|---|
| Your browser does not display the web page   | Your router does not connect to the Internet  |
| Make sure that the computer is connected to the router through one of the LAN Ethernet ports, or is connected through WiFi.                                    | Review your settings.   |
| Make sure that the router is receiving power, and that its Power LED is lit  | Make sure that you selected the correct options and typed everything correctly.           |
| Close and reopen your browser or clear the browser cache.  | Contact your ISP to verify that you are using the correct configuration information.      |
| Browse to <b>orbilogin.com</b> .   | Read the information in <a href="#">Troubleshooting</a> on page 206.                      |
| If your computer is set to a static or fixed IP address (this setting is uncommon), change its settings to obtain an IP address automatically from the router. | If problems persist, register your NETGEAR product and contact NETGEAR technical support. |

## Log in to the Orbi router web interface

When you log in to the Orbi, the browser displays the router web interface. You can use the router web interface to change the router or satellite settings.

### To log in to your Orbi:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

# Change the language

By default, the language is set as Auto.

## To change the language:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. In the upper right corner, select a language from the menu.
5. When prompted, click the **OK** button to confirm this change.  
The page refreshes with the language that you selected.

# What to do if you get a browser security warning

Access to the router web interface is encrypted through the Hyper Text Transfer Protocol Secure (HTTPS) protocol, instead of the Hyper Text Transfer Protocol (HTTP). The extra security of HTTPS requires your browser to verify that **orbilogin.com** (which is the same as 192.168.1.1) is safe. As a result, a security warning can display in your browser when you try to access that domain. This is expected behavior. You can proceed, or add an exception for the security warning.

To proceed with a security warning or add an exception for a security warning:

- **Google Chrome:** Click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the domain name or IP address of the device.
- **Apple Safari:** Click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window displays, click the **Visit Website** button. If another

pop-up window displays to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.

- **Mozilla Firefox:** Click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
- **Microsoft Edge:** Select **Details > Go on to the webpage**.
- **Microsoft Internet Explorer:** Click the **Continue to this website (not recommended)** link.

# 3

## Specify Your Internet Settings

---

Usually, the quickest way to set up the router to use your Internet connection is to allow Orbi to detect the Internet connection when you first access the router with a web browser. You can also customize or specify your Internet settings.

This chapter contains the following sections:

- [Setup Wizard](#)
- [Manually set up the Internet connection](#)
- [IPv6 Internet connections](#)
- [MTU size](#)

# Setup Wizard

You can use the Setup Wizard to detect your Internet settings and automatically set up your router.

## To use the Setup Wizard:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup Wizard**.  
The Setup Wizard page displays.
5. Select the **Yes** radio button.  
If you select **No**, you are taken to the Internet Setup page (see [Manually set up the Internet connection](#) on page 32).
6. Click the **Next** button.  
The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration and checks your operation mode.

## Manually set up the Internet connection

You can set up, view, or change the router's Internet connection settings.

The type of Internet connection (with or without login) depends on your ISP.

## Set up an Internet connection without a login

### To set up an Internet connection that does not use a login:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Internet**.  
The Internet Setup page.
5. Leave the Does your Internet connection require a login **No** radio button selected.
6. If your Internet connection requires an account name or host name, do the following:
  - a. Next to the **Account Name (If Required)** field, click the **Edit** button.  
The Device Name page displays.
  - b. Type the name in the **Device Name** field.
  - c. Click the **Apply** button.  
The Internet Setup page displays again.
7. If your Internet connection requires a domain name, type it in the **Domain Name (If Required)** field.  
For the other sections in this page, the default settings usually work, but you can change them.
8. Select an Internet IP Address radio button:
  - **Get Dynamically from ISP:** Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
  - **Use Static IP Address:** Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP router to which your router connects.

9. Select a Domain Name Server (DNS) Address radio button:
  - **Get Automatically from ISP:** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
  - **Use These DNS Servers:** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a second DNS server address and a third DNS server address are available, enter them also.
10. Select a Router MAC Address radio button:
  - **Use Default Address:** Use the default MAC address.
  - **Use Computer MAC Address:** The router captures and uses the MAC address of the computer that you are now using. If your ISP allows a single MAC address only, you must use the one computer that the ISP allows.
  - **Use This MAC Address:** Enter the MAC address that you want to use.
11. Click the **Apply** button.

Your settings are saved.
12. Click the **Test** button to test your Internet connection.

## Set up an Internet connection with a login

### **To set up an Internet connection that uses a login:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
  2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
  3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.
  4. Select **Internet**.

The Internet Setup page displays.
  5. Select the Does your Internet connection require a login **Yes** radio button.
-

The page adjusts.

6. From the **Internet Service Provider** menu, select the encapsulation method:  
The selections are **PPPoE**, **L2TP**, and **PPTP**.
  7. In the **Login** field, enter the login name your ISP gave you.  
This login name is often an email address.
  8. In the **Password** field, type the password that you use to log in to your Internet service.
  9. If your ISP requires a service name, type it in the **Service Name (if Required)** field.
  10. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.
  11. To change the number of minutes until the Internet login time out, in the **Idle Timeout (In minutes)** field, type the number of minutes.  
This is how long the router keeps the Internet connection active when no one on the network is using the Internet connection. A value of 0 (zero) means never log out. The default value is 5.
  12. Select an Internet IP Address radio button:
    - **Get Dynamically from ISP:** Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
    - **Use Static IP Address:** Enter the IP address, IP subnet mask, and gateway IP address that your ISP assigned. The gateway is the ISP router to which your router connects.
  13. Select a Domain Name Server (DNS) radio button:
    - **Get Automatically from ISP:** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
    - **Use These DNS Servers:** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a second DNS server address and a third DNS server address are available, enter them also.
  14. Select a Router MAC Address radio button:
    - **Use Default Address:** Use the default MAC address.
    - **Use Computer MAC Address:** The router captures and uses the MAC address of the computer that you are now using. If your ISP allows a single MAC address only, you must use the one computer that the ISP allows.
    - **Use This MAC Address:** Enter the MAC address that you want to use.
-

15. Click the **Apply** button.

Your settings are saved.

16. Click the **Test** button to test your Internet connection.

## IPv6 Internet connections

The router supports many different types of IPv6 Internet connections for which you can set the settings manually.

### Requirements for entering IPv6 addresses

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. You can reduce any four-digit group of zeros within an IPv6 address to a single zero or omit it. The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

### Set up IPv6 Internet connections

You can set up an IPv6 Internet connection if the router does not detect it automatically.

#### **To set up an IPv6 Internet connection:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. From the **Internet Connection Type** menu, select the IPv6 connection type:
  - If you are not sure, select **Auto Detect** so that the router detects the IPv6 type that is in use.
  - If your Internet connection does not use PPPoE, DHCP, or fixed, but is IPv6, select **Auto Config**.  
Your Internet service provider (ISP) can provide this information. For more information about IPv6 Internet connection, see the following sections:
    - [Use auto detection for an IPv6 Internet connection](#) on page 37
    - [Use auto configuration for an IPv6 Internet connection](#) on page 39
    - [Set up an IPv6 6to4 tunnel Internet connection](#) on page 40
    - [Set up an IPv6 6rd tunnel Internet connection](#) on page 42
    - [Set up an IPv6 pass-through Internet connection](#) on page 44
    - [Set up an IPv6 fixed Internet connection](#) on page 45
    - [Set up an IPv6 DHCP Internet connection](#) on page 46
    - [Set up an IPv6 PPPoE Internet connection](#) on page 48
6. Click the **Apply** button.  
Your settings are saved.

## Use auto detection for an IPv6 Internet connection

### To set up an IPv6 Internet connection through auto detection:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.  
The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Auto Detect**.

The page adjusts.

The router automatically detects the information in the following fields:

- **Connection Type:** This field indicates the connection type that is detected.
- **Router's IPv6 Address on WAN:** This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN:** This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. In the LAN Setup section, select an IP Address Assignment radio button:

- **Use DHCP Server:** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
- **Auto Config:** This is the default setting.

This setting specifies how the router assigns IPv6 addresses to the devices on your business network (the LAN).

7. (Optional) Select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

If you do not specify an ID here, the router generates one automatically from its MAC address.

8. Select an IPv6 Filtering radio button:

- **Secured:** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
- **Open:** In open mode, the router inspects UDP packets only.

9. Click the **Apply** button.

Your settings are saved.

## Use auto configuration for an IPv6 Internet connection

### To set up an IPv6 Internet connection through auto configuration:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.  
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Auto Config**.  
The page adjusts.  
The router automatically detects the information in the following fields:
  - **Router's IPv6 Address on WAN:** This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address. If no address is acquired, the field displays Not Available.
  - **Router's IPv6 Address on LAN:** This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address. If no address is acquired, the field displays Not Available.
6. (Optional) In the **DHCP User Class (If Required)** field, enter a host name.  
If your ISP gave you a specific host name, enter it here. Otherwise, leave this field blank.
7. (Optional) In the **DHCP Domain Name (If Required)** field, enter a domain name.  
You can type the domain name of your IPv6 ISP. Do not enter the domain name for the IPv4 ISP here. For example, if your ISP's mail server is mail.xxx.yyy.zzz, type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this

field. For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.

8. In the IPv6 Domain Name Server (DNS) Address section, select a radio button:
  - **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
  - **Use These DNS Servers.** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
9. In the LAN Setup section, select an IP Address Assignment radio button:
  - **Use DHCP Server:** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
  - **Auto Config:** This is the default setting.
10. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the router's LAN interface.  
If you do not specify an ID here, the router generates one automatically from its MAC address.
11. Select an IPv6 Filtering radio button:
  - **Secured:** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
  - **Open:** In open mode, the router inspects UDP packets only.
12. Click the **Apply** button.  
Your settings are saved.

## Set up an IPv6 6to4 tunnel Internet connection

The remote relay router is the router to which your router creates a 6to4 tunnel. Make sure that the IPv4 Internet connection is working before you apply the 6to4 tunnel settings for the IPv6 connection.

### To set up an IPv6 Internet connection by using a 6to4 tunnel:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **6to4 Tunnel**.

The page adjusts.

The router automatically detects the information in the Router's IPv6 Address on LAN field. This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. Select a Remote 6to4 Relay Router radio button:

- **Auto:** Your router uses any remote relay router that is available on the Internet. This is the default setting.
- **Static IP Address:** Enter the static IPv4 address of the remote relay router. Your IPv6 ISP usually provides this address.

7. In the IPv6 Domain Name Server (DNS Address), select a radio button:

- **Get Automatically from ISP:** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers:** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

8. In the LAN Setup section, select an IP Address Assignment radio button:

- **Use DHCP Server:** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
- **Auto Config:** This is the default setting.

This setting specifies how the router assigns IPv6 addresses to the devices on your business network (the LAN).

9. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the router's LAN interface.  
If you do not specify an ID here, the router generates one automatically from its MAC address.
10. Select an IPv6 Filtering radio button:
  - **Secured:** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
  - **Open:** In open mode, the router inspects UDP packets only.
11. Click the **Apply** button.  
Your settings are saved.

## Set up an IPv6 6rd tunnel Internet connection

The 6rd protocol makes it possible to deploy IPv6 to sites using a service provider's IPv4 network. 6rd uses the service provider's own IPv6 address prefix. This limits the operational domain of 6rd to the service provider's network and is under direct control of the service provider. The IPv6 service provided is equivalent to native IPv6. The 6rd mechanism relies on an algorithmic mapping between the IPv6 and IPv4 addresses that are assigned for use within the service provider's network. This mapping allows for automatic determination of IPv4 tunnel endpoints from IPv6 prefixes, allowing stateless operation of 6rd.

With a 6rd Tunnel configuration, the router follows the RFC5969 standard, supporting two ways to establish a 6rd tunnel IPv6 WAN connection:

- **Auto Detect Mode:** In IPv6 Auto Detect mode, when the router receives option 212 from the DHCPv4 option, auto detect selects the IPv6 as 6rd Tunnel setting. The router uses the 6rd option information to establish the 6rd connection.
- **Manual Mode:** Select 6rd. If the router receives option 212, the fields are automatically completed. Otherwise, you must enter the 6rd settings.

### To set up an IPv6 6rd Tunnel Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. In the **Internet Connection Type** menu, select **6rd**.

The page adjusts.

The router can automatically detect the information in the following sections:

- **6rd (IPv6 Rapid Deployment) Configuration:** The router detects the service provider's IPv4 network and attempts to establish an IPv6 6rd Tunnel connection. If the IPv4 network returns 6rd parameters to the router, the page adjusts to display the correct settings in this section.
- **Router's IPv6 Address on LAN:** This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. If the router does not automatically detect the information in the 6rd (IPv6 Rapid Development) Configuration section, specify the 6rd prefix, 6rd prefix length, 6rd IPv4 border relay address, and 6rd IPv4 address mask length that the router must use.

7. In the IPv6 Domain Name Server (DNS) Address section, select a radio button:

- **Get Automatically from ISP:** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers:** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

8. In the LAN Setup section, select an IP Address Assignment radio button:

- **Use DHCP Server:** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
- **Auto Config:** This is the default setting.

This setting specifies how the router assigns IPv6 addresses to the devices on your business network (the LAN).

9. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the router's LAN interface.  
If you do not specify an ID here, the router generates one automatically from its MAC address.
10. Select an IPv6 Filtering radio button:
  - **Secured**: In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
  - **Open**: In open mode, the router inspects UDP packets only.
11. Click the **Apply** button.  
Your settings are saved.

## Set up an IPv6 pass-through Internet connection

In pass-through mode, the router works as a Layer 2 Ethernet switch with two ports (LAN and WAN Ethernet ports) for IPv6 packets. The router does not process any IPv6 header packets.

### **To set up a pass-through IPv6 Internet connection:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.  
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Pass Through**.  
The page adjusts, but no additional fields display.
6. Click the **Apply** button.  
Your settings are saved.

## Set up an IPv6 fixed Internet connection

### To set up a fixed IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Fixed**.

The page adjusts.

6. In the WAN Setup section, configure the fixed IPv6 addresses for the WAN connection:

- **IPv6 Address/Prefix Length:** The IPv6 address and prefix length of the router WAN interface.
- **Default IPv6 Gateway:** The IPv6 address of the default IPv6 gateway for the router's WAN interface.
- **Primary DNS Server:** The primary DNS server that resolves IPv6 domain name records for the router.
- **Secondary DNS Server:** The secondary DNS server that resolves IPv6 domain name records for the router.

**Note:** If you do not specify the DNS servers, the router uses the DNS servers that are configured for the IPv4 Internet connection on the Internet Setup page. (See [Manually set up the Internet connection](#) on page 32.)

7. In the LAN Setup section, select an IP Address Assignment radio button:
  - **Use DHCP Server:** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
  - **Auto Config:** This is the default setting.

This setting specifies how the router assigns IPv6 addresses to the devices on your business network (the LAN).

8. In the **IPv6 Address/Prefix Length** fields, specify the static IPv6 address and prefix length of the router's LAN interface.  
If you do not specify an ID here, the router generates one automatically from its MAC address.

9. Select an IPv6 Filtering radio button:
  - **Secured:** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
  - **Open:** In open mode, the router inspects UDP packets only.

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

## Set up an IPv6 DHCP Internet connection

### **To set up an IPv6 Internet connection with a DHCP server:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.  
The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **DHCP**.

The page adjusts.

The router automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN:** This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( \_ ) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN:** This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( \_ ) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. (Optional) In the **User Class (If Required)** field, enter a host name.

Most people can leave this field blank, but if your ISP gave you a specific host name, enter it here.

7. (Optional) In the **Domain Name (If Required)** field, enter a domain name.

You can type the domain name of your IPv6 ISP. Do not enter the domain name for the IPv4 ISP here. For example, if your ISP's mail server is mail.xxx.yyy.zzz, type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this field. For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.

8. In the IPv6 Domain Name Server (DNS Address), select a radio button:

- **Get Automatically from ISP:** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers:** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

9. In the LAN Setup section, select an IP Address Assignment radio button:

- **Use DHCP Server:** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
- **Auto Config:** This is the default setting.

This setting specifies how the router assigns IPv6 addresses to the devices on your business network (the LAN).

10. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the router's LAN interface.

If you do not specify an ID here, the router generates one automatically from its MAC address.

11. Select an IPv6 Filtering radio button:

- **Secured:** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
- **Open:** In open mode, the router inspects UDP packets only.

12. Click the **Apply** button.

Your settings are saved.

## Set up an IPv6 PPPoE Internet connection

### To set up a PPPoE IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **PPPoE**.

The page adjusts.

The router automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN:** This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (\_\_) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN:** This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the

prefix, which is also indicated by the underline (   ) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. If already you set up your IPv4 ISP connection for PPPoE and want to use the same login information for IPv6, select the **Use the same Login information as IPv4 PPPoE** check box.

To manually configure the PPPoE settings for IPv6, specify the following settings:

- **Login:** Enter the login name that your ISP gave you. This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, you would type JerAB in this field. Some ISPs (like Earthlink) require that you use your full email address when you log in. If your ISP requires your full email address, type it in this field.
- **Password.** Enter the password for the ISP connection.
- **Service Name (if Required).** Enter a service name. If your ISP did not provide a service name, leave this field blank.

**Note:** The default setting of the **Connection Mode** field is Always On to provide a steady IPv6 connection. The router never terminates the connection. If the connection is terminated, for example, when the modem is turned off, the router attempts to reestablish the connection immediately after the PPPoE connection becomes available again.

7. In the IPv6 Domain Name Server (DNS Address), select a radio button
  - **Get Automatically from ISP:** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
  - **Use These DNS Servers:** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
8. In the LAN Setup section, select an IP Address Assignment radio button:
  - **Use DHCP Server:** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
  - **Auto Config:** This is the default setting.

This setting specifies how the router assigns IPv6 addresses to the devices on your business network (the LAN).

9. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the router's LAN interface.

If you do not specify an ID here, the router generates one automatically from its MAC address.

10. Select an IPv6 Filtering radio button:

- **Secured:** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
- **Open:** In open mode, the router inspects UDP packets only.

11. Click the **Apply** button.

Your settings are saved.

## MTU size

The maximum transmission unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If a device in the data path uses a lower MTU setting than the other devices, the data packets must be split or “fragmented” to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU unchanged unless one of these situations occurs:

- You experience problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that does not open, or displays only part of a web page
  - Yahoo email
  - MSN portal
- You use VPN and experience severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you are experiencing connectivity or performance problems.

**Note:** An incorrect MTU setting can cause Internet communication problems. For example, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

### To change the MTU size:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > WAN Setup**.

The WAN Setup page displays.

5. In the **MTU Size** field, enter a value from 616 to 1500.

6. Click the Apply button.

Your settings are saved.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. The following table describes common MTU sizes and applications.

Table 3. Common MTU sizes

| MTU  | Application   |
|------|---|
| 1500 | The largest Ethernet packet size. This setting is typical for connections that do not use PPPoE or VPN, and is the default value for NETGEAR routers, adapters, and switches. |
| 1492 | Used in PPPoE environments.   |
| 1472 | Maximum size to use for ping. (Larger packets are fragmented.)  |
| 1468 | Used in some DHCP environments.   |
| 1436 | Used in PPTP environments or with VPN.  |

# 4

## Control Access to the Internet

---

The router comes with a built-in firewall that helps protect your business network from unwanted intrusions from the Internet.

This chapter includes the following sections:

- [MAC access control lists](#)
- [Network access control list](#)
- [Block Internet sites by using keywords](#)
- [Delete keywords that are used to block Internet sites](#)
- [Trusted computer](#)
- [Block services from the Internet](#)
- [Schedule when to block Internet sites and services](#)
- [Email notifications for security events](#)

# MAC access control lists

A MAC access control list (ACL) for a WiFi network (that is, an SSID) or the wired network (that is, the LAN) allows or denies a device access to the network based only on the MAC address of the device. If you block a device for one WiFi network or for the wired network, the device is blocked only for that WiFi network or for the wired network. You can set up an independent MAC ACL for each WiFi network and for the wired network. (The router supports multiple MAC ACLs.) With a MAC ACL, you can allow or deny access to a device on a specific WiFi network or the wired network.

**Note:** A MAC ACL differs from the network access control list (see [Network access control list](#) on page 58). The network access control list is not specific to a particular WiFi network or to the wired network but is based on both WiFi and wired devices that the router detects on the entire Orbi network. To allow or deny access to a device on a specific WiFi network or the wired network, use a MAC ACL. MAC ACLs and the network access control list are mutually exclusive. Use either MAC ACLs or the network access control list.

If you set up a MAC ACL with a policy that allows access to a specific network, devices on the MAC ACL are an exception to the default policy:

- A device for which you place the MAC address on the MAC ACL is *denied access* to that network.
- All other devices are allowed access to that network.

If you set up a MAC ACL with a policy that denies access to a specific network, devices on the MAC ACL are an exception to the default policy:

- A device for which you place the MAC address on the MAC ACL is *allowed access* to that work.
- All other devices are denied access to that network.

A blocked device can still get an IP address from the router but cannot communicate with other devices on the network or connect to the Internet.

**Note:** Each network device owns a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0-9, a-f, or A-F (uppercase or lowercase) only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of a device. If you cannot see the label, you can display the MAC address using the network configuration utilities of a computer. You might also find the MAC addresses on [Attached Devices](#) page of the router (see [View satellites, WiFi devices, and wired devices connected to the Orbi network](#) on page 151).

## Enable a MAC ACL for a specific network

When you enable a MAC ACL for a specific network, you must specify the default policy for that network. The default policy determines whether devices that you add to the MAC ACL are allowed or denied access to that specific network.

You can set up an independent MAC ACL for each of the WiFi networks and for the wired network. That is, the router supports multiple MAC ACLs.

### To enable a MAC ACL for a specific network:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Security > MAC ACL**.  
The MAC ACL page displays.
5. Go to the section for the network for which you want to set up a MAC ACL.

**Note:** Each section name corresponds to the SSID (WiFi network name) of a WiFi network, but the section for the Ethernet network is called Wired. If you did not change the SSIDs (see [Manage the WiFi Networks](#) on page 85), the unique preset SSIDs for your product are displayed.

6. For the specific network, click the Enable MAC Access Control **Disabled** button.  
The button changes to the green Enabled button.

**Note:** If you enabled the network access control list (see [Enable the network access control list and specify the access rule](#) on page 59), you cannot enable any MAC ACLs. The network access control list and MAC ACLs are mutually exclusive. Use either the network access control list or MAC ACLs.

7. From the **Default Policy** menu, select one of the following options:
  - **Allow:** The policy is to allow all devices access except for the devices that you add to the MAC ACL. Devices on the MAC ACL are denied access to the specific network.
  - **Deny:** The policy is to deny all devices access except for the devices that you add to the MAC ACL. Devices on the MAC ACL are allowed access to the specific network.

You can now add and manage devices on the MAC ACL. For more information, see the following sections:

- [Add automatically detected devices to a MAC ACL](#) on page 55
- [Manually add, remove, or change the information for a device on a MAC ACL](#) on page 56

## Add automatically detected devices to a MAC ACL

After you set up a MAC ACL for a network and specify the default policy for the MAC ACL, the router automatically detects devices that are connected or were connected to the network for which you set up the MAC ACL.

You can select one or multiple devices from the detected list and add them to the MAC ACL.

### **To add automatically detected devices to a MAC ACL:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Security > MAC ACL**.  
The MAC ACL page displays.
5. Go to the section for the network for which you want to manage the MAC ACL.

6. If the Enable MAC Access Control Disabled button displays for the specific network, click the **Disabled** button.  
The button changes to the green Enabled button.
7. Click the **ADD DEVICE** button.  
The Manual Access Management pop-up window opens.
8. Select the check boxes for the devices that you want to add to the MAC ACL.
9. Click the **ADD** button.  
The devices are added to the MAC ACL on the MAC ACL page. Devices on the MAC ACL are an exception to the default policy:
  - If the default policy of the MAC ACL is to allow access, the added devices are denied access.
  - If the default policy of the MAC ACL is to deny access, the added devices are allowed access.

## Manually add, remove, or change the information for a device on a MAC ACL

After you set up a MAC ACL for a network and specify the default policy for the MAC ACL, you can manually add a device, remove a device, or change the name (but not the MAC address) for a device on the MAC ACL.

By manually adding a device, you can proactively control access for a device that is not or not yet detected, or that was not detected by the router.

To manually add, remove, or change the name for a device on a MAC ACL:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.

4. Select **ADVANCED > Security > MAC ACL**.

The MAC ACL page displays.

5. Go to the section for the network for which you want to manage the MAC ACL.

6. To manually add a device to the MAC ACL, do the following:

- a. Click the **MANUAL** button.

The Manual Access Management pop-up window opens.

- b. Enter the MAC address and device name for the device that you want to add.

- c. In the Manual Access Management pop-up window, click the **ADD** button.

The device is added to the MAC ACL on the MAC ACL page. Devices on the MAC ACL are an exception to the default policy:

- If the default policy of the MAC ACL is to allow access, the added device is denied access.
- If the default policy of the MAC ACL is to deny access, the added device is allowed access.

7. To remove a device from the MAC ACL, do the following:

- a. Select the check box for the device.

- b. Click the **REMOVE DEVICE** button.

The device is removed from the MAC ACL.

8. To change the name for a device on the MAC ACL, do the following:

- a. Next to the device in the table, click the **EDIT** button.

The Manual Access Management pop-up window opens.

- b. Change the device name.

- c. In the Manual Access Management pop-up window, click the **EDIT** button.

The device name is changed in the MAC ACL on the MAC ACL page.

## Disable a MAC ACL for a specific network

You can disable a MAC ACL that you already set up. The devices are not removed from the MAC ACL, but all devices on the MAC ACL can connect to the network for which you setup the MAC ACL, even if the default policy of the MAC ACL is to deny access to the devices.

To disable a MAC ACL for a specific network:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Security > MAC ACL**.  
The MAC ACL page displays.
5. Go to the section for the network for which you want to disable the MAC ACL.
6. For the specific network, click the Enable MAC Access Control **Enabled** button.  
The button changes to the gray Disabled button. The MAC ACL is disabled.

## Network access control list

You can use the network access control list (ACL) to block or allow access to the entire Orbi network. An ACL functions with the MAC addresses of WiFi and wired devices that the router detects on the Orbi network and that you can either allow access to your network or deny access to your network. That is, the router can detect the MAC addresses of devices that are or were connected to the Orbi network and list the MAC addresses of these devices.

**Note:** The network access control list differs from a MAC ACL (see [MAC access control lists](#) on page 53). A MAC ACL is specific to a particular WiFi network or to the wired network but is not based on devices that the router detects on the entire Orbi network. With a MAC ACL, you can allow or deny access to a device on a specific WiFi network or the wired network. The network access control list and MAC ACLs are mutually exclusive. Use either the network access control list or MAC ACLs.

If you set up a network ACL with an access rule that allows access to the Orbi network, devices on the network ACL are an exception to the access rule:

- A device for which you place the MAC address on the network ACL is *denied access* to the Orbi network.
- All other devices are allowed access to the Orbi network.

If you set up a network ACL with an access rule that denies access to the Orbi network, devices on the network ACL are an exception to the access rule:

- A device for which you place the MAC address on the network ACL is *allowed access* to the Orbi network.
- All other devices are denied access to the Orbi network.

**Note:** Each network device owns a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0-9, a-f, or A-F (uppercase or lowercase) only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of a device. If you cannot see the label, you can display the MAC address using the network configuration utilities of a computer. You might also find the MAC addresses on Attached Devices page of the router (see [View satellites, WiFi devices, and wired devices connected to the Orbi network](#) on page 151).

## Enable the network access control list and specify the access rule

When you enable network access control, you must select whether new devices are allowed to access the Orbi network or are blocked from accessing the network. By default, connected devices are allowed access to the Orbi network, but you can also block these devices from accessing the Orbi network.

### **To enable and manage the network access control list for the entire Orbi network:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Security > Access Control**.

The Access Control page displays.

5. Select the **Turn on Access Control** check box.

You must select this check box before you can specify an access rule and use the **ALLOW** and **BLOCK** buttons. When the **Turn on Access Control** check box is cleared, all devices are allowed to connect, even if a device is in the list of blocked devices.

**Note:** If you enabled one or more MAC ACLs (see [Enable a MAC ACL for a specific network](#) on page 54), you cannot use the **ALLOW** and **BLOCK** buttons. MAC ACLs and the network access control list are mutually exclusive. Use either MAC ACLs or the network access control list.

6. Click the **Apply** button.

Your settings are saved.

7. Select an access rule for new devices:

- **Allow all new devices to connect:** With this setting, if you add a new device, it can access the Orbi network. You do not need to enter its MAC address on this page. We recommend that you leave this radio button selected.
- **Block all new devices from connecting:** With this setting, if you add a new device, before it can access the Orbi network, you must enter its MAC address for an Ethernet connection and its MAC address for a WiFi connection in the allowed list. For more information, see .

The access rule does not affect previously blocked or allowed devices. It applies only to devices joining the Orbi network in the future after you apply these settings.

8. To manage access for devices that are connected or were connected to the Orbi network, do the following:

- If you blocked all new devices from connecting, to allow the device that you are currently using to continue to access the Orbi network, select the check box next to your computer or device in the table, and click the **ALLOW** button.
- To either continue to allow or to block other computers and devices that are connected or were connected, select the check box next to the device in the table, and click either the **ALLOW** button or the **BLOCK** button.

9. Click the **Apply** button.

Your settings are saved.

## Manage the allowed devices on the network access control list

If you set up an access list that blocks all new devices from accessing the Orbi network, you must specify which devices are allowed to access the Orbi network.

You can add a device, remove a device, or edit the information for a device.

### To manage devices that are allowed to access to Orbi network:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Security > Access Control**.  
The Access Control page displays.
5. Click the **View list of allowed devices not currently connected to the network** link.  
A table displays the detected device name, MAC address, and connection type of the devices that are not connected but allowed to access the Orbi network.
6. To add a device to the allowed list, do the following:
  - a. Click the **ADD** button.  
The Add Allowed Device page displays.
  - b. Enter the MAC address and device name for the device that you want to allow.
  - c. On the Add Allowed Device page, click the **Apply** button.  
The device is added to the allowed list on the Access Control page.
7. To remove a device from the allowed list, do the following:
  - a. Select the check box for the device.
  - b. Click the **REMOVE FROM THE LIST** button.

The device is removed from the allowed list.

8. To change the information for a device on the allowed list, do the following:
  - a. Select the check box for the device.
  - b. Click the **EDIT** button.  
The Edit Allowed Device page displays.
  - c. Change the access rule, MAC address, or device name.
  - d. On the Edit Allowed Device page, click the **Apply** button.  
The device is changed on the allowed list on the Access Control page.
9. Click the **Apply** button.  
Your settings are saved.

## Manage the blocked devices on the network access control list

If you set up an access list that allows all new devices to access the Orbi network but you want to block some devices from accessing the Orbi network, you must specify the devices that you want to block.

You can add a device, remove a device, or change the information for a device.

### **To manage devices that are blocked from accessing the Orbi network:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning on page 29](#).
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Security > Access Control**.  
The Access Control page displays.

5. Click the **View list of blocked devices not currently connected to the network** link.

The Access Control page displays.

A table displays the detected device name, MAC address, and connection type of the devices that are not connected and are blocked from accessing the Orbi network.

6. To add a device to the blocked list, do the following:

- a. Click the **ADD** button.

The Add Blocked Device page displays.

- b. Enter the MAC address and device name for the device that you want to block.

- c. On the Add Blocked Device page, click the **Apply** button.

The device is added to the blocked list on the Access Control page.

7. To remove a device from the blocked list, do the following:

- a. Select the check box for the device.

- b. Click the **REMOVE FROM THE LIST** button.

The device is removed from the blocked list.

8. To change the information for a device on the blocked list, do the following:

- a. Select the check box for the device.

- b. Click the **EDIT** button.

The Edit Blocked Device page displays.

- c. Change the access rule, MAC address, or device name.

- d. On the Edit Blocked Device page, click the **Apply** button.

The device is changed on the blocked list on the Access Control page.

9. Click the **Apply** button.

Your settings are saved.

## Block Internet sites by using keywords

You can use keywords to block certain Internet sites from your network. You can use blocking all the time or based on a schedule.

### To block Internet sites:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Security > Block Sites**.  
The Block Sites page displays.
5. Select a keyword blocking option:
  - **Per Schedule**: To block the keywords based on a schedule, select the **Per Schedule** radio button. For information about how to set the schedule, see [Schedule when to block Internet sites and services](#) on page 68.
  - **Always**: To block the keywords all the time, select the **Always** radio button..
6. In the **Type keyword or domain name here** field, enter a keyword or domain that you want to block.  
For example:
  - Specify XXX to block <http://www.badstuff.com/xxx.html>.
  - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
  - Enter a period (.) to block all Internet browsing access.
7. Click the **Add Keyword** button.  
The keyword is added to the keyword list. The keyword list supports up to 32 entries.
8. Click the **Apply** button.  
Keyword blocking takes effect.

# Delete keywords that are used to block Internet sites

## To delete keywords that are used to block Internet sites:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Security > Block Sites**.  
The Block Sites page displays.
5. Do one of the following:
  - To delete a single word, select it and click the **Delete Keyword** button.  
The keyword is removed from the list.
  - To delete all keywords on the list, click the **Clear List** button.  
All keywords are removed from the list.
6. Click the **Apply** button.  
Your settings are saved.

## Trusted computer

You can exempt one trusted computer from blocking. The computer that you exempt must be assigned a fixed IP address. You can use the reserved IP address feature to specify the IP address. See [Reserved LAN IP addresses](#) on page 122.

### To specify a trusted computer:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Security > Block Sites**.  
The Block Sites page displays.
5. Scroll down and select the **Allow trusted IP address to visit blocked sites** check box.
6. In the **Trusted IP Address** field, enter the IP address of the trusted computer.
7. Click the **Apply** button.  
Your settings are saved.

## Block services from the Internet

You can block Internet services on your network based on the type of service. You can block the services all the time or based on a schedule.

### To block services:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Security > Block Services**.

The Block Services page displays.

5. Specify when to block the services:

- **Per Schedule:** To block the services based on a schedule, select the **Per Schedule** radio button. For information about how to set the schedule, see [Schedule when to block Internet sites and services](#) on page 68.
- **Always:** To block the services all the time, select the **Always** radio button.

6. Click the **Add** button.

The Block Services Setup page displays.

7. To add a service that is in the **Service Type** list, select the application or service. The settings for this service automatically display in the fields.

8. To add a service or application that is not the list, select **User Defined**.

- a. If you know that the application uses either TCP or UDP, select the appropriate protocol.

Otherwise, select **TCP/UDP (both)**.

- b. Enter the starting port and ending port numbers.

If the service uses a single port number, enter that number in both fields.

To find out which port numbers the service or application uses, you can contact the publisher of the application, ask user groups or newsgroups, or search on the Internet.

- c. In the **Service Type/User Defined** field, enter a name for the service.

9. To specify how to filter the services, select one of the following radio buttons:

- **Only This IP Address:** Block services for a single device.
- **IP Address Range:** Block services for a range of devices with consecutive IP addresses on your network.
- **All IP Addresses:** Block services for all devices on your network.

10. Click the **Add** button.

Your settings are saved. The Block Services page displays again and the added service displays in the table.

11. Click the **Apply** button.

Your settings are saved.

## Schedule when to block Internet sites and services

When you schedule blocking, the same schedule is used to block sites and to block services. For information about how to specify what you want the router to block, see [Block Internet sites by using keywords](#) on page 63 and [Block services from the Internet](#) on page 66.

### To schedule blocking:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Security > Schedule**.

The Schedule page displays.

5. Specify when to block keywords and services:

- **Days to Block:** Select the check box for each day that you want to block the keywords or select the Every Day check box, which automatically selects the check boxes for all days.
- **Time of Day to Block:** Select a start and end time in 24-hour format, or select All Day for 24-hour blocking.

6. Click the **Apply** button.

Your settings are saved.

## Email notifications for security events

The router can email you its logs of router activity. The log records router activity and security events such as attempts to access blocked sites or services.

### To set up email notifications:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Security > E-mail**.  
The E-mail page displays.
5. Select the **Turn E-mail Notification On** check box.
6. In the **Primary E-mail Address** field, enter the email address to which logs and alerts are sent.  
This email address is also used for the From address. If this field is blank, log and alert messages are not sent.
7. In the **Your Outgoing Mail Server** field, enter the name of your ISP outgoing (SMTP) mail server (such as mail.myISP.com).  
You might be able to find this information in the configuration window of your email program. If you leave this field blank, log and alert messages are not sent.
8. In the **Outgoing Mail Server Port Number** field, enter your mail server's port number.  
You might be able to find this information in the configuration window of your email program.

9. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box and do the following:
  - In the **User Name** field, type the user name for the outgoing email server.
  - In the **Password** field, type the password for the outgoing email server.
10. To send alerts immediately, select the **Send Alerts Immediately** check box.  
Email alerts are sent immediately when someone attempts to visit a blocked site.
11. To send logs based on a schedule, specify these settings:
  - From **Send logs according to this schedule** menu, select the schedule type.
  - From the **Day** menu, select the day.
  - From the **Time** menu, select the time, and select the **a.m.** or **p.m.** radio button.
12. Click the **Apply** button.  
Your settings are saved.  
  
Logs are sent automatically. If the log fills before the specified time, it is sent. After the log is sent, it is cleared from the router memory. If the router cannot email the log and the log buffer fills, the router overwrites the log.

# 5

## Manage the VLANs

---

This chapter includes the following sections:

- [About VLANs in general](#)
- [About VLANs on the router](#)
- [How the router organizes LANs, VLANs, and WLANs](#)
- [VLAN profiles](#)
- [VLAN membership for a LAN, WiFi network, or port](#)
- [Port mode: Trunk mode or Access mode](#)

**Note:** The router comes with a preset VLAN configuration that you can use without making any changes. If your network setup is simple, or does not require you to separate traffic into different VLANs, you might be able to use the preset VLAN configuration. We recommend that you read [How the router organizes LANs, VLANs, and WLANs](#) on page 73.

For information about how to use VLANs in your network, including examples of use cases, see [How to Use VLANs in Your Network](#) on page 215.

## About VLANs in general

A local area network (LAN) maps network devices together based on physical or geographic location. A *virtual* local area network (VLAN) maps network devices together on a basis *other* than physical or geographic location, for example, by department, type of user, level of security clearance, or primary application. Traffic flowing between VLANs must go through a router, such as an Orbi Pro router, just as if the VLANs were two separate LANs.

A VLAN groups computers, servers, and other network devices so that they behave as if they are all connected to the same network segment. For example, marketing personnel might work in different rooms in an office building, or even in an adjacent building, yet they can use the same marketing-only VLAN, allowing them to share resources and network bandwidth as if they were connected to the same LAN. The resources of other departments might be invisible to the users of the marketing VLAN, accessible to all, or accessible only to specified individuals, depending on how you configure the VLAN.

VLANs have a number of advantages:

- **Facilitate network segmentation:** Devices for users who communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's network traffic is contained largely within the VLAN, which reduces traffic that is not relevant to the group and improves the efficiency across the whole network.
- **Facilitate management:** Changes such as adding or moving network devices can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- **Provide increased performance:** VLANs free up bandwidth by limiting device-to-device and broadcast traffic throughout the network.
- **Ensure enhanced network security:** VLANs create virtual boundaries that can be traversed only through a router, allowing router-based security measures to be used to restrict access to each VLAN.

## About VLANs on the router

The router supports virtual local area network (VLAN) management. VLAN management enables you to limit user access by network and increase security through data separation. You can further increase security through client isolation and network isolation.

The following table shows the four preset VLAN profiles on the router.

Table 4. Preset VLAN profiles on the router

| VLAN ID | VLAN Profile Name |
|---------|-------------------|
| 1       | Default           |
| 20      | Employee          |
| 30      | IoT               |
| 40      | Guest             |

If you do not require specific VLAN configurations, we recommend that you keep the router's default VLAN configuration.

If your network environment does require you to use custom-configured VLANs, you can either change the VLANs on the router to match the VLANs that are already defined in your network, or define the router's preset VLANs on your other network components (for example, switches and access points). For more information, see [VLAN profiles](#) on page 74 and [VLAN membership for a LAN, WiFi network, or port](#) on page 80.

## How the router organizes LANs, VLANs, and WLANs

You do not need to use the VLANs in order to use the router and any satellites. However, if your network environment is not complex or does not require you to separate multiple types of traffic, you could just connect your wired devices to LAN 1 and your WiFi devices to the Wireless 1 network.

The router comes with four preset LANs, VLANs, and WLANs, as shown in the following table. A fifth LAN is disabled, but you can configure and enable it if your network environment requires an additional LAN.

With the preset modes, your administrative traffic, employee traffic, Internet of Things (IoT) traffic, and guest traffic can be separated entirely without the need to set up any other VLANs on the router.

Table 5. Default organization of the LANs, VLANs, and WLANs

| LAN ID  | Ethernet Ports *               | Preset VLAN ID | VLAN Profile Name | WLAN Name      | WLAN Usage      |
|---------|--------------------------------|----------------|-------------------|----------------|-----------------|
| LAN 1   | All LAN ports and the WAN port | 1              | Default           | Wireless 1     | admin access    |
| LAN 2   | None                           | 20             | Employee          | Wireless 2**   | Employee access |
| LAN 3   | None                           | 30             | IoT               | Wireless 3**   | IoT access      |
| LAN 4   | None                           | 40             | Guest             | Guest Portal** | Guest access    |
| LAN 5** | --                             | --             | --                | --             | --              |

\* LANs (networks) and LAN ports are two different concepts. By default, all LAN ports and the WAN port on the router, and all LAN ports on any connected satellites, are Ethernet ports in the same physical network segment (LAN 1), and members of VLAN 1. However, you can assign a LAN port to a different VLAN (see [Change the VLAN profile for an Ethernet port](#) on page 82).

\*\* Disabled by default, but you can enable it.

Except for LAN 1, you can change the VLAN profile assignments for the LANs (see [Change the VLAN profile for a LAN](#) on page 80). For more information about LANs in general, see [Manage the LANs](#) on page 107.

By default, VLAN 1 is enabled for the Wireless 1 network. For any other WLANs that you enable, you can change the VLAN profile assignments for the WLANs (see [Enable, change, or disable the VLAN profile for a WiFi network](#) on page 81). For information about the WLANs in general, see [Manage the WiFi Networks](#) on page 85.

## VLAN profiles

A VLAN profile consists of a VLAN ID, VLAN name, the client isolation settings, and the network isolation setting.

You can change the preset VLAN profiles, add custom VLAN profiles, and delete custom VLAN profiles.

### Add a new VLAN profile

You can add a new VLAN profile, which consists of a VLAN name, VLAN ID, the client isolation settings, and the network isolation setting.

If your router is part of a network with switches and access points, VLAN traffic segregation works only if the VLAN is defined on all other network components, excluding end devices such as computers and WiFi clients.

**Note:** If you want to add a new VLAN profile directly to a LAN on a LAN Setup page, see [Add a new VLAN profile directly to a LAN](#) on page 76.

**To add a new VLAN profile:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.  
The VLAN / Bridge Settings page displays.  
The existing VLAN profiles display in a table at the bottom of the page. If you added a VLAN profile directly to a LAN on a LAN Setup page, the VLAN profile also displays in the table.

5. Click the **ADD** button.  
A new row is added to added to the VLAN table.
6. Specify the VLAN settings (that is, the VLAN profile) as described in the following table.

| Field   | Description                 |
|---------|-----------------------------|
| Name    | Enter a name for the VLAN.  |
| VLAN ID | Enter an ID from 1 to 4094. |

(Continued)

| Field             | Description  |
|-------------------|--|
| Client Isolation  | Client isolation prevents hosts and clients in the VLAN from reaching ports, hosts, and clients in the <i>same</i> VLAN, thereby increasing security.<br>Select the check box to enable this option.   |
| Network Isolation | Network isolation, also referred to as network segmentation, prevents hosts and clients in the VLAN from reaching ports, hosts, and clients in <i>other</i> VLANs, thereby increasing security.<br>Select the check box to enable this option. |

- Click the **Apply** button.

Your settings are saved and the VLAN profile is added to the table.

You can now assign a LAN, WiFi network, port, or combination of these as members of the new VLAN. For more information, see [VLAN membership for a LAN, WiFi network, or port](#) on page 80.

## Add a new VLAN profile directly to a LAN

You can add a new VLAN profile directly to a LAN. A VLAN profile consists of a VLAN name, VLAN ID, the client isolation settings, and the network isolation setting.

If your router is part of a network with switches and access points, VLAN traffic segregation works only if the VLAN is defined on all other network components, excluding end devices such as computers and WiFi clients.

In the router web interface, you can add a new VLAN profile for LAN 2, LAN 3, LAN 4, and LAN 5 on the associated LAN page.

**Note:** If you want to add a new VLAN profile on the VLAN / Bridge Settings page, see [Add a new VLAN profile](#) on page 74. On the VLAN / Bridge Settings page, you can also manage the VLAN settings.

### To add a new VLAN profile directly to a LAN:

- Launch a web browser from a computer or mobile device that is connected to your Orbi network.
- Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.  
The LAN Setup page for LAN 1 displays.
5. Select the tab (**LAN 2, LAN 3, LAN 4, or LAN 5**) for the LAN for which you want to add a new VLAN profile.  
You cannot add a VLAN profile for LAN 1.  
The page for the selected LAN displays.
6. If you selected LAN 5 and this is the first time that you configure LAN 5, select the **Enable LAN Setup 5** check box.
7. From the **VLAN Profile** menu, select **New VLAN Profile+**.  
The VLAN Profile Management window displays.
8. Specify the VLAN settings (that is, the VLAN profile) as described in the following table.

| Field             | Description  |
|-------------------|--|
| Name              | Enter a name for the VLAN.   |
| VLAN ID           | Enter an ID from 1 to 4094.  |
| Client Isolation  | Client isolation prevents hosts and clients in the VLAN from reaching ports, hosts, and clients in the <i>same</i> VLAN, thereby increasing security.<br>Select the check box to enable this option.   |
| Network Isolation | Network isolation, also referred to as network segmentation, prevents hosts and clients in the VLAN from reaching ports, hosts, and clients in <i>other</i> VLANs, thereby increasing security.<br>Select the check box to enable this option. |

9. Click the **ADD** button.  
The VLAN profile is added.
10. To assign the new VLAN profile to the LAN, select it from **VLAN Profile** menu.
11. Click the **Apply** button.  
Your settings are saved.

You can now also assign a WiFi network, port, or combination of these as members of the new VLAN. For more information, see [VLAN membership for a LAN, WiFi network, or port](#) on page 80.

## Change the client isolation or network isolation for a VLAN profile

For a preset or custom VLAN, you cannot change the profile name or VLAN ID, but you can change the client isolation or network isolation settings.

**Note:** If you want to change the profile name or VLAN ID for an existing VLAN, create a new VLAN with the profile name or VLAN ID that you require (see [Add a new VLAN profile](#) on page 74), move the members of the existing VLAN to the new VLAN (see [VLAN membership for a LAN, WiFi network, or port](#) on page 80), and then delete the existing VLAN (see [Delete a VLAN profile](#) on page 79).

### To change the client isolation or network isolation settings for a VLAN profile:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.  
The VLAN / Bridge Settings page displays.
5. Select the radio button next to the VLAN.
6. To change the client isolation settings, select or clear the check box in the Client Isolation column.  
Selecting the check box enables client isolation, which prevents hosts and clients in the VLAN from reaching ports, hosts, and clients in the *same* VLAN, thereby increasing security.

7. To change the network isolation settings, select or clear the check box in the Network Isolation column.

Selecting the check box enables network isolation, also referred to as network segmentation, which prevents hosts and clients in the VLAN from reaching ports, hosts, and clients in *other* VLANs, thereby increasing security.

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

## Delete a VLAN profile

Note the following about deleting VLANs:

- You cannot delete a VLAN profile that still has a LAN, WLAN, or interface as a member. You can delete a VLAN only if no members are assigned to the VLAN.
- You cannot delete the preset VLAN 1 profile with the name Default. However, you if you want, you *can* delete one or more of the other preset VLAN profiles (VLAN 20, the Employee VLAN; VLAN 30, the IoT VLAN; or VLAN 40, the Guest VLAN), if no members are assigned to the VLAN.

### To delete a VLAN profile:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.  
The VLAN / Bridge Settings page displays.
5. Select the radio button next to the custom VLAN you want to delete.
6. Click the **DELETE** button.  
The VLAN profile is removed from the table.

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

## VLAN membership for a LAN, WiFi network, or port

By default, each LAN and each WiFi network is a member of a preset VLAN (see [How the router organizes LANs, VLANs, and WLANs](#) on page 73). By default, each port is a member of VLAN 1, the Default VLAN.

You can change the VLAN membership for a LAN, WiFi network, or port.

**CAUTION:** Be sure that you fully understand the consequences of changing a VLAN membership. Incorrect configuration might cause network problems, such as traffic being discarded.

### Change the VLAN profile for a LAN

You can change the VLAN profile for a LAN. Note the following:

- The VLAN profile for LAN 1 is set and you cannot change it.
- If a LAN is assigned to a VLAN profile, you cannot assign another LAN to the same VLAN profile.  
This also means that you cannot change the preset VLAN profile for LAN 2, LAN 3, and LAN 4 until you add a new VLAN profile (that is, a custom VLAN profile) and assign LAN 2, LAN 3, or LAN 4 to it. Doing so releases the preset VLAN profile so that you can assign a different LAN to it.
- If an Ethernet port and a LAN are assigned to same VLAN profile, you cannot change the VLAN profile for the LAN until you assign the Ethernet port to a different VLAN profile.

#### To change the VLAN profile for a LAN:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.  
The LAN Setup page for LAN 1 displays.
5. Select the tab (**LAN 2**, **LAN 3**, **LAN 4**, or **LAN 5**) for the LAN for which you want to change the VLAN profile.  
You cannot change the VLAN profile for LAN 1.  
The page for the selected LAN displays.
6. From the **VLAN Profile** menu, select another VLAN profile.  
You cannot change the preset VLAN profile for LAN 2, LAN 3, or LAN 4 until you add a new VLAN profile (that is, a custom VLAN profile) and assign LAN 2, LAN 3, or LAN 4 to it. Doing so releases the preset VLAN profile so that you can assign a different LAN to it.
7. Click the **Apply** button.  
Your settings are saved.

## Enable, change, or disable the VLAN profile for a WiFi network

By default, the VLANs are not enabled for any WiFi network, except for VLAN 40, which is enabled for the Guest Portal. (However, the Guest Portal itself is disabled by default.)

### To enable, change, or disable the VLAN profile for a WiFi network:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > Wireless Setup**.

The Advanced Wireless Settings page displays.

5. Select the tab (**Wireless 1**, **Wireless 2**, **Wireless 3**, or **Guest Portal**) for which you want to change the VLAN profile.

The page for the selected WiFi network displays.

6. Do one of the following:

- **Enable:** To enable the VLAN profile, select the **VLAN Profile** check box.
- **Change:** To change the VLAN profile, from the **VLAN Profile** menu, select another VLAN profile.
- **Disable:** To disable the VLAN profile, clear the **VLAN Profile** check box.

7. Click the **Apply** button.

Your settings are saved.

## Change the VLAN profile for an Ethernet port

By default, all Ethernet ports (that is, the WAN port and the LAN ports) are assigned to the Default VLAN profile, VLAN 1. In most situations, you do not need to change these assignments. However, if your network environment or router setup requires you to change an assignment, you *can* do so.

Note the following:

- If two LAN ports form a link aggregation group (LAG), they must be assigned to the same VLAN profile.
- You can assign the WAN port to any VLAN profile.

### **To assign a port to another VLAN profile on the router (also referred to as the Base in this context) or satellite:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.

The VLAN / Bridge Settings page displays.

For the router (Base) and each satellite, the ports display on the page:

- **Blue:** The ports are connected to devices that are turned on.
- **Gray:** The ports are either not connected or are connected to devices that are not turned on.

5. In either the Base (router) or Satellite section, for the Ethernet port that you want to change, select a VLAN profile from the **VLAN Profile** menu.

6. Click the **Apply** button.

Your settings are saved.

## Port mode: Trunk mode or Access mode

By default, all Ethernet ports (the WAN port and the LAN ports) on the router and any satellites function in Trunk mode, but they can also function in Access mode:

- **Trunk mode.** If a port must forward tagged packets with a specific VLAN tag only, assign Trunk mode to the port, add a VLAN profile with the VLAN tag (that is, the VLAN ID; see [Add a new VLAN profile](#) on page 74), and assign the port to the new VLAN profile. Packets that include tags other than the specific VLAN tag are dropped by the port.
- **Access mode.** If a port connects *only* to a client or end device, you can assign Access mode to the port.

By default, all Ethernet ports are assigned to the Default VLAN profile and function in Trunk mode. However, for any port that is assigned to the Default VLAN profile, no real difference exists between Trunk mode and Access mode. You can connect a modem, gateway, client device, or end device to such a port. That is, for a port that is assigned

to the Default VLAN profile, Trunk mode actually functions in a *hybrid mode* in that it allows both tagged and untagged traffic:

- If a port receives untagged traffic (that is, without a VLAN tag), the port forwards the traffic to the LAN and the WLAN.
- If a port receives tagged traffic (that is, *with* a VLAN tag), the port forwards the traffic to other ports that function in Trunk mode and that are assigned to the same VLAN profile (by default, the Default VLAN profile with VLAN ID 1).

**To change a port mode to Trunk mode or Access mode on the router (also referred to as the Base in this context) or satellite:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.  
The VLAN / Bridge Settings page displays.  
For the router (Base) and each satellite, the ports display on the page:
  - **Blue**: The ports are connected to devices that are turned on.
  - **Gray**: The ports are either not connected or are connected to devices that are not turned on.
5. In either the Base (router) or Satellite section, for the Ethernet port that you want to change, select **Access** or **Trunk** from the **Mode** menu.
6. Click the **Apply** button.  
Your settings are saved.

# 6

## Manage the WiFi Networks

---

This chapter includes the following sections:

- [About the WiFi networks](#)
- [admin \(default\) WiFi network](#)
- [Employee WiFi network](#)
- [Internet of things WiFi network](#)
- [Guest WiFi network and captive portal](#)

For information about advanced WiFi features, see [Manage the Advanced WiFi Settings](#) on page 173.

**IMPORTANT:** When you log in to the router and change the WiFi settings, the router automatically sends the new settings to any connected satellites.

## About the WiFi networks

The router supports four WiFi networks, also referred to as WiFi local area networks (WLANs) or wireless networks. These WiFi networks can operate simultaneously, but by default, only the Wireless 1 network is operationally enabled. To use another WiFi network, you must first enable it.

Each WiFi network has an intended usage and is preset to a VLAN profile, as described in the following table. (For more information about VLANs, see [About VLANs on the router](#) on page 72.)

Table 6. WiFi network default settings

| Feature                               | Wireless 1                        | Wireless 2                                    | Wireless 3                                    | Guest Portal   |
|---------------------------------------|-----------------------------------|---|---|--|
| Default operational status            | Enabled                           | Disabled                                      | Disabled                                      | Disabled   |
| Intended WiFi network usage           | Administrative and general access | Employee access                               | IoT access                                    | Guest access   |
| Preset VLAN ID and VLAN profile name  | VLAN 1<br>Default                 | VLAN 20<br>Employee                           | VLAN 30<br>IoT                                | VLAN 40<br>Guest   |
| WiFi network name (SSID)              | See router label for default SSID | Default SSID appended with -2                 | Default SSID appended with -3                 | Default SSID appended with -GUEST                            |
| Default authentication and encryption | WPA2-PSK [AES]                    | WPA2-PSK [AES]                                | WPA2-PSK [AES]                                | None (open)  |
| Default WiFi password (network key)   | See router label                  | See the Wireless Settings page for Wireless 2 | See the Wireless Settings page for Wireless 3 | None   |
| Default authentication mode           | Local                             | Local   | Local   | Local<br>Other options are captive portal and Facebook Wi-Fi |
| SSID broadcast                        | Enabled, non-configurable         | Enabled, configurable                         | Enabled, configurable                         | Enabled, configurable  |
| SSID separation for 2.4GHz and 5 GHz  | Disabled, non-configurable        | Disabled, configurable                        | Disabled, configurable                        | Disabled, non-configurable                                   |

You can configure the settings and security for each of these four WiFi networks, as described in this chapter.

# admin (default) WiFi network

Your Orbi Pro WiFi 6 router and satellite come preset with the same admin WiFi network name (SSID) and WiFi network key (password). You can find the admin SSID and password on the router label and on the satellite label. The preset WiFi settings on the labels are for your admin WiFi network that you can use to manage and monitor your router, satellite, and network. The admin WiFi network is the default WiFi network.

The router web interface calls the admin WiFi network the Wireless 1 network.

## Change the admin WiFi network name, channel, or VLAN

If you change your WiFi settings, make a note of the new settings and store it in a safe place where you can easily find it.

If your computer or mobile device is using a WiFi connection when you change the network name (SSID) or other WiFi security settings, you are disconnected when you click the **Apply** button. To avoid this problem, use a computer with a wired connection to access the router.

The router web interface calls the admin WiFi network the Wireless 1 network.

### To change the admin WiFi settings:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Wireless**.  
The Wireless settings for the Wireless 1 network display on the page.
5. To change the admin network name (SSID), type a new name in the **Name (SSID)** field.  
The name can be up to 32 characters long and it is case-sensitive. If you did not change the SSID during the setup process, the default SSID is shown. (The default

SSID is randomly generated and is on the router label.) If you change the name, make sure to write down the new name and keep it in a safe place.

6. To change a 2.4 GHz or 5 GHz WiFi channel, select a channel from the **Channel** menu.

The channels that are available depend on your country or region. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which channel works best for your.

When you use multiple WiFi routers, access points, WiFi gateways, satellites, and extenders in your network, you experience less interference if adjacent devices use different channels. For example, for the 2.4 GHz radio band, we recommend a channel spacing with a minimum of four channels between adjacent devices (for example, use channels 1 and 5, or 6 and 10).

7. Although the preset Default VLAN profile for the Wireless 1 network works well for most situations, if you want to change the VLAN profile, select the **VLAN Profile** check box, and select another VLAN profile from the menu.

The preset VLAN profile name is Default, the VLAN has ID 1, and the combination is shown in the menu as Default(1).

For more information about VLANs, see [Manage the VLANs](#) on page 71, including [How the router organizes LANs, VLANs, and WLANs](#) on page 73.

8. Click the **Apply** button.

Your settings are saved. The router sends the new settings to the satellite.

If you are using a WiFi connection and you changed the SSID, you are disconnected from the network.

9. Make sure that you can connect to the WiFi network with its new settings.

If you cannot connect using WiFi, check the following:

- Is your WiFi-enabled computer or mobile device connected to another WiFi network in your area? Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
- Is your computer or WiFi device trying to connect to your network with its old settings (before you changed the settings)? If so, update the WiFi network selection in your computer or WiFi device to match the current settings for your network.

## Change the admin WiFi password or security level

You can change the admin password and security level (authentication and encryption settings). The router supports Wi-Fi Protected Access 3 (WPA3), WPA2, and mixed WPA + WPA2, including enterprise level WPA3 and enterprise level WPA2.

**CAUTION:** We recommend that you do not disable security for your admin WiFi network.

The router web interface calls the admin WiFi network the Wireless 1 network.

### To change the admin WiFi password or security level:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **Wireless**.

The Wireless settings for the Wireless 1 network display on the page.

5. Under Security Options, select a WiFi security option:

- **WPA2-PSK [AES]:** The WPA2 option uses AES encryption. This type of security allows only WiFi devices that support WPA2 or WPA3 to join the network. When you select this option, the **Password (Network Key)** field displays. Do the following:
  - a. In the **Password (Network Key)** field, enter the network key (password) that you want to use.  
It is a text string from 8 to 63 characters.
  - b. Write down the new password and keep it in a secure place for future reference.
- **WPA-PSK [TKIP] + WPA2-PSK [AES]:** If your network includes legacy devices (devices that support only WPA), select this radio button. This option, which uses AES and TKIP encryption, allows WiFi devices that support WPA, WPA2, or WPA3 to join the network.

When you select this option, the **Password (Network Key)** field displays. Do the following:

- a. In the **Password (Network Key)** field, enter the network key (password) that you want to use.  
It is a text string from 8 to 63 characters.
- b. Write down the new password and keep it in a secure place for future reference.

- **WPA2 Enterprise:** If your network is connected to a RADIUS server that can provide authentication and your network includes WPA2 and WPA3 devices, select this radio button. WPA2 Enterprise can provide a high level of security and allows WPA2 and WPA3 devices to connect to the network. (WPA devices cannot connect.) Before a WiFi client can connect to the network, the WiFi client must be configured on the RADIUS server and authenticated against the RADIUS server. The router functions as the authenticator between the WiFi client and the RADIUS server, which provides the actual authentication.

When you select this option, additional fields display so that you can specify the RADIUS server. Do the following:

- a. In the **IP address** field, enter the IP address of the RADIUS server to which the router must connect.
- b. In the **Port** field, enter the port number that the router must use to communicate with the RADIUS server.  
By default, the port number is 1812.
- c. In the **Shared Secret** field, enter the password that the router must use to communicate with the RADIUS server.  
This password must be configured on the RADIUS server. This password is used to authenticate the router (not a WiFi client) against the RADIUS server.

- **WPA3-Personal [SAE]:** This is the most secure personal authentication option. WPA3 uses SAE encryption and allows only WiFi devices that support WPA3 to connect to the network. WiFi devices that support WPA or WPA2 cannot connect to the network.

When you select this option, additional fields display so that you can add a key. Do the following:

- a. In the **Password (Network Key)** field, enter the network key (password) that you want to use.  
It is a text string from 8 to 127 characters.
- b. Write down the new password and keep it in a secure place for future reference.

- **WPA3 Enterprise:** If your network is connected to a RADIUS server that can provide authentication and your network includes WPA3 devices only, select this radio button. WPA3 Enterprise can provide the highest level of security but WPA and WPA2 devices cannot connect. Before a WiFi client can connect to the network, the WiFi client must be configured on the RADIUS server and authenticated against the RADIUS server. The router functions as the authenticator between the WiFi client and the RADIUS server, which provides the actual authentication.

When you select this option, additional fields display so that you can specify the RADIUS server. Do the following:

- a. In the **IP address** field, enter the IP address of the RADIUS server to which the router must connect.
- b. In the **Port** field, enter the port number that the router must use to communicate with the RADIUS server.  
By default, the port number is 1812.
- c. In the **Shared Secret** field, enter the password that the router must use to communicate with the RADIUS server.  
This password must be configured on the RADIUS server. This password is used to authenticate the router (not a WiFi client) against the RADIUS server.

6. Click the **Apply** button.

Your settings are saved.

## Employee WiFi network

When employee devices connect to the employee WiFi network, they cannot see other devices that are connected to the network and cannot access the local area network (LAN).

The router web interface calls the employee WiFi network the Wireless 2 network.

### Enable the employee WiFi network and manage the settings

Before you can set up the employee WiFi network, you must enable it. You must be connected to the admin network to enable the employee WiFi network and change the settings.

The router web interface calls the employee WiFi network the Wireless 2 network.

### To enable the employee WiFi network and manage the WiFi settings:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Wireless > Wireless 2**.  
The WiFi settings for the Wireless 2 network display on the page.
5. To enable the Wireless 2 network, select the **Enable Wireless 2 network** check box.  
By default, the Wireless 2 network is disabled.
6. To broadcast the Wireless 2 network SSID, select the **Enable SSID Broadcast** check box.  
By default, the broadcast is enabled.
7. To separate the single SSID for the Wireless 2 network in an SSID for the 2.4 GHz band and another SSID for the 5 GHz band, select the **Enable SSID separation for 2.4G/5GHz** check box.  
For each band, a Wireless 2 Network Name (SSID) field displays. The SSID for the 5 GHz band is appended with **\_5G**, but you can also type another name.  
By default, the Wireless 2 network provides a single SSID for both bands.
8. To change the Wireless 2 network name (SSID), type a new name in the **Wireless 2 Network Name (SSID)** field.  
The name can be up to 32 characters long and it is case-sensitive. The default SSID is derived from the randomly generated SSID that is on the router's label. If you change the name, make sure to write down the new name and keep it in a safe place.
9. Although the preset Employee VLAN profile for the Wireless 2 network works well for most situations, if you want to change the VLAN profile, select the **VLAN Profile** check box, and select another VLAN profile from the menu.  
The preset VLAN profile name is Employee, the VLAN has ID 20, and the combination is shown in the menu as Employee(20).

For more information about VLANs, see [Manage the VLANs](#) on page 71, including [How the router organizes LANs, VLANs, and WLANs](#) on page 73.

10. Click the **Apply** button.

Your settings are saved. The router sends the new settings to the satellite.

11. Make sure that a user can connect to the WiFi network with its new settings.

If you cannot connect using WiFi, check the following:

- Is your WiFi-enabled computer or mobile device connected to another WiFi network in your area? Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
- Is your computer or mobile device trying to connect to your network with its old settings (before you changed the settings)? If so, update the WiFi network selection in your computer or WiFi device to match the current settings for your network.

## Change the employee WiFi password or security level

You must be connected to the admin network to change the employee password and security level (authentication and encryption settings). The router supports Wi-Fi Protected Access 3 (WPA3), WPA2, and mixed WPA + WPA2, including enterprise level WPA3 and enterprise level WPA2.

The router web interface calls the employee WiFi network the Wireless 2 network.

### **To change the employee WiFi network password or security level:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **Wireless > Wireless 2**.

The WiFi settings for the wireless 2 network display on the page.

5. Under Security Options, select a WiFi security option:

- **WPA2-PSK [AES]:** The WPA2 option uses AES encryption. This type of security allows only WiFi devices that support WPA2 or WPA3 to join the network. When you select this option, the **Password (Network Key)** field displays. Do the following:
  - a. In the **Password (Network Key)** field, enter the network key (password) that you want to use.  
It is a text string from 8 to 63 characters.
  - b. Write down the new password and keep it in a secure place for future reference.
  
- **WPA-PSK [TKIP] + WPA2-PSK [AES]:** If your network includes legacy devices (devices that support only WPA), select this radio button. This option, which uses AES and TKIP encryption, allows WiFi devices that support WPA, WPA2, or WPA3 to join the network. When you select this option, the **Password (Network Key)** field displays. Do the following:
  - a. In the **Password (Network Key)** field, enter the network key (password) that you want to use.  
It is a text string from 8 to 63 characters.
  - b. Write down the new password and keep it in a secure place for future reference.
  
- **WPA2 Enterprise:** If your network is connected to a RADIUS server that can provide authentication and your network includes WPA2 and WPA3 devices, select this radio button. WPA2 Enterprise can provide a high level of security and allows WPA2 and WPA3 devices to connect to the network. (WPA devices cannot connect.) Before a WiFi client can connect to the network, the WiFi client must be configured on the RADIUS server and authenticated against the RADIUS server. The router functions as the authenticator between the WiFi client and the RADIUS server, which provides the actual authentication. When you select this option, additional fields display so that you can specify the RADIUS server. Do the following:
  - a. In the **IP address** field, enter the IP address of the RADIUS server to which the router must connect.
  - b. In the **Port** field, enter the port number that the router must use to communicate with the RADIUS server.  
By default, the port number is 1812.
  - c. In the **Shared Secret** field, enter the password that the router must use to communicate with the RADIUS server.

This password must be configured on the RADIUS server. This password is used to authenticate the router (not a WiFi client) against the RADIUS server.

- **WPA3-Personal [SAE]:** This is the most secure personal authentication option. WPA3 uses SAE encryption and allows only WiFi devices that support WPA3 to connect to the network. WiFi devices that support WPA or WPA2 cannot connect to the network.

When you select this option, additional fields display so that you can add a key. Do the following:

- a. In the **Password (Network Key)** field, enter the network key (password) that you want to use.  
It is a text string from 8 to 127 characters.
- b. Write down the new password and keep it in a secure place for future reference.

- **WPA3 Enterprise:** If your network is connected to a RADIUS server that can provide authentication and your network includes WPA3 devices only, select this radio button. WPA3 Enterprise can provide the highest level of security but WPA and WPA2 devices cannot connect. Before a WiFi client can connect to the network, the WiFi client must be configured on the RADIUS server and authenticated against the RADIUS server. The router functions as the authenticator between the WiFi client and the RADIUS server, which provides the actual authentication.

When you select this option, additional fields display so that you can specify the RADIUS server. Do the following:

- a. In the **IP address** field, enter the IP address of the RADIUS server to which the router must connect.
- b. In the **Port** field, enter the port number that the router must use to communicate with the RADIUS server.  
By default, the port number is 1812.
- c. In the **Shared Secret** field, enter the password that the router must use to communicate with the RADIUS server.  
This password must be configured on the RADIUS server. This password is used to authenticate the router (not a WiFi client) against the RADIUS server.

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

# Internet of things WiFi network

The Internet of things (IoT) network is intended for WiFi-enabled smart devices that can range from light bulbs to appliances to inventory trackers. The possibilities for smart devices are endless.

When you connect IoT devices to the IoT WiFi network, the devices cannot detect other devices that are connected to the network and cannot access the local area network (LAN).

The router web interface calls the IoT WiFi network the Wireless 3 network.

## Enable the IoT WiFi network and manage the settings

Before you can set up the Internet of things (IoT) WiFi network, you must enable it. You must be connected to the admin network to enable the IoT WiFi network and change the settings.

The router web interface calls the IoT WiFi network the Wireless 3 network.

### **To enable the IoT WiFi network and manage the WiFi settings:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Wireless > Wireless 3**.  
The WiFi settings for the Wireless 3 network display on the page.
5. To enable the Wireless 3 network, select the **Enable Wireless 3 network** check box.  
By default, the Wireless 3 network is disabled.
6. To broadcast the Wireless 3 network SSID, select the **Enable SSID Broadcast** check box.  
By default, the broadcast is enabled.

7. To separate the single SSID for the Wireless 3 network in an SSID for the 2.4 GHz band and another SSID for the 5 GHz band, select the **Enable SSID separation for 2.4G/5GHz** check box.

For each band, a Wireless 3 Network Name (SSID) field displays. The SSID for the 5 GHz band is appended with \_5G, but you can also type another name.

By default, the Wireless 3 network provides a single SSID for both bands.

8. To change the Wireless 3 network name (SSID), type a new name in the **Wireless 3 Network Name (SSID)** field.

The name can be up to 32 characters long and it is case-sensitive. The default SSID is derived from the randomly generated SSID that is on the router's label . If you change the name, make sure to write down the new name and keep it in a safe place.

9. Although the preset IoT VLAN profile for the Wireless 3 network works well for most situations, if you want to change the VLAN profile, select the **VLAN Profile** check box, and select another VLAN profile from the menu.

The preset VLAN profile name is IoT, the VLAN has ID 30, and the combination is shown in the menu as IoT(30).

For more information about VLANs, see [Manage the VLANs](#) on page 71, including [How the router organizes LANs, VLANs, and WLANs](#) on page 73.

10. Click the **Apply** button.

Your settings are saved. The router sends the new settings to the satellite.

11. Make sure that an IoT device can connect to the WiFi network with its new settings.

If you cannot connect using WiFi, check the following:

- Is your WiFi-enabled computer or mobile device connected to another WiFi network in your area? Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
- Is your computer or mobile device trying to connect to your network with its old settings (before you changed the settings)? If so, update the WiFi network selection in your computer or WiFi device to match the current settings for your network.

## Change the IoT WiFi password or security level

You must be connected to the admin network to change the IoT password and security level (authentication and encryption settings). The router supports Wi-Fi Protected Access 3 (WPA3), WPA2, and mixed WPA + WPA2, including enterprise level WPA3 and enterprise level WPA2.

The router web interface calls the IoT WiFi network the Wireless 3 network.

**To change the IoT WiFi network password or or security level:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **Wireless > Wireless 3**.

The WiFi settings for the wireless 3 network display on the page.

5. Under Security Options, select a WiFi security option:

- **WPA2-PSK [AES]:** The WPA2 option uses AES encryption. This type of security allows only WiFi devices that support WPA2 or WPA3 to join the network. When you select this option, the **Password (Network Key)** field displays. Do the following:

- a. In the **Password (Network Key)** field, enter the network key (password) that you want to use.  
It is a text string from 8 to 63 characters.
- b. Write down the new password and keep it in a secure place for future reference.

- **WPA-PSK [TKIP] + WPA2-PSK [AES]:** If your network includes legacy devices (devices that support only WPA), select this radio button. This option, which uses AES and TKIP encryption, allows WiFi devices that support WPA, WPA2, or WPA3 to join the network.

When you select this option, the **Password (Network Key)** field displays. Do the following:

- a. In the **Password (Network Key)** field, enter the network key (password) that you want to use.  
It is a text string from 8 to 63 characters.
- b. Write down the new password and keep it in a secure place for future reference.

- **WPA2 Enterprise:** If your network is connected to a RADIUS server that can provide authentication and your network includes WPA2 and WPA3 devices, select this radio button. WPA2 Enterprise can provide a high level of security and allows WPA2 and WPA3 devices to connect to the network. (WPA devices cannot connect.) Before a WiFi client can connect to the network, the WiFi client must be configured on the RADIUS server and authenticated against the RADIUS server. The router functions as the authenticator between the WiFi client and the RADIUS server, which provides the actual authentication. When you select this option, additional fields display so that you can specify the RADIUS server. Do the following:
  - a. In the **IP address** field, enter the IP address of the RADIUS server to which the router must connect.
  - b. In the **Port** field, enter the port number that the router must use to communicate with the RADIUS server. By default, the port number is 1812.
  - c. In the **Shared Secret** field, enter the password that the router must use to communicate with the RADIUS server. This password must be configured on the RADIUS server. This password is used to authenticate the router (not a WiFi client) against the RADIUS server.
  
- **WPA3-Personal [SAE]:** This is the most secure personal authentication option. WPA3 uses SAE encryption and allows only WiFi devices that support WPA3 to connect to the network. WiFi devices that support WPA or WPA2 cannot connect to the network. When you select this option, additional fields display so that you can add a key. Do the following:
  - a. In the **Password (Network Key)** field, enter the network key (password) that you want to use. It is a text string from 8 to 127 characters.
  - b. Write down the new password and keep it in a secure place for future reference.
  
- **WPA3 Enterprise:** If your network is connected to a RADIUS server that can provide authentication and your network includes WPA3 devices only, select this radio button. WPA3 Enterprise can provide the highest level of security but WPA and WPA2 devices cannot connect. Before a WiFi client can connect to the network, the WiFi client must be configured on the RADIUS server and authenticated against the RADIUS server. The router functions as the authenticator between the WiFi client and the RADIUS server, which provides the actual authentication.

When you select this option, additional fields display so that you can specify the RADIUS server. Do the following:

- a. In the **IP address** field, enter the IP address of the RADIUS server to which the router must connect.
- b. In the **Port** field, enter the port number that the router must use to communicate with the RADIUS server.  
By default, the port number is 1812.
- c. In the **Shared Secret** field, enter the password that the router must use to communicate with the RADIUS server.  
This password must be configured on the RADIUS server. This password is used to authenticate the router (not a WiFi client) against the RADIUS server.

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

## Guest WiFi network and captive portal

You can set up a guest WiFi network (guest portal), which allows visitors to access the Internet using a dedicated SSID. You can also set up a captive portal for the guest portal. With a captive portal, when visitors connect to the guest portal and open a browser to access the Internet, they are redirected to a splash page where they must agree to the Terms of Conditions before they can access Internet.

By default, visitors do not need to enter a password to connect to the guest portal and data is not encrypted. Open access without security might be a good option for a coffee shop. For situations in which authentication is required, you can use Facebook Wi-Fi or set a password.

When visitors use the guest portal, they cannot see other devices that are connected to the guest portal (or any other WiFi network on the router) and they cannot access the local area network (LAN).

The router web interface calls the guest WiFi network the Guest Portal network.

## Set up a guest WiFi network with open access or password authentication

The router web interface calls the guest WiFi network the Guest Portal network.

### To set up a guest WiFi network with open access or local password authentication:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Wireless > Guest Portal**.  
The WiFi settings for guest access display on the page.
5. To enable the guest portal, select the **Enable Guest Portal Network** check box.  
By default, the guest portal is disabled.
6. Leave the **Enable SSID Broadcast** check box selected.  
Allowing the router to broadcast its WiFi network name (SSID) makes it easier to find your network and connect to it. If you clear this check box, that creates a hidden network.
7. To change the network name, type a new name in the **Guest Portal Network Name (SSID)** field.  
The name can be up to 32 characters long and it is case-sensitive. The default SSID is the randomly generated SSID that is on the router's label, but appended with -GUEST. If you change the name, make sure to write down the new name and keep it in a safe place.
8. Although the preset Guest VLAN profile for the Guest Portal WiFi network works well for most situations, if you want to change the VLAN profile, select the **VLAN Profile** check box, and select another VLAN profile from the menu.  
The preset VLAN profile name is Guest, the VLAN has ID 40, and the combination is shown in the menu as Guest(40).

For more information about VLANs, see [Manage the VLANs](#) on page 71, including [How the router organizes LANs, VLANs, and WLANs](#) on page 73.

9. Scroll down to the Authentication Mode section and make sure that the **Local** radio button is selected.
10. In the Authentication Options section, either specify an open network or set an authentication password by doing one of the following:
  - **None:** To specify an open network without authentication, select the **None** radio button.
  - **Password Authentication:** To set an authentication password, select the **Password Authentication** radio button and specify a password in the field. The password must be a minimum of 8 characters and can be a maximum of 63 characters (or 64 hexadecimal digits).

**Note:** In order for guests to access the Internet through the Orbi Pro network, they must enter this password in the guest portal.
11. To set an expiration time for how long guests can access the Internet, select a time from the **Expiration** menu. After guests are authenticated, they can access the Internet for that period of time.

If you select Never from the menu, guest access time is not restricted to any period.
12. Click the **Apply** button.

Your settings are saved. The router sends the new settings to the satellite.

## Set up Facebook Wi-Fi for the guest WiFi network

You can set up Facebook Wi-Fi on your Orbi WiFi network to offer your customers free WiFi access if they check in to your existing Facebook business page.

**Note:** If a user attempts to access a website over HTTP (by default, over port 80), the user is directed to the Facebook Login page. If a user attempts to access a secure website over HTTPS (by default, over port 443), a Security Warning window opens in their web browser. The user must click the **Allow** button on the Security Warning window to see the Facebook Login page.

The router web interface calls the guest WiFi network the Guest Portal network.

### To set up Facebook Wi-Fi for the guest WiFi network:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Wireless > Guest Portal**.  
The WiFi settings for guest access display on the page.
5. Select the **Enable Guest Portal Network** check box.
6. Select the **Enable SSID Broadcast** check box.  
By default, this check box is selected. Allowing the router to broadcast its WiFi network name (SSID) makes it easier to find your network and connect to it. If you clear this check box, that creates a hidden network.
7. To change the network name, type a new name in the **Guest Portal Network Name (SSID)** field.  
The name can be up to 32 characters long and it is case-sensitive. If you change the name, make sure to write down the new name and keep it in a safe place.
8. Although the preset Guest VLAN profile for the Guest Portal WiFi network works well for most situations, if you want to change the VLAN profile, select the **VLAN Profile** check box, and select another VLAN profile from the menu.  
The preset VLAN profile name is Guest, the VLAN has ID 40, and the combination is shown in the menu as Guest(40).  
For more information about VLANs, see [Manage the VLANs](#) on page 71, including [How the router organizes LANs, VLANs, and WLANs](#) on page 73.
9. In the **Authentication Mode** section, select the **Facebook Wi-Fi** radio button.  
The page adjust and displays the **Add Page** button, which is masked out until you click the **Apply** button.
10. Click the **Apply** button.

Your settings are saved.

11. Click the **Add Page** button.

The Facebook Wi-Fi settings page displays.

12. On the Facebook Wi-Fi settings page, do the following:

a. Click the **Connect** button.

The Facebook Page menu displays.

b. From the **Facebook Page** menu, select an existing Facebook business page.

You must be an admin for the page, and the page must be associated with a valid address.

c. To allow users to skip checking in to Facebook, click the **Skip check-in** icon.

As an option, you can require users to enter a WiFi code before they can gain WiFi access. You can set the WiFi code. If you enable this option, users can skip checking in to Facebook, but they must enter the WiFi code.

d. To select the period after which users are automatically logged out, click the **Session length** icon, and select a period.

e. To add terms of service to the Facebook check-in page, select the option to add terms of service and type or copy your terms of service.

f. Click the **Save Settings** button.

The Facebook Wi-Fi settings are saved.

The name of the selected Facebook business page displays in the Facebook Page field in the router web interface along with the **Change Page** button, which lets you replace the selected Facebook business page with another one.

g. Return to the Guest Portal page in the router web interface.

13. On the page with the WiFi settings for guest access, click the **Apply** button.

Your settings are saved.

## Set up a guest WiFi network with a captive portal

A captive portal is an entry to a guest network that requires guests to view a splash page and agree to terms and conditions before using the network. When you use a captive portal on the router, guests cannot see other devices that are connected and they cannot access the local area network (LAN).

The router web interface calls the guest WiFi network the Guest Portal network.

### To set up a guest WiFi network with a captive portal:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Wireless > Guest Portal**.  
The WiFi settings for guest access display on the page.
5. Select the **Enable Guest Portal Network** check box.
6. Leave the **Enable SSID Broadcast** check box selected.  
Allowing the router to broadcast its WiFi network name (SSID) makes it easier to find your network and connect to it. If you clear this check box, that creates a hidden network.
7. To change the network name, type a new name in the **Guest Portal Network Name (SSID)** field.  
The name can be up to 32 characters long and it is case-sensitive. The default SSID is the randomly generated SSID that is on the router's label, but appended with -GUEST. If you change the name, make sure to write down the new name and keep it in a safe place.
8. Although the preset Guest VLAN profile for the Guest Portal WiFi network works well for most situations, if you want to change the VLAN profile, select the **VLAN Profile** check box, and select another VLAN profile from the menu.  
The preset VLAN profile name is Guest, the VLAN has ID 40, and the combination is shown in the menu as Guest(40).  
For more information about VLANs, see [Manage the VLANs](#) on page 71, including [How the router organizes LANs, VLANs, and WLANs](#) on page 73.
9. Scroll down to the Authentication Mode section and make sure that the **Local** radio button is selected.

10. In the Authentication Options section, set a guest portal password by selecting the **Password Authentication** radio button and entering a password in the field.

The password must be a minimum of 8 characters and can be a maximum of 63 characters (or 64 hexadecimal digits).

**Note:** In order for guests to access the Internet, they must enter this password in the guest portal and click the **AGREE** button to accept terms and conditions.

11. To set an expiration time for how long users can access the Internet, select a time from the **Expiration** menu.

After guests are authenticated, they can access the Internet for that period of time. After the period expires, guests are redirected to the Terms and Conditions page.

12. In the Portal Customization section, configure the following settings:

- To include a custom Terms and Conditions page, do the following: .
  - a. On the Terms and Conditions subsection, click the **Browse** button.
  - b. Locate and select the terms and conditions file on your computer.  
The file must be a `.txt` file, encoded in UTF8 format, and can be up to 1 MB.
- To include a custom logo file, do the following:
  - a. In the Logo subsection, click the **Browse** button.
  - b. Locate and select the logo file on your computer.  
The file must be a `.jpg`, `.jpeg`, `.gif`, or `.png` file. The file size can be up to 10 MB and the dimensions must be 200 x 200 pixels.

13. To preview the guest portal, click the **Preview** button.

To preview the Terms and Conditions page, either the terms and conditions and logo files must both be set to Default or you must upload new files for both. You cannot preview the Terms and Conditions page if one file is set to Default.

14. To set up a redirect URL, select the **URL** radio button and enter the URL for the page to which you want to redirect guests to in the field.

After guests agree to the terms and conditions, they are redirected to this page.

15. Click the **Apply** button.

Your settings are saved.

# 7

## Manage the LANs

---

This chapter includes the following sections:

- [About the LANs](#)
- [LAN settings](#)
- [DHCP servers](#)
- [Reserved LAN IP addresses](#)

## About the LANs

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end devices. Endpoints can communicate with each other without the need for a router such as an Orbi Pro router. Routers connect LANs together, routing the traffic to the appropriate port.

The router supports five local area networks (LANs): LAN 1 through LAN 5, each of which functions with a different default IP address and supports a different DHCP IP address range.

Each LAN is preset to a VLAN profile. For many network environments, the preset LAN configurations on the router work fine. If your network requires different settings, you *can* change the LAN settings on the router.

**Note:** LANs (networks) and LAN *ports* are two different concepts. By default, all LAN ports and the WAN port on the router and all LAN ports on any connected satellites are Ethernet ports in the same physical network segment (LAN 1) and members of VLAN 1. However, you can assign a LAN port to a different VLAN (see [Change the VLAN profile for an Ethernet port](#) on page 82).

Table 7. LANs and their associated IP addresses and VLANs

| LAN Name | Default LAN IP Address | DHCP IP Address Range         | Preset VLAN ID | VLAN Profile Name |
|----------|------------------------|-------------------------------|----------------|-------------------|
| LAN 1    | 192.168.1.1            | 192.168.1.2 - 192.168.1.254   | 1              | Default           |
| LAN 2    | 192.168.20.1           | 192.168.20.2 - 192.168.20.254 | 20             | Employee          |
| LAN 3    | 192.168.30.1           | 192.168.30.2 - 192.168.30.254 | 30             | IoT               |
| LAN 4    | 192.168.40.1           | 192.168.40.1 - 192.168.40.254 | 40             | Guest             |
| LAN 5*   | --                     | --                            | --             | --                |

\* Disabled by default, but you can enable it.

For more information about VLANs, see [Manage the VLANs](#) on page 71.

# LAN settings

Although the default LAN settings work well for most situations, you *can* change the settings for each of the five LANs on the router.

## Change the default LAN 1 settings

LAN 1 is the default LAN that is assigned to the default VLAN profile with the name Default and ID 1. You cannot change the VLAN profile for LAN 1.

By default, the router uses private IP addresses on the LAN side and functions as a DHCP server. The router's default LAN IP configuration is as follows:

- **LAN IP address:** 192.168.1.1
- **Subnet mask:** 255.255.255.0

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network requires a different IP addressing scheme, you can change these settings.

You might want to change these settings if you need a specific IP subnet that one or more devices on the network uses, or if you use competing subnets with the same IP scheme.

**Note:** The IP settings for LAN 1 can be automatically changed if the Orbi Pro WiFi 6 router detects a double NAT condition. (For more information about double NAT, visit <https://kb.netgear.com/30186/What-is-double-NAT-and-why-is-it-bad>.) The router can detect this condition during the setup process if you select router mode even though another router is already present in your network. If your Orbi Pro WiFi 6 router is connected to another router that is already operating with the 192.168.1.x LAN scheme, the LAN scheme of the Orbi Pro WiFi 6 router is automatically changed to 10.0.0.1, and the DHCP address range is changed to 10.0.0.2-10.0.0.254.

### To change the settings for the default LAN 1:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > LAN Setup > LAN 1**.

The LAN Setup page displays.

5. In the **IP Address** field, type the IP address.

The default IP address is 192.168.1.1.

6. In the **IP Subnet Mask**, type the subnet mask of the router.

The IP address and subnet mask identifies which addresses are local to a specific device and which must be reached through a gateway or router.

The default IP subnet mask is 255.255.255.0.

7. Change the RIP settings.

Router Information Protocol (RIP) allows a router to exchange routing information with other routers.

- a. Select a setting from the **RIP Direction** menu:

- **Both**: The router broadcasts its routing table periodically and incorporates information that it receives.
- **Out Only**: The router broadcasts its routing table periodically.
- **In Only**: The router incorporates the RIP information that it receives.

- b. Select a setting from the **RIP Version** menu:

- **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-2**: This format carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.

8. Click the **Apply** button.

Your settings are saved.

If you changed the LAN IP address of the router, you are disconnected when this change takes effect.

9. To reconnect, close your browser, relaunch it, and log in to the router.

## Change the employee LAN 2 settings

By default, LAN 2 is assigned to the Employee VLAN profile with ID 20. If you use this LAN and associated VLAN, you can separate employee traffic from other types of traffic on your router. The default IP address of LAN 2 is 192.168.20.1.

In most situations, you do not need to change the settings for LAN 2, but you can do so to customize the IP address or VLAN. You can also disable LAN 2.

### To change the employee LAN 2 settings:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup > LAN 2**.  
The LAN Setup page displays.
5. If you previously disabled the LAN setup for LAN 2, select the **Enable LAN2 Setup** check box.
6. In the **IP Address** field, type the IP address.  
The default IP address is 192.168.20.1.
7. In the **IP Subnet Mask**, type the subnet mask of the router.  
The IP address and subnet mask identifies which addresses are local to a specific device and which must be reached through a gateway or router.  
The default IP subnet mask is 255.255.255.0.
8. Although the preset Employee VLAN profile for the LAN 2 works well for most situations, if you want to change the VLAN profile, select the **VLAN Profile** check box, and select another VLAN profile from the menu.  
The preset VLAN profile name is Employee, the VLAN has ID 20, and the combination is shown in the menu as Employee(20).

For more information about VLANs, see [Manage the VLANs](#) on page 71, including [How the router organizes LANs, VLANs, and WLANs](#) on page 73. For information about adding a new VLAN to a LAN, see [Add a new VLAN profile directly to a LAN](#) on page 76.

9. Click the **Apply** button.

Your settings are saved.

If you changed the LAN IP address of the router, you are disconnected when this change takes effect.

10. To reconnect, close your browser, relaunch it, and log in to the router.

## Change the IoT LAN 3 settings

By default, LAN 3 is assigned to the IoT VLAN profile with ID 30. If you use this LAN and associated VLAN, you can separate Internet of things (IoT) traffic from other types of traffic on your router. The default IP address of LAN 2 is 192.168.30.1.

In most situations, you do not need to change the settings for LAN 3, but you can do so to customize the IP address or VLAN. You can also disable LAN 3.

### To change the IoT LAN 3 settings:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > LAN Setup > LAN 3**.

The LAN Setup page displays.

5. If you previously disabled the LAN setup for LAN 3, select the **Enable LAN3 Setup** check box.

6. In the **IP Address** field, type the IP address.

The default IP address is 192.168.30.1.

7. In the **IP Subnet Mask**, type the subnet mask of the router.  
The IP address and subnet mask identifies which addresses are local to a specific device and which must be reached through a gateway or router.  
The default IP subnet mask is 255.255.255.0.
8. Although the preset IoT VLAN profile for LAN 3 works well for most situations, if you want to change the VLAN profile, select the **VLAN Profile** check box, and select another VLAN profile from the menu.  
The preset VLAN profile name is IoT, the VLAN has ID 30, and the combination is shown in the menu as IoT(30).  
For more information about VLANs, see [Manage the VLANs](#) on page 71, including [How the router organizes LANs, VLANs, and WLANs](#) on page 73. For information about adding a new VLAN to a LAN, see [Add a new VLAN profile directly to a LAN](#) on page 76.
9. Click the **Apply** button.  
Your settings are saved.  
If you changed the LAN IP address of the router, you are disconnected when this change takes effect.
10. To reconnect, close your browser, relaunch it, and log in to the router.

## Change the guest LAN 4 settings

By default, LAN 4 is assigned to the Guest VLAN profile with ID 40. If you use this LAN and associated VLAN, you can separate guest traffic from other types of traffic on your router. The default IP address of LAN 2 is 192.168.40.1.

In most situations, you do not need to change the settings for LAN 4, but you can do so to customize the IP address or VLAN. You can also disable LAN 4.

### **To change the guest LAN setting:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > LAN Setup > LAN 4**.

The LAN Setup page displays.

5. If you previously disabled the LAN setup for LAN 4, select the **Enable LAN4 Setup** check box.

6. In the **IP Address** field, type the IP address.

The default IP address is 192.168.40.1.

7. In the **IP Subnet Mask**, type the subnet mask of the router.

The IP address and subnet mask identifies which addresses are local to a specific device and which must be reached through a gateway or router.

The default IP subnet mask is 255.255.255.0.

8. Although the preset Guest VLAN profile for the Guest Portal WiFi network works well for most situations, if you want to change the VLAN profile, select the **VLAN Profile** check box, and select another VLAN profile from the menu.

The preset VLAN profile name is Guest, the VLAN has ID 40, and the combination is shown in the menu as Guest(40).

For more information about VLANs, see [Manage the VLANs](#) on page 71, including [How the router organizes LANs, VLANs, and WLANs](#) on page 73. For information about adding a new VLAN to a LAN, see [Add a new VLAN profile directly to a LAN](#) on page 76.

9. Click the **Apply** button.

Your settings are saved.

If you changed the LAN IP address of the router, you are disconnected when this change takes effect.

10. To reconnect, close your browser, relaunch it, and log in to the router.

## Set custom settings for LAN 5

You can set a custom VLAN profile for LAN 5.

### To set up LAN 5:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup > LAN 5**.
5. Select the **Enable LAN5 Setup** check box.  
By default, LAN 5 is disabled.
6. In the **IP Address** field, type the IP address.  
The default IP address is 192.168.50.1.
7. In the **IP Subnet Mask**, type the subnet mask of the router.  
The IP address and subnet mask identifies which addresses are local to a specific device and which must be reached through a gateway or router.  
The default IP subnet mask is 255.255.255.0.
8. From the **VLAN Profile** menu, select a custom VLAN profile.  
For more information about how to add a new VLAN profile, see [Add a new VLAN profile directly to a LAN](#) on page 76.
9. Click the **Apply** button.  
Your settings are saved.  
If you changed the LAN IP address of the router, you are disconnected when this change takes effect.
10. To reconnect, close your browser, relaunch it, and log in to the router.

## DHCP servers

You can set a Dynamic Host Configuration Protocol (DHCP) server for each LAN.

By default, the router acts as a DHCP server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN.

## Set up a DHCP server for the default LAN 1

The DHCP IP addresses for the default LAN 1 must be part of the same IP address subnet as the router's default LAN IP address. Using the default addressing scheme, define a range between 192.168.1.2 and 192.168.1.254.

### To set up the DHCP server for the default LAN 1:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup > LAN 1**.  
The LAN Setup page displays.
5. If you previously disabled the DHCP server feature, select the **Use Router as DHCP Server** check box.
6. Specify the range of IP addresses that the router assigns:
  - a. In the **Starting IP Address** field, enter the lowest number in the range.  
This IP address must be in the same subnet as the router. The default starting IP address is 192.168.1.2.
  - b. In the **Ending IP Address** field, enter the number at the end of the range of IP addresses.  
This IP address must be in the same subnet as the router. The default ending IP address is 192.168.1.254.
7. In the **lease time hour(s)** field, set the duration of the IP address lease in hours.  
By default, the lease expires after one day (24 hours), after which the WiFi client must renew the lease.
8. Click the **Apply** button.  
Your settings are saved.

The router delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range that you defined
- Subnet mask
- Gateway IP address (the router's LAN IP address)
- DNS server IP address (the router's LAN IP address)

## Set up a DHCP server for the employee LAN 2

The DHCP IP addresses for the employee LAN 2 must be part of the same IP address subnet as the router's default LAN IP address. Using the default addressing scheme, define a range between 192.168.20.2 and 192.168.20.254, although you can save part of the range for devices with fixed addresses.

### **To set up the DHCP server for the employee LAN 2:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > LAN Setup > LAN 2**.

The LAN Setup page displays.

5. If you previously disabled the DHCP server feature, select the **Use Router as DHCP Server** check box.

6. Specify the range of IP addresses that the router assigns:

- a. In the **Starting IP Address** field, enter the lowest number in the range.

This IP address must be in the same subnet as the router. The default starting IP address is 192.168.20.2.

- b. In the **Ending IP Address** field, enter the number at the end of the range of IP addresses.

This IP address must be in the same subnet as the router. The default ending IP address is 192.168.20.254.

7. In the **lease time hour(s)** field, set the duration of the IP address lease in hours. By default, the lease expires after one day (24 hours), after which the WiFi client must renew the lease.

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

The router delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range that you defined
- Subnet mask
- Gateway IP address (the router's LAN IP address)
- DNS server IP address (the router's LAN IP address)

## Set up a DHCP server for the IoT LAN 3

The DHCP IP addresses for the IoT LAN 3 must be part of the same IP address subnet as the router's default LAN IP address. Using the default addressing scheme, define a range between 192.168.30.2 and 192.168.30.254, although you can save part of the range for devices with fixed addresses.

### **To set up the DHCP server for the IoT LAN 3:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning on page 29](#).

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup > LAN 3**.  
The LAN Setup page displays.

5. If you previously disabled the DHCP server feature, select the **Use Router as DHCP Server** check box.
6. Specify the range of IP addresses that the router assigns:
  - a. In the **Starting IP Address** field, enter the lowest number in the range.  
This IP address must be in the same subnet as the router. The default starting IP address is 192.168.30.2.
  - b. In the **Ending IP Address** field, enter the number at the end of the range of IP addresses.  
This IP address must be in the same subnet as the router. The default ending IP address is 192.168.30.254.
7. In the **lease time hour(s)** field, set the duration of the IP address lease in hours.  
By default, the lease expires after one day (24 hours), after which the WiFi client must renew the lease.
8. Click the **Apply** button.  
Your settings are saved.

The router delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range that you defined
- Subnet mask
- Gateway IP address (the router's LAN IP address)
- DNS server IP address (the router's LAN IP address)

## Set up a DHCP server for the guest LAN 4

The DHCP IP addresses for the guest LAN 4 must be part of the same IP address subnet as the router's default LAN IP address. Using the default addressing scheme, define a range between 192.168.40.2 and 192.168.40.254, although you can save part of the range for devices with fixed addresses.

### **To set up the DHCP server for the guest LAN 4:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup > LAN 4**.  
The LAN Setup page displays.
5. If you previously disabled the DHCP server feature, select the **Use Router as DHCP Server** check box.
6. Specify the range of IP addresses that the router assigns:
  - a. In the **Starting IP Address** field, enter the lowest number in the range.  
This IP address must be in the same subnet as the router. The default starting IP address is 192.168.40.2.
  - b. In the **Ending IP Address** field, enter the number at the end of the range of IP addresses.  
This IP address must be in the same subnet as the router. The default ending IP address is 192.168.40.254.
7. In the **lease time hour(s)** field, set the duration of the IP address lease in hours.  
By default, the lease expires after one day (24 hours), after which the WiFi client must renew the lease.
8. Click the **Apply** button.  
Your settings are saved.  
The router delivers the following parameters to any LAN device that requests DHCP:
  - An IP address from the range that you defined
  - Subnet mask
  - Gateway IP address (the router's LAN IP address)
  - DNS server IP address (the router's LAN IP address)

## Set up a DHCP server for the custom LAN 5

The DHCP IP addresses for the custom LAN 5 must be part of the same IP address subnet as the router's default LAN IP address. Using the default addressing scheme, define a range between 192.168.50.2 and 192.168.50.254, although you can save part of the range for devices with fixed addresses.

### To set up the DHCP server for the custom LAN 5:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
  2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
  3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
  4. Select **ADVANCED > Setup > LAN Setup > LAN 5**.  
The LAN Setup page displays.
  5. If you previously disabled the DHCP server feature, select the **Use Router as DHCP Server** check box.
  6. Specify the range of IP addresses that the router assigns:
    - a. In the **Starting IP Address** field, enter the lowest number in the range.  
This IP address must be in the same subnet as the router. The default starting IP address is 192.168.50.2.
    - b. In the **Ending IP Address** field, enter the number at the end of the range of IP addresses.  
This IP address must be in the same subnet as the router. The default ending IP address is 192.168.50.254.
  7. In the **lease time hour(s)** field, set the duration of the IP address lease in hours.  
By default, the lease expires after one day (24 hours), after which the WiFi client must renew the lease.
  8. Click the **Apply** button.  
Your settings are saved.  
  
The router delivers the following parameters to any LAN device that requests DHCP:
    - An IP address from the range that you defined
    - Subnet mask
    - Gateway IP address (the router's LAN IP address)
    - DNS server IP address (the router's LAN IP address)
-

## Disable the DHCP server for a LAN

By default, the router acts as a DHCP server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the router.

You can use another device on your network as the DHCP server, or specify the network settings of all your computers.

### To disable a DHCP server feature in the router:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window opens.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.
5. Select the LAN tab for the LAN for which you want to disable the DHCP server: **LAN 1**, **LAN 2**, **LAN 3**, **LAN 4**, or **LAN 5**.  
The LAN Setup page displays.
6. Clear the **Use Router as DHCP Server** check box.
7. Click the **Apply** button.
8. (Optional) If this service is disabled and no other DHCP server is on your network, set your computer IP addresses manually so that they can access the router.

## Reserved LAN IP addresses

When you specify a reserved IP address for a computer on a LAN, that computer always receives the same LAN IP address each time it accesses the router's DHCP server. Assign reserved IP addresses to devices (such as servers) that require permanent IP settings.

## Reserve a LAN IP address

### To reserve an IP address:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > LAN Setup**.

5. Select the LAN tab for the LAN for which you want to reserve an IP address: **LAN 1**, **LAN 2**, **LAN 3**, **LAN 4**, or **LAN 5**.

The LAN Setup page displays.

6. In the Address Reservation section of the page, click the **Add** button.

The LAN Address Reservation page displays. Any detected devices display in the Address Reservation Table.

7. To reserve an IP address for a detected device, select the radio button in the Address Reservation Table.

8. To manually reserve an IP address for a device that is not connected or detected, do the following:

- a. In the **IP Address** field, type the IP address to assign to the device.
- b. In the **MAC Address** field, type or copy the MAC address of the device.
- c. In the **Device Name** field, type a name.

9. Click the **Apply** button.

The reserved address is entered into the table.

The reserved address is not assigned until the next time the computer contacts the router's DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

## Edit a reserved LAN IP address

### To edit a reserved address entry:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.
5. Select the LAN tab for the LAN for which you want to edit a reserved IP address entry: **LAN 1, LAN 2, LAN 3, LAN 4, or LAN 5**.  
The LAN Setup page displays.
6. Select the radio button next to the reserved address.
7. Click the **Edit** button.  
The LAN Address Reservation page displays.
8. Change the settings.
9. Click the **Apply** button.  
Your settings are saved.

## Delete a reserved LAN IP address entry

### To delete a reserved address entry:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > LAN Setup**.

5. Select the LAN tab for the LAN for which you want to delete a reserved IP address entry: **LAN 1**, **LAN 2**, **LAN 3**, **LAN 4**, or **LAN 5**.

The LAN Setup page displays.

6. Select the radio button next to the reserved address.

7. Click the **Delete** button.

The reserved IP address entry is removed.

# 8

## Manage the WAN and other Network Settings

---

This chapter includes the following sections:

- [WAN settings](#)
- [Dynamic DNS](#)
- [DMZ server](#)
- [Static routes](#)
- [Universal Plug and Play](#)
- [Link aggregation](#)

# WAN settings

You can view or configure wide area network (WAN) settings for the Internet port. You can set up a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the router to respond to a ping to its WAN (Internet) port.

## To view the WAN settings:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**  
The WAN Setup page displays.
5. View or change the following settings:
  - **Disable Port Scan and DoS Protection.** DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, and many others. Select this check box only in special circumstances.
  - **Default DMZ Server.** This feature is sometimes helpful when you are playing online games or videoconferencing, but it makes the firewall security less effective. See [DMZ server](#) on page 131.
  - **Respond to Ping on Internet Port.** This feature allows your router to be discovered. Use this feature only as a diagnostic tool or if you have a specific reason.
  - **Disable IGMP Proxying.** IGMP proxying allows a client on a LAN or WiFi network to receive the multicast traffic it is interested in from the Internet. By default, IGMP

proxying is disabled. If you clear the check box, IGMP proxying is enabled and you can select which type of IGMP messages are forwarded by the router:

- **Auto:** The router automatically detects the supported protocol (IGMPv3 or IGMPv2) and forwards the message accordingly. This is the default setting, which we recommend.
- **IGMPv3:** The router forwards IGMPv3 messages but can also forward IGMPv2 messages. (IGMPv3 is backward compatible with IGMPv2.).
- **IGMPv2:** The router forwards IGMPv2 messages *only* and ignores IGMPv3 messages.

If you do not need this feature, select the check box to disable it.

- **MTU Size (in bytes).** The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. Change the MTU only if you are sure that it is necessary for your ISP connection. See [MTU size](#) on page 50.
- **NAT Filtering.** Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT protects computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from working. Open NAT provides a much less secured firewall, but allows almost all Internet applications to work.
- **Disable SIP ALG.** The application-level gateway (ALG) for the Session Initiation Protocol (SIP) is enabled by default for enhanced 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, the router provides the option to disable the SIP ALG.

6. Click the **Apply** button.

Your settings are saved.

## Dynamic DNS

Internet service providers (ISPs) assign IP addresses to identify each Internet account. Most ISPs use dynamically assigned IP addresses, which means that the IP address can change at any time. If you know your IP address, you can use it to access your business network remotely. However, because the IP address is assigned dynamically, it can change.

To make it easier to connect, you can get a free account with a Dynamic DNS service that lets you use a domain name instead of an IP address to access your business network. To use this account, you must set up the router to use Dynamic DNS. The router then

notifies the Dynamic DNS service provider whenever its IP address changes. When you access your Dynamic DNS account, the service finds the current IP address of your business network and automatically connects you.

If your ISP assigns a private WAN IP address, the Dynamic DNS service does not work because private addresses are not routed on the Internet.

## Set up a new Dynamic DNS account

NETGEAR offers you the opportunity to set up and register for a free Dynamic DNS account.

### **To set up Dynamic DNS and register for a free NETGEAR account:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.

The Dynamic DNS page displays.

5. Select the **Use a Dynamic DNS Service** check box.

6. In the **Service Provider** list, select **NETGEAR**.

7. Select the **No** radio button.

8. In the **Host Name** field, type the name that you want to use for your URL.

Your free URL includes the host name that you specify, and ends with *mynetgear.com*. For example, if you set *myname* as the host name, the URL (domain name) is *myname.mynetgear.com*.

9. In the **Email** field, type the email address that you want to use for your account.

10. In the **Password (6-32 characters)** field, type the password for your account.

11. Select the check box to agree to the terms of service and privacy policy.

12. Click the **Register** button.

13. Follow the onscreen instructions to register for your NETGEAR Dynamic DNS service.
14. To check that Dynamic DNS is enabled in the router, click the **Show Status** button.  
A message displays the Dynamic DNS status.

## Specify a DNS account that you already created

If you already own a Dynamic DNS account with NETGEAR, no-IP, or Dyn, you can set up the router to use your account.

### To set up Dynamic DNS if you already created an account:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.  
The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. In the **Service Provider** list, select your provider.
7. Select the **Yes** radio button.  
The page adjusts and displays the **Show Status**, **Cancel**, and **Apply** buttons.
8. In the **Host Name** field, type the host name for your account.
9. Depending on the type of account, specify your user name or email address:
  - For a No-IP or Dyn account, in the **User Name** field, enter the user name for your account.
  - For a NETGEAR account, in the **Email** field, enter the email address for your account.
10. Depending on the type of account, in either the **Password (6-32 characters)** field or the **Password** field, type the password for your DDNS account.

11. Click the **Apply** button.  
Your settings are saved.
12. To verify that your Dynamic DNS service is enabled in the router, click the **Show Status** button.  
A message displays the Dynamic DNS status.

## Change the Dynamic DNS settings

### To change your settings:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.  
The Dynamic DNS page displays.
5. Change your DDNS account settings as necessary.
6. Click the **Apply** button.  
Your settings are saved.

## DMZ server

The default DMZ (demilitarized zone) server feature is helpful when you are using some online games 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 default DMZ server.

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 that you configured on the Port Forwarding/Port Triggering page of the router web interface (see [Customize Internet Traffic Rules for Ports](#) on page 185). Instead of discarding this traffic, you can specify that the router forwards the traffic to one computer on your network. This computer is called the default DMZ server.

**CAUTION:** DMZ servers pose a security risk. A computer designated as the default 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.

### **To set up a default DMZ server:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.  
The WAN Setup page displays.
5. Select the **Default DMZ Server** check box.
6. Type the IP address.
7. Click the **Apply** button.  
Your settings are saved.

## Static routes

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

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

- Your main Internet access is through a cable modem to your ISP. The cable modem is connected to your Orbi Pro WiFi 6 router.
- Your business network also includes an ADSL router that you use to access a remote office site. This ADSL router is connected to a DSL modem, which is used on-demand only.
- Your LAN subnet is 192.168.1.0, and the ADSL router's address on your LAN is 192.168.1.100.
- The public IP address range at the remote office site is 134.177.0.0.

When you set up your Orbi Pro WiFi 6 router, two implicit static routes were created:

1. A default route was created between your Orbi Pro WiFi 6 router and the cable modem that connects to your ISP.
2. A second static route was created between your Orbi Pro WiFi 6 router and your LAN for all 192.168.1.0 addresses.

With this configuration, if you try to access a device on the 134.177.0.0 network at the remote office site, your Orbi Pro WiFi 6 router forwards your request to your ISP. In turn, the ISP forwards your request to the remote office site, where the firewall will deny the request.

In this situation, you must define a static route, telling your Orbi Pro WiFi 6 router to access 134.177.0.0 addresses through your ADSL router at its LAN address of 192.168.1.100.

Here is an example static route setting for this configuration:

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

## Set up a static route

### To set up a static route:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.  
The Static Routes page displays.
5. Click the **Add** button.  
The page adjusts.
6. In the **Route Name** field, type a name for this static route (for identification purposes only.)
7. To limit access to the LAN only, select the **Private** check box.  
If Private is selected, the static route is not reported in RIP.
8. Select the **Active** check box to make this route take effect.
9. Type the IP address of the final destination.
10. Type the IP subnet mask for this destination.  
If the destination is a single host, type **255.255.255.255**.
11. Type the gateway IP address.  
This address must be on the same LAN segment as the router.
12. Type a number from 2 through 15 as the metric value.  
This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.
13. Click the **Apply** button.  
The static route is added.

## Change a static route

### To edit a static route:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.  
The Static Routes page displays.
5. In the table, select the radio button for the route.
6. Click the **Edit** button.  
The Static Routes page adjusts.
7. Edit the route information.
8. Click the **Apply** button.  
Your settings are saved.

## Delete a static route

### To delete a static route:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Static Routes**.

The Static Routes page displays.

5. In the table, select the radio button for the route.

6. Click the **Delete** button.

The route is removed from the table.

## Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance, enable UPnP.

### To enable Universal Plug and Play:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > UPnP**.

The UPnP page displays.

5. Select the **Turn UPnP On** check box.

By default, this check box is selected. UPnP for automatic device configuration can be enabled or disabled. If the **Turn UPnP On** check box is cleared, the router does

not allow any device to automatically control router resources, such as port forwarding.

6. 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. 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 networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.

8. Click the **Apply** button.

The UPnP Portmap Table displays the IP address of each UPnP device that is accessing the router and which ports (internal and external) that device opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

9. To refresh the information in the UPnP Portmap Table, click the **Refresh** button.

## Link aggregation

Both the Orbi Pro router and satellite support link aggregation, which lets you set up a link aggregation group (LAG) between the router and a satellite, between two satellites, between the router and a switch, or between the satellite and a switch. The switch must support 802.3ad link aggregation for static LAGs.

A LAG connection allows you to group two 1 Gbps LAN ports into either a single 2 Gbps connection for increased throughput or a 1 Gbps connection for redundancy.

Link aggregation is enabled by default on the router and the satellite, but you must bind the ports before you connect the cables. If you use a switch, you must configure link aggregation on the switch before you make the cable connections to the switch.

**CAUTION:** If you configure link aggregation incorrectly, a network loop can occur. Follow the right order for configuration and cable connections, as described in the procedures.

## Add a link aggregation group

You can add a link aggregation group (LAG) between the router and a satellite, between two satellites, between the router and a switch, or between the satellite and a switch. The switch must support 802.3ad link aggregation for static LAGs.

### To add a LAG:

1. If you want to add a LAG between the router and a switch or between a satellite and a switch, first do the following on the switch:

Configure static link aggregation on the two Ethernet ports that you plan to use for the LAG connection to the router or the satellite.

To prevent a network loop, configure the switch ports *before* connecting them to the router or satellite LAN ports.

2. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

3. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

4. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.

The VLAN / Bridge Settings page displays.

For the router (Base) and each satellite, the ports display on the page:

- **Blue:** The ports are connected to devices that are turned on.
- **Gray:** The ports are either not connected or are connected to devices that are not turned on.

6. In either the Base (router) or Satellite section, click an Ethernet port that you want to become part of a LAG.

The Bind button displays between the selected Ethernet port and the adjacent Ethernet port. (If the port does not support link aggregation, the Bind button does not display.)

7. Click the **Bind** button.

The ports are bound in a LAG. The ports now share a single VLAN Profile menu and Mode menu, that is, they share the same VLAN and port mode.

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

## Remove a link aggregation group

You can remove a link aggregation group (LAG). First remove the LAG, and then remove the cables.

### **To remove a LAG:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
  2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
  3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
  4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.  
The VLAN / Bridge Settings page displays.  
For the router (Base) and each satellite, the ports display on the page:
    - **Blue:** The ports are connected to devices that are turned on.
    - **Gray:** The ports are either not connected or are connected to devices that are not turned on.
  5. In either the Base (router) or Satellite section, click an Ethernet port that is part of the LAG.  
The Unbind button displays.
  6. Click the **Unbind** button.  
The ports are unbound.
  7. Click the **Apply** button.  
Your settings are saved.
-

## Set up a LAG connection between an Orbi Pro WiFi 6 AX5400 satellite and router

You can connect the Orbi Pro WiFi 6 AX5400 satellite over a LAG connection to the Orbi Pro WiFi 6 AX5400 router.

**CAUTION:** Be sure to follow the steps in the right order and to connect the correct ports for a LAG connection, as described in the following procedure. If you do not configure the LAG connection in the right order, a network loop can occur. If you use other LAN ports, the LAG connection will fail.

### To set up your Orbi Pro WiFi 6 AX5400 satellite over a LAG connection to the router:

1. Place your satellite in the room where you want WiFi service.
2. Connect an Ethernet cable to LAN port 1 on the satellite.
3. Connect the other end of the Ethernet cable to LAN port 1 on the router.

**CAUTION:** Do not yet connect the LAN 2 port on the satellite to the LAN 2 port on the router or to any other port on the router. You will do so at the end of this procedure, as described in the last two steps.

4. Connect the satellite to a power source.

The Power LED on the back of the satellite lights green.

The satellite bar LED pulses white. The satellite automatically syncs to the Orbi Pro WiFi 6 AX5400 router.

**Note:** The first time that you sync the satellite and the router, the sync process can take up to five minutes because the router might automatically update the satellite's firmware.

After the sync process is complete, the satellite bar LED lights blue for about three minutes and then turns off. Blue indicates that the router and satellite successfully synced, and the wired connection between the router and satellite is good.

5. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
6. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

7. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

8. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.

The VLAN / Bridge Settings page displays. Note the following:

- **Base section:** This is the section for the router (base). The rightmost port is the WAN port. The leftmost port is the LAN 1 port, which displays blue. To the right of it, the LAN 2 port displays gray because it does not yet have a cable attached.
- **Satellite section:** The leftmost port is the LAN 1 port, which displays blue. To the right of it, the LAN 2 port displays gray because it does not yet have a cable attached.

9. In the Base (router) section, do the following:

- a. Click LAN port 1.

The Bind button displays between the LAN 1 and LAN 2 ports.

- b. Click the **Bind** button.

The LAN 1 and LAN 2 ports are bound in a LAG on the router.

We recommend that you leave the default selection from the **Mode** menu as **Trunk**.

10. In the Satellite section, do the following:

- a. Click LAN port 1.

The Bind button displays between the LAN 1 and LAN 2 ports.

- b. Click the **Bind** button.

The LAN 1 and LAN 2 ports are bound in a LAG on the satellite.

For the satellite too, we recommend that you leave the default selection from the **Mode** menu as **Trunk**.

11. Click the **Apply** button.

Your settings are saved.

12. Connect an Ethernet cable to LAN port 2 on the satellite.

13. Connect the other end of the Ethernet cable to LAN port 2 on the router.

The satellite and the router establish a LAG connection.

# 9

## Manage and Monitor Your Orbi Pro System

---

This chapter describes the router settings for administering, maintaining, and monitoring your Orbi Pro system

The chapter includes the following sections:

- [Firmware for the router and satellite](#)
- [admin password](#)
- [Monitor the router, satellite, and Orbi network](#)
- [Syslog server](#)
- [Traffic meter](#)
- [NTP server](#)
- [Time zone](#)
- [Configuration file](#)
- [Remote management](#)
- [Remote access](#)
- [AP mode](#)
- [Router mode](#)
- [Sync button security](#)

# Firmware for the router and satellite

You can use the router web interface to check if new firmware is available and update your router and satellite, or you can manually update the firmware for your router and satellite.

## Enable the automatic firmware update feature

You can let the router automatically update its firmware and the firmware for any Orbi satellites on the network.

### To enable the automatic firmware update feature:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > Firmware Update**.  
The Firmware Update page displays.
5. In the Orbi Router Auto Firmware Update section, select the **Enable** radio button.
6. Click the **Apply** button.  
Your settings are saved.

## Check for firmware updates

### To check for new firmware and update your router and satellite:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window opens.

3. Enter the router admin user name and password.

The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Administration > Firmware Update**.

The Firmware Update page displays.

5. Click the **Check** button.

The router checks to see if new firmware is available for the router and satellite.

6. If new firmware is available, click the **Update All** button.

The router locates and downloads the firmware for the router and satellite and begins the update.

**CAUTION:** 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 or satellite.

When the upload is complete, your router and satellite restart. The update process typically takes about one minute. Read the new firmware release notes to find out if you must reconfigure the router after updating.

## Manually update firmware

If a satellite is connected to your router, you can log in to the router to manually upload the firmware on your satellite.

**CAUTION:** Update firmware in the correct order by following these firmware update guidelines:

- Update the firmware on your satellite first, and then update your router.
- Do not update the firmware on your satellite and router at the same time.
- Do not update more than one Orbi device (router or satellite) at a time. If you need to update more than one Orbi device, wait for the first Orbi device to finish updating before updating your next Orbi device.

**To manually update the firmware on your Orbi router and satellite, follow these high level steps:**

1. Visit [netgear.com/support](https://netgear.com/support) and download the firmware for both your Orbi router and satellite.
2. Update the firmware on your Orbi satellite.  
For more information, see [Manually update satellite firmware](#) on page 145.
3. Update the firmware on your Orbi router.  
For more information, see [Manually update router firmware](#) on page 146.

## Manually update satellite firmware

We recommend that you update your satellite's firmware *before* you update the router's firmware.

**To manually update your satellite's firmware:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > Firmware Update > Manual Update**.  
The Firmware Update page displays.
5. Select the check box next to your satellite's model name.  
If you have more than one satellite, only update one satellite at a time. You must wait for the first satellite to finish updating before updating the next satellite.
6. Click the **Update** button.  
The Orbi satellite Firmware Update window opens.
7. If the browser ask you for the admin password, enter the same password that you entered for the router.

8. Click the **Browse** button.
9. Locate and select the satellite firmware file that you downloaded.  
The firmware file name ends in `.img` or `.chk`.
10. Click the **Upload** button.  
It takes a few minutes to complete the process.

**CAUTION:** 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 or satellite.

11. After the Orbi satellite finishes updating, check the firmware version on the Firmware Update page.  
The firmware on your Orbi satellite is updated.

## Manually update router firmware

We recommend that you update your router's firmware *after* you update the satellite's firmware.

**CAUTION:** Be sure that your satellite completes its firmware update before you update your router's firmware.

### To manually update your router's firmware:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > Firmware Update > Manual Update**.  
The Firmware Update page displays.

5. Click the **Browse** button.
6. Locate and select the router firmware file you downloaded.  
The firmware file name ends in `.img` or `.chk`.
7. Click the **Upload** button.  
It takes a few minutes to complete the process.

**CAUTION:** 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.

8. After the router finishes updating, check the firmware version in the Router Information pane on the ADVANCED home page.  
The firmware on your Orbi router is updated.

## admin password

The admin password is the password that you need to log in to the router web interface and satellite web interface. You can change this password, and you can enable the password reset feature so that you can reset the password if it is forgotten.

### Change the admin password

This feature let you change the default password that is used to log in to the router with the user name admin. This password is not the one that you use to access the Orbi WiFi network.

**Note:** Be sure to change the password for the user name admin to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

#### To set the password for the user name admin:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window opens.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Administration > Set Password**.

The Set Password page displays.

5. Type the old password, and type the new password twice.
6. To be able to reset the password, select the **Enable Password Reset** check box.  
We recommend that you enable password reset.
7. Click the **Apply** button.  
Your settings are saved.

## Enable admin password reset

The router admin password is used to log in to your router web interface. We recommend that you enable password reset so that you can reset the password if you forget it. This reset process is supported in Chrome, Safari, Firefox, Edge, and Internet Explorer

### To enable password reset:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > Set Password**.  
The Set Password page displays.
5. Select the **Enable Password Reset** check box.
6. Select two security questions and provide answers to them.
7. Click the **Apply** button.  
Your settings are saved.

## Reset the admin password

If you set up the password reset feature, you can reset your router admin password if you forgot it. This reset process is supported in Chrome, Safari, Firefox, Edge, and Internet Explorer.

### To reset your admin password:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Click the **Cancel** button.  
If password reset is enabled, you are prompted to enter the serial number of the router.  
The serial number is on the router label.
4. Enter the router's serial number in the field.
5. Click the **Continue** button.  
The Router Password Reset page displays.
6. Enter the answers to your security questions.
7. Click the **Continue** button.  
The page adjusts.
8. Type a new admin password, confirm your new password, and set new security questions and answers.
9. Click the **Next** button.  
The page displays a confirmation.
10. Click the **Login Again** button.  
A login window opens.
11. With your new admin password, log in to the router.

# Monitor the router, satellite, and Orbi network

You can monitor the behavior and many of the features of your router, satellite, and Orbi network

## View router status and usage information

### To view router status and usage information:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Click the **ADVANCED** tab.  
The ADVANCED Home page displays the router status.

## View the satellite status in the satellite web interface

The satellite web interface lets you view satellite status information that you cannot view from the router web interface. You can find the IP address of the satellite in the router web interface. You can then launch a new web browser window, enter the satellite IP address, and access the satellite web interface.

To view your satellite's status, it must be connected to your Orbi network.

### To view your satellite's status:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Attached Devices**.  
The Attached Devices page displays.
5. In the Wireless Devices section, find your satellite's IP address.
6. Launch a new web browser window and enter your satellite's IP address in the web browser's address bar.  
A login window opens.
7. Enter the same admin user name and password that you entered for the router.  
The satellite status displays. The page displays information about the satellite connections, hardware and firmware versions, and the WiFi networks in the 2.4 GHz and 5 GHz bands.
8. To view detailed information about devices that are connected to the satellite networks, select **Connected Devices**.  
The Connected Devices page displays. For each device, the page displays the IP address, device name, MAC address, and connection type.

## View satellites, WiFi devices, and wired devices connected to the Orbi network

You can view all satellites, WiFi devices, and wired devices that are connected to your Orbi network.

### **To view devices connected to your network:**

1. In the Connected Satellites section, find your satellite's IP address.
2. Select **Attached Devices**.  
The Attached Devices page displays.

The Wired Devices table displays the following information:

- **Status:** Displays only if a MAC ACL (see [MAC access control lists](#) on page 53) or network access control (see [Network access control list](#) on page 58) is enabled. The field displays if a device is allowed or blocked. (For satellites, N/A is shown.)
- **Device Name:** The device model, name, type, and IP address.
- **IP Address:** The device IP address. The device's IP address can change because the router assigns an IP address to each device when it joins the network.
- **MAC Address:** The device MAC address. The unique MAC address for each device does not change.
- **Connection Type:** The device is connected to the Orbi network through a wired Ethernet connection.
- **Connected Orbi:** The Orbi router or satellite that the device is connected to. The Orbi router's or satellite's MAC address also displays.

The Wireless Devices table displays the following information:

- **Status:** Displays only if a MAC ACL (see [MAC access control lists](#) on page 53) or network access control (see [Network access control list](#) on page 58) is enabled. The field displays if a device is allowed or blocked. (For satellites, N/A is shown.)
- **Device Name:** The device model, name, type, and IP address.
- **IP Address:** The device IP address. The device's IP address can change because the router assigns an IP address to each device when it joins the network.
- **MAC Address:** The device MAC address. The unique MAC address for each device does not change.
- **Channel:** The channel on which the device is connected to the WiFi network.
- **SSID:** The radio band of the WiFi network to which the device is connected.
- **Connected Orbi:** The Orbi router or satellite that the device is connected to. The Orbi router's or satellite's MAC address also displays.
- **TX/RX Rate (Mbps):** The average rate in Mbps at which the device transmits (TX) and receives (RX) traffic.
- **Association Time:** The period in hours, minutes, and seconds that the device is connected to the WiFi network.
- **Link Status:** The quality and strength in dBm of the WiFi connection of the device.

3. To update the page with the most recent information, click the **Refresh** button.

## Check the Internet connection status or renew the connection

### To check the Internet connection status:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window opens.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Click the **ADVANCED** tab.
5. In the Internet Port pane, click the **Connection Status** button.  
The Connection Status window displays.

The information that displays depends on the type of Internet connection. When the router receives an IP address dynamically (which is the most common type of connection), the following information displays:

- **IP Address:** The IP address that is assigned to the router.
- **Subnet Mask:** The subnet mask that is assigned to the router.
- **Default Gateway:** The IP address for the default gateway that the router communicates with.
- **DHCP Server:** The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.
- **DNS Server:** The IP address of the Domain Name Service server that provides translation of network names to IP addresses.
- **Lease Obtained:** The date and time when the lease was obtained.
- **Lease Expires:** The date and time that the lease expires.

6. When the router receives an IP address dynamically, you can perform the following actions:
  - **Release:** Click the **Release** button to terminate the DHCP IP address, that is, terminate the Internet connection.
  - **Renew:** Click the **Renew** button to renew the DHCP IP address, that is, renew the Internet connection.
7. To close the window, click the **Close Window** button.

## Display port and radio statistics

### To display port and radio statistics:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window opens.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Click the **ADVANCED** tab.
5. In the Internet Port pane, click the **Show Statistics** button.  
The Show Statistics window displays and shows following information:
  - **System Up Time:** The time elapsed since the router was last restarted.
  - **Port:** The statistics for the WAN (Internet) and LAN (Ethernet) ports, the WiFi radios (indicated as WLANs in the window), and the WiFi backhaul connection (indicated as the WLAN Backhaul in the window) between the router and the satellite. For each port and radio, and for the backhaul connection, the window displays the following information:
    - **Status:** The link status of the port.
    - **TxPkts:** The number of packets transmitted on this port since reset or manual clear.
    - **RxPkts:** The number of packets received on this port since reset or manual clear.
    - **Collisions:** The number of collisions on this port since reset or manual clear.

- **Tx B/s:** The current transmission (outbound) bandwidth used on the WAN and LAN ports.
  - **Rx B/s:** The current reception (inbound) bandwidth used on the WAN and LAN ports.
  - **Up Time:** The time elapsed since this port acquired the link.
  - **Poll Interval:** The interval at which the statistics are updated in this page.
6. To change the polling frequency, enter a time in seconds in the **Poll Interval** field and click the **Set Interval** button.
  7. To stop the polling entirely, click the **Stop** button.

## View and manage logs of router activity

The log is a detailed record of the websites users accessed or attempted to access and many other router actions. You can specify which actions are logged. Up to 256 entries can be stored in the log.

### To view and manage logs:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > Logs**.  
The Logs page displays the following information:
  - **Date and time:** The date and time the log entry was recorded.
  - **Source IP:** The IP address of the initiating device for this log entry.

- **Target address:** The name or IP address of the website or news group visited or to which access was attempted.
  - **Action:** The action that occurred, such as whether Internet access was blocked or allowed.
5. To manage the actions that the router logs, check or clear the check boxes for the following actions:
    - **Attempted access to allowed sites:** Selected by default.
    - **Attempted access to blocked sites and services:** Selected by default.
    - **Connections to the Web-based interface of this Router:** Selected by default.
    - **Router operation (startup, get time etc):** Selected by default.
    - **Known DoS attacks and Port Scans:** Selected by default.
    - **Port Forwarding / Port Triggering:** Selected by default.
    - **Wireless access:** Selected by default.
    - **VPN Service:** Selected by default.
    - **Insight:** Cleared by default.
  6. To refresh the log page, click the **Refresh** button.
  7. To email the log immediately, click the **Send Log** button.  
If you cannot email the logs, set up email notifications (see [Email notifications for security events](#) on page 69).
  8. To clear the log entries, click the **Clear Log** button.

## Syslog server

If a syslog server is present on your network, you can configure the router to send its system logs to the syslog server.

### To enable the syslog function and specify the syslog server:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Advanced > Administration > Logs**.  
The Logs page displays.
5. At the bottom of the page, in the Syslog Server section, select the **Enable Syslog** radio button.  
The Syslog fields become available.
6. Specify the IP address and port number for the syslog server:
  - **Syslog Server IP Address:** Enter the IP address of the syslog server on your network.
  - **Syslog Port:** Enter the port number through which the router can reach the syslog server. By default, the port number is 514.
7. Click the **Apply** button.  
Your settings are saved. The router sends its logs to the syslog server.

## Traffic meter

You can enable traffic metering to monitor the volume of Internet traffic that passes through the router's WAN (Internet) port. With the traffic meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

### Start the traffic meter without traffic restrictions

You can monitor the traffic volume without setting a limit on the volume or connection time.

#### **To start or restart the traffic meter without configuring traffic volume or connection time restrictions:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Traffic Meter**.

The Traffic Meter page displays.

5. Select the **Enable Traffic Meter** check box.

By default, no traffic limit is specified and the traffic volume or connection time is not controlled.

6. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.

7. To start the traffic counter immediately, click the **Restart Counter Now** button.

8. Click the **Apply** button.

Your settings are saved.

The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see [View the Internet traffic volume and statistics](#) on page 161.

## Restrict Internet traffic by volume

You can record and restrict the traffic by volume in MB. This is useful when your ISP measures your traffic volume.

### **To record and restrict the Internet traffic by volume:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Traffic Meter**.

The Traffic Meter page displays.

5. Select the **Enable Traffic Meter** check box.
6. Select the **Traffic volume control by** radio button.
7. From the corresponding menu, select an option:
  - **Download only**. The restriction is applied to incoming traffic only.
  - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
8. In the **Monthly Limit** field, enter how many MBytes (MB) per month are allowed.
9. If your ISP charges you for extra data volume when you make a new connection, enter the extra data volume in MB in the **Round up data volume for each connection by** field.
10. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
11. In the Traffic Control section, enter a value in MB to specify when the router issues a warning message before the monthly limit in MB is reached.

This setting is optional. The router issues a warning when the balance falls below the number of MB that you enter. By default, the value is 0 and no warning message is issued.
12. To enable the router to disconnect and disable the Internet connection when the limit is reached, select the **Disconnect and disable the Internet connection** button.
13. Click the **Apply** button.

Your settings are saved.

The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see [View the Internet traffic volume and statistics](#) on page 161.

## Restrict Internet traffic by connection time

You can record and restrict the traffic by connection time. This is useful when your ISP measures your connection time.

### To record and restrict the Internet traffic by connection time:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.  
The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.
6. Select the **Connection time control** radio button.  
The router must be connected to the Internet for you to be able to select the **Connection time control** radio button.
7. In the **Monthly Limit** field, enter how many hours per month are allowed.  
The router must be connected to the Internet for you to be able to enter information in the **Monthly Limit** field.
8. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
9. In the Traffic Control section, enter a period in minutes to specify when the router issues a warning message before the monthly limit in hours is reached.  
This setting is optional. The router issues a warning when the balance falls under the number of minutes that you enter. By default, the value is 0 and no warning message is issued.
10. To enable the router to disconnect and disable the Internet connection when the limit is reached, select the **Disconnect and disable the Internet connection** button.
11. Click the **Apply** button.  
Your settings are saved.

The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see [View the Internet traffic volume and statistics](#) on page 161.

## View the Internet traffic volume and statistics

If you enabled the traffic meter (see [Start the traffic meter without traffic restrictions](#) on page 157), you can view the Internet traffic volume and statistics.

### To view the Internet traffic volume and statistics shown by the traffic meter:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.  
The Traffic Meter page displays.
5. Scroll down to the Internet Traffic Statistics section.  
The Internet Traffic Statistics section displays when the traffic counter was started and what the traffic balance is. The table displays information about the connection time and traffic volume in MB.
6. To refresh the information onscreen, click the **Refresh** button.  
The information is updated.
7. To display more information about the data traffic and to change the polling interval, click the **Traffic Status** button.  
The Traffic Status pop-up windows displays.

## Unblock the traffic meter after the traffic limit is reached

If you configured the traffic meter to disconnect and disable the Internet connection after the traffic limit is reached, you cannot access the Internet until you unblock the traffic meter.

**CAUTION:** If your ISP set a traffic limit, your ISP might charge you for the overage traffic.

### To unblock the traffic meter:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.  
The Traffic Meter page displays.
5. In the Traffic Control section, clear the **Disconnect and disable the Internet connection** check box.
6. Click the **Apply** button.  
Your settings are saved.

## NTP server

By default, the router uses the NETGEAR Network Time Protocol (NTP) server to sync the network time. You can change the NTP server to your preferred NTP server.

### To change the NTP server to your preferred NTP server:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window opens.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > NTP Settings**.

The NTP Settings page displays.

5. Select the **Set your preferred NTP server** radio button.
6. Enter the NTP server domain name or IP address in the **NTP server** field.
7. Click the **Apply** button.  
Your settings are saved.

## Time zone

### To set your time zone manually:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > NTP Settings**.  
The NTP Settings page displays.
5. Select your time zone from the menu.
6. If you live in a region that observes daylight saving time, select the **Automatically adjust for daylight savings time** check box.
7. Click the **Apply** button.  
Your settings are saved.

## Configuration file

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, restore it, or reset it to the factory default settings.

## Back up settings

### To back up the router's configuration settings:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window opens.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > Backup Settings**.  
The Backup Settings page displays.
5. Click the **Back Up** button.
6. Specify a location on your network.  
A copy of the current settings is saved in the location you specified.

## Manage the automatic backup options

You can let the router automatically back up configuration settings before a firmware upgrade.

You can also schedule an automatic backup at a regular interval.

### To manage the automatic backup options:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning on page 29](#).
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.

4. Select **ADVANCED > Administration > Backup Settings**.

The Backup Settings page displays.

5. To let the router automatically back up configuration settings before a firmware upgrade, select the **Backup before upgrade** check box.
6. To schedule automatic backups, next to Back up periodically, enter the a number from 1 to 365 in the **Day(s)** field.  
If you enter 1, the backup occurs daily, if you enter 2, the backup occurs every other day, and so on. By default, the entry is 0 and no automatic backup occurs.
7. Click the **Apply** button.  
Your settings are saved.

## Erase the current configuration settings

You can erase the current configuration and restore the factory default settings. You might want to do this if you move the router to a different network.

### To erase the configuration settings:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > Backup Settings**.  
The Backup Settings page displays.
5. Click the **ERASE** button.  
The factory default settings are restored. The user name is admin, the password is **password**, and the LAN IP address is 192.168.1.1. DHCP is enabled.

## Restore configuration settings

### To restore configuration settings that you backed up:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Administration > Backup Settings**.  
The Backup Settings page displays.
5. Click the **Browse** button to find and select the `.cfg` file.
6. Click the **Restore** button.  
The file is uploaded to the router and the router reboots.

**CAUTION:** Do not interrupt the reboot process.

## Remote management

You can access your router over the Internet to view or change its settings. You must know the router's WAN IP address to use this feature. For information about Dynamic DNS, see [Dynamic DNS](#) on page 128.

**Note:** Be sure to change the password for the user name admin to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters. See [Change the admin password](#) on page 147.

### To set up remote management:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Remote Management**.  
The Remote Management page displays.
5. Select the **Turn Remote Management On** check box.
6. In the Allow Remote Access By section, specify the external IP addresses to be allowed to access the router's remote management.

**Note:** For enhanced security, restrict access to as few external IP addresses as is practical.

Select one of the following:

- To allow access from a single IP address on the Internet, select the **Only This Computer** radio button. Enter the IP address to be allowed access.
  - To allow access from a range of IP addresses on the Internet, select the **IP Address Range** radio button. Enter a beginning and ending IP address to define the allowed range.
  - To allow access from any IP address on the Internet, select the **Everyone** radio button.
7. Specify the port number for accessing the router.  
The default port for secure HTTP (HTTPS) access is 8443. You can enter a custom port number for the remote router access. Choose a number from 1024 to 65535, but do not use the number of any common service port.
  8. Click the **Apply** button.  
Your settings are saved.

## Remote access

### To use remote access:

1. Launch a web browser on a computer that is not on your business network.
2. Type your router's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number.

For example, if your external address is 134.177.0.123 and you use port number 8080, enter **https://134.177.0.123:8080** in your browser.

## AP mode

You can set up the Orbi Pro router to function as an access point (AP) on the same local network as another router or gateway. When the Orbi Pro router functions as an AP, its router features are disabled to prevent any conflict with the other router or gateway on the network.

For example, you can use the Orbi router as a WiFi access point that connects to a gateway or modem router that you already use for your Internet service. In this situation, you do not need to change the settings for the gateway or modem router.

**Note:** If your network includes two or more Orbi Pro routers, we recommend that you use router mode (the default operation mode) on all Orbi Pro routers.

### To set up the Orbi router as an AP after you set up your Internet connection:

1. Use an Ethernet cable to connect the Internet port of this router to a LAN port on your existing router or gateway.
2. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

3. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

4. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Router/AP Mode**.

The Router/AP Mode page displays.

6. Select the **AP Mode** radio button.

The page adjusts.

7. Select the IP address setting:

- **Get dynamically from existing router:** The other router on the network assigns an IP address to the Orbi Prorouter while the Orbi Pro router is in AP mode.
- **Use fixed IP Address (not recommended):** Use this setting if you want to manually assign a specific IP address to the Orbi Pro router while the Orbi Pro router is in AP mode. Using this option effectively requires advanced network experience.

**Note:** To prevent interference with other WiFi routers or WiFi gateways in your network, we recommend that you use different WiFi settings on each WiFi routers or WiFi gateway. You can also turn off the WiFi radio on the other router or gateway and use the Orbi Pro router and satellite only for WiFi client access.

8. Click the **Apply** button.

The IP address of the router changes, and you are disconnected.

9. To reconnect, close and restart your browser and enter **orbilogin.com**.

## Router mode

If you set up your Orbi Pro router as an access point, you can change it back to a router.

**Note:** If your network includes two or more Orbi Pro routers, we recommend that you use router mode (the default operation mode) on all Orbi Pro routers.

### **To set up the Orbi Pro router as a router:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Router/AP Mode**.  
The Router/AP Mode page displays.
5. Select the **Router Mode** radio button.  
The page adjusts.
6. Click the **Apply** button.  
Your settings are saved.
7. Log back in to the router to go through the interactive Internet setup process (see [Use the interactive Internet setup process](#) on page 27).

## Sync button security

You can disable the physical Sync button on the router, satellite, or both. If you disable the physical Sync button, you can still use the Sync button in the router web interface to sync the connection between the router and a satellite. However, the WPS function of the Sync button (see [WiFi connection using WPS](#) on page 26) is disabled.

### Manage the Sync button on the router

By default, the physical Sync button on the router is enabled. You can disable the button for security reasons.

If you press the Sync button and the router's LED bar pulses magenta, this LED behavior indicates that the Sync button is disabled.

#### **To manage your router's Sync button using the router web interface:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Sync Button**.  
The Sync Button page displays.
5. Do one of the following:
  - **Disable the Sync button:** Click the **Enabled** button.
  - **Enable the Sync button:** Click the **Disabled** button.
6. Click the **Apply** button.  
Your settings are saved.

## Manage the Sync button on the satellite

By default, the physical Sync button on the satellite is enabled. You can disable the button for security reasons.

If you press the Sync button and the satellite's LED bar pulses magenta, this LED behavior indicates that the Sync button is disabled.

### **To manage your satellite's Sync button using the router web interface:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
  2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
  3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
  4. Select **Attached Devices**.
-

The Attached Devices page displays.

5. In the Wireless Devices table, click in the **Device Name** field for the satellite.  
The Edit Device page displays.
6. In the SYNC section, do one of the following:
  - **Disable the Sync button:** Click the **Enabled** button.
  - **Enable the Sync button:** Click the **Disabled** button.
7. Click the **Apply** button.  
Your settings are saved.

# 10

## Manage the Advanced WiFi Settings

---

This chapter includes the following sections:

- [Download bandwidth per SSID](#)
- [Region of operation](#)
- [SSID broadcast for a radio](#)
- [20/40 MHz coexistence for the 2.4 GHz radio](#)
- [Wi-Fi multimedia for a radio](#)
- [CTS/RTS threshold and preamble mode for a radio](#)
- [Transmission output power for a radio](#)
- [Backhaul password](#)
- [MU-MIMO](#)
- [Protected Management Frames](#)

Depending on the type of advanced WiFi setting, the setting applies either to all WiFi networks on *one* radio or to all WiFi networks on the router. That is, these settings do not apply to one individual WiFi network only.

For information about the individual WiFi networks, see [Manage the WiFi Networks](#) on page 85.

**IMPORTANT:** When you log in to the router and change the WiFi settings, the router automatically sends the new settings to any connected satellites.

# Download bandwidth per SSID

You can set up four WiFi networks for your Orbi Pro WiFi 6 network: one for administrative access, one for employee access, one for Internet of things (IoT) devices, and one for guest access. You can manage the download bandwidth per WiFi network (SSID) by assigning a percentage of the total bandwidth (100 percent) to each SSID. The available download bandwidth on an SSID determines the network priority for devices connected to the SSID.

If the download bandwidth usage on an SSID exceeds the assigned bandwidth for the SSID, the router limits the bandwidth on the SSID, which might affect the download speed for devices connected to the SSID.

In setting the download bandwidth ratio for an SSID, consider the number and type of devices that connect to the SSID and the typical download bandwidth usage for those devices. For example, more devices might connect to the IoT WiFi network than to the employee network, but the typical bandwidth usage for IoT devices might be lower than for employee devices.

**Note:** The router does not control the uplink bandwidth, that is, the bandwidth from devices to the router.

## To set the download bandwidth ratios for the SSIDs:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **Wireless**.  
The Wireless Settings page displays the admin WiFi settings.

**Note:** Even though this is the page for the admin WiFi settings, the bandwidth ratios that you specify on this page apply to the admin WiFi network, employee WiFi network, IoT WiFi network, and guest WiFi network. (All bandwidth ratios together must add up to 100 percent.) Similarly, if you specify bandwidth ratios on the employee WiFi settings page, IoT WiFi settings page, or the guest WiFi network page, they also apply to all other WiFi networks.

5. Select the **Enable Bandwidth per SSID** check box.  
In the Bandwidth per SSID graphic, the colored icons are enabled.
6. Specify the bandwidth ratios by moving the icons on the bandwidth line.  
The icons represent the following WiFi networks:
  - **Blue:** Admin WiFi network (Wireless 1).
  - **Green:** Employee WiFi network (Wireless 2).
  - **Purple:** IoT WiFi network (Wireless 3).
  - **Gray:** Guest WiFi network (Guest Portal).

As you move an icon, the bandwidth ratio for the WiFi network changes and the percentage displays in the icon.

All bandwidth ratios together add up to 100 percent of the available download bandwidth. If you change one ratio, the ratio for another WiFi network might also change.

7. Click the **Apply** button.  
Your settings are saved. The router sends the new settings to the satellite.

## Region of operation

You can change the region of operation, which is region in which you operate the router. For some countries or regions, such as North America, you cannot change the region because it is preset.

**Note:** Make sure the country is set to the location where the device is operating. You are responsible for complying within the local, regional, and national regulations set for channels, power levels, and frequency ranges.

**WARNING:** It might not be legal to operate the router in a region other than the regions listed in the menu. If your country or region is not listed, check with your local government agency.

### To change the region of operation:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.  
The Advanced Wireless Settings page displays.
5. From the **Region** menu, select the region in which the router must operate.
6. Click the **Apply** button.  
Your settings are saved. The router restarts with the settings for the new region.

## SSID broadcast for a radio

By default, the router broadcasts its WiFi network names (SSIDs) so that WiFi clients can detect them in their scanned network lists. Turning off the SSID broadcast provides additional WiFi security, but users must know an SSID to be able to join its WiFi network.

For each 2.4 GHz and 5 GHz radio individually, you can enable or disable SSID broadcast, which then applies to all WiFi networks that use the radio.

### To enable or disable SSID broadcast:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings page displays.

5. For a radio, select or clear the **Enable SSID Broadcast** check box.

When this check box is selected (which it is by default), the router broadcasts its SSIDs on the radio so that they display when you scan for local WiFi networks on your computer or WiFi device.

6. Click the **Apply** button.

Your settings are saved.

## 20/40 MHz coexistence for the 2.4 GHz radio

20/40 coexistence allows a 20 MHz and 40 MHz channel width to be supported simultaneously. By default, 20/40 MHz coexistence is enabled on the 2.4 GHz radio to prevent interference between WiFi networks in your environment at the expense of the WiFi speed. If no other WiFi networks are present in your environment, you can disable 20/40 MHz coexistence to increase the WiFi speed on the 2.4 GHz radio to the maximum supported speed for the WiFi mode.

20/40 MHz coexistence does not apply to a 5 GHz radio.

### **To enable or disable 20/40 MHz coexistence for the 2.4 GHz radio:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings page displays.

5. Select or clear the **Enable 20/40 MHz Coexistence** check box.  
Selecting this check box enables 20/40 MHz coexistence and clearing this check box disables 20/40 MHz coexistence.  
By default, 20/40 MHz coexistence is enabled and the check box is selected.
6. Click the **Apply** button.  
Your settings are saved. The 2.4 GHz radio restarts and WiFi clients might need to reconnect.

## Wi-Fi multimedia for a radio

Wi-Fi multimedia (WMM) prioritizes WiFi voice and video traffic over the WiFi link. By default, WMM is enabled for all radios on the router.

WMM prioritizes WiFi data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM, WMM must be enabled for both the application and the client running that application. Legacy applications that do not support WMM and applications that do not require WMM are assigned to the best effort category, which receives a lower priority than voice and video.

For each 2.4 GHz and 5 GHz radio individually, you can enable or disable WMM, which then applies to all WiFi networks that use the radio.

**Note:** We recommend that you do not disable the WMM settings. If you disable the WMM settings for a radio, the maximum link rate that your router can reach on the radio is 54 Mbps.

### To enable or disable WMM:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings page displays.

5. For a radio, select or clear the **Enable WMM (Wi-Fi multimedia) settings** check box.

When this check box is selected (which it is by default), WMM is enabled.

6. Click the **Apply** button.

Your settings are saved.

## CTS/RTS threshold and preamble mode for a radio

For most WiFi networks, the clear to send/request to send (CTS/RTS) threshold and preamble mode work fine and we recommend that you do not change the settings. (In general, these settings are intended for WiFi testing.)

**CAUTION:** Do not change these settings unless directed by NETGEAR support or unless you are sure what the consequences are. Incorrect settings might disable the WiFi function of a radio unexpectedly.

### To change the CTS/RTS threshold and preamble mode for a radio:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning on page 29](#).

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings page displays.

5. In the **CTS/RTS Threshold (1-2347)** field for a radio, enter a value from 1 to 2437. The default value is 2347.

**CAUTION:** Incorrect settings might disable the WiFi function for the selected radio unexpectedly.

6. From the **Preamble Mode** menu for a radio, select **Automatic**, **Long Preamble**, or **Short Preamble**.
  - **Long Preamble:** A long transmit preamble might provide a more reliable connection or a slightly longer range.
  - **Short Preamble:** A short transmit preamble might give better performance.
  - **Automatic:** The automatic option (which is the default option) lets the router process both long and short preambles.

**CAUTION:** Incorrect settings might disable the WiFi function for the selected radio unexpectedly.

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

## Transmission output power for a radio

By default, the transmission output power of the router is set at the maximum. If two or more WiFi routers, access points, WiFi gateways, or combination of these WiFi devices are operating in the same area and on the same channel, interference can occur. In such a situation, you might want to decrease the transmission output power for one or both radios.

Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.

### To change the transmission output power for a radio:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.  
The Advanced Wireless Settings page displays.
5. From the **Transmit Power Control** menu , select **100%**, **50%**, or **25%**.  
The default setting is 100%.
6. Click the **Apply** button.  
Your settings are saved. The radio restarts and WiFi clients might need to reconnect.

## Backhaul password

The backhaul password is a security key that is used in WiFi communication between the router and the satellite. You can generate a new backhaul password. After you generate a new backhaul password, you must use the **Sync** button to build a new backhaul connection so that the router and satellite can communicate with each other using WiFi.

### **To generate a new backhaul password:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.  
The Advanced Wireless Settings page displays.
5. In the **Backhaul Password** section, click the **Generate** button.

The router generates a new backhaul password.

Generating a new password might cause the Orbi satellite to lose connection from the Orbi router. To reconnect, use the **Sync** button.

## MU-MIMO

Multuser multiple input, multiple output (MU-MIMO) improves performance when multiple MU-MIMO-capable WiFi clients transfer data at the same time. With MU-MIMO, the router can transmit to multiple clients simultaneously using the same channel. MU-MIMO is used in the downstream direction and requires the WiFi clients to be capable of 802.11ac or 802.11ax.

### **To enable or disable MU-MIMO:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.  
The Advanced Wireless Settings page displays.
5. Select or clear the **Enable MU-MIMO** check box.  
By default, the check box is selected, and MU-MIMO is enabled.
6. Click the **Apply** button.  
Your settings are saved. WiFi clients might need to reconnect.

# Protected Management Frames

Protected Management Frames (PMF), according to the 802.11w standard, is a security feature that protects unicast and multicast management frames from being intercepted and changed for malicious purposes.

The PMF feature is disabled by default, but you can enable it as a requirement for management frames. However, some legacy devices might not be capable of supporting PMF and might not be able to connect. As a solution, you can enable PMF as optional, which lets the router activate PMF based on whether devices can support PMF.

Make sure that you understand the technology before enabling this feature.

**Note:** If you enable PMF, some incompatible client devices might disconnect. If you use the combined WPA-PSK [TKIP] + WPA2-PSK [AES] security option and configure PMF as a requirement, PMF might not take effect.

## To enable or disable PMF:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.  
The Advanced Wireless Settings page displays.
5. At the bottom of the page, make one of the following selections from the **Protected Management Frames (802.11w)** menu:
  - **Disabled:** PMF is disabled. This is the default settings.
  - **Optional:** PMF is optional for all WiFi networks.
  - **Required:** PMF is required.

Your selection applies to all WiFi networks on the router and satellites.

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

# 11

## Customize Internet Traffic Rules for Ports

---

You can use port forwarding and port triggering to set up rules for Internet traffic. You need networking knowledge to set up these features.

This chapter includes the following sections:

- [Port forwarding to a local server](#)
- [Port triggering](#)

# Port forwarding to a local server

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 with specific protocols to computers on your local network. You can specify the servers for applications and you can also specify a default DMZ server to which the router forwards all other incoming protocols.

## Set up port forwarding to a local server

### To forward specific incoming protocols:

1. Decide which type of service, application, or game you want to provide.
2. Find the local IP address of the computer on your network that will provide the service.  
The server computer must always use the same IP address. To specify this setting, use the reserved IP address feature. See [Reserved LAN IP addresses](#) on page 122.
3. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
4. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
5. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
6. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.  
The Port Forwarding/Port Triggering page displays.
7. Leave the **Port Forwarding** radio button selected as the service type.
8. In the **Service Name** menu, select the service name.  
If the service that you want to add is not in the list, create a custom service. See [Add a custom port forwarding service](#) on page 187.

9. In the **Server IP Address** field, enter the IP address of the computer that will provide the service.
10. Click the **Add** button.  
The service displays in the list.

## Add a custom port forwarding service

### To add a custom service:

1. Find out which port number or range of numbers the application uses.  
You can usually find this information by contacting the publisher of the application or user groups or news groups.
2. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
3. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
4. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.  
The Port Forwarding/Port Triggering page displays.
6. Leave the **Port Forwarding** radio button selected as the service type.
7. Click the **Add Custom Service** button.  
The Ports - Custom Services page displays.
8. In the **Service Name** field, enter a descriptive name.
9. In the **Protocol** menu, select the protocol.  
If you are unsure, select **TCP/UDP**.
10. In the **External Port range** field, enter the port numbers.

11. Specify the internal ports by one of these methods:
  - Leave the **Use the same port range for Internal port** check box selected.
  - Type the port numbers in the **Internal port range** field.
12. Type the IP address in the **Internal IP address** fields or select the radio button for an attached device listed in the table.
13. Click the **Apply** button.

The service is now in the list on the Port Forwarding/Port Triggering page.

## Edit a port forwarding service

### To edit a port forwarding entry:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.

The Port Forwarding/Port Triggering page displays.
5. Leave the **Port Forwarding** radio button selected as the service type.
6. In the table, select the radio button next to the service name.
7. Click the **Edit Service** button.

The Ports - Custom Services page displays.
8. Specify changes to any of the following settings:
  - **Service Name:** Type the service name.
  - **Protocol:** If you are unsure, select TCP/UDP.
  - **External port range.**

- For the internal ports, leave the **Use the same port range for Internal port** check box selected or enter the ports in the **Internal port range** field.
  - **Internal IP address.** Type the IP address in the **Internal IP address** fields, or select the radio button for an attached device listed in the table.
9. Click the **Apply** button.  
Your settings are saved.

## Delete a port forwarding entry

### To delete a port forwarding entry:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.  
The Port Forwarding/Port Triggering page displays.
5. Select the **Port Forwarding** radio button as the service type.
6. In the table, select the radio button next to the service name.
7. Click the **Delete Service** button.

## 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 either a fixed IP address or a dynamic IP address using DHCP address reservation.  
In this example, your router always gives your web server an IP address of 192.168.1.33.
2. In the **Port Forwarding/Port Triggering** page, configure the router to 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. (Optional) Register a host name with a Dynamic DNS service, and specify that name on the Dynamic DNS page of the router.  
Dynamic DNS makes it much easier to access a server from the Internet because you can type the name in the Internet browser. Otherwise, you must know the IP address that the ISP assigned, which typically changes.

## How the router implements the port forwarding rule

The following sequence shows the effects of a port forwarding rule:

1. When you type the URL `www.example.com` in your browser, the browser sends a web page request message with the following destination information:
  - **Destination address:** The IP address of `www.example.com`, which is the address of your router.
  - **Destination port number:** 80, which is the standard port number for a web server process.
2. Your router receives the message and finds your port forwarding rule for incoming port 80 traffic.
3. The router changes the destination in the message to IP address 192.168.1.33 and sends the message to that computer.
4. Your web server at IP address 192.168.1.33 receives the request and sends a reply message to your router.
5. Your router performs Network Address Translation (NAT) on the source IP address, and sends the reply through the Internet to the computer or WiFi device that sent the web page request.

# Port triggering

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

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

With port triggering, the router monitors traffic 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.

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.

## Add a port triggering service

### To add a port triggering service:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.  
The Port Forwarding/Port Triggering page displays.
5. Select the **Port Triggering** radio button.  
The page adjusts.
6. Click the **Add Service** button.  
The Port Triggering - Services page displays.

7. In the **Service Name** field, type a descriptive service name.
8. In the **Service User** menu, select **Any**, or select **Single address** and enter the IP address of one computer:
  - **Any** (the default) allows any computer on the Internet to use this service.
  - **Single address** restricts the service to a particular computer.
9. Select the service type, either **TCP** or **UDP**.
10. In the **Triggering Port** field, enter the number of the outbound traffic port that will open the inbound ports.
11. Select the inbound connection type, either **TCP** or **UDP**, or **TCP/UDP** (both).  
If you are not sure, select **TCP/UDP**.
12. Enter the inbound connection port information in the **Starting Port** and **Ending Port** fields.
13. Click the **Apply** button.  
The service is now in the Portmap Table. You must enable port triggering before the router used port triggering for the service that you added. See [Enable port triggering](#) on page 192.

## Enable port triggering

### To enable port triggering:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.  
The Port Forwarding/Port Triggering page displays.

5. Select the **Port Triggering** radio button.  
The page adjusts.
6. Clear the **Disable Port Triggering** check box.  
If this check box is selected, the router does not use port triggering even if you specified port triggering settings.
7. In the **Port Triggering Timeout** field, enter a value up to 9999 minutes.  
This value controls how long the inbound ports stay open when the router detects no activity. This value is required because the router cannot detect when the application terminates.
8. Click the **Apply** button.  
Your settings are saved.

## 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). 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 the port triggering rule you define:

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. The IRC server 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 or 113.

# 12

## Use OpenVPN to Access Your Network

---

You can use OpenVPN software to remotely access your router with virtual private networking (VPN). This chapter explains how to install and use OpenVPN software to set up a VPN tunnel.

This chapter includes the following sections:

- [About VPN connections](#)
- [LAN IP addressing in VPN networks](#)
- [Enable OpenVPN service in the router](#)
- [Install OpenVPN software on a VPN client](#)
- [Use VPN to access your Internet service at your business](#)

**Note:** If you are a NETGEAR Insight Premium or Pro subscriber, you can enable and configure another VPN feature on your router: Business VPN. You cannot enable and configure this feature in the router web interface; You must use the NETGEAR Insight app or Insight Cloud Portal. For more information about NETGEAR Insight, visit <https://www.netgear.com/insight/>.

## About VPN connections

A virtual private network (VPN) lets you use the Internet to securely access your network when you are away from your business.

This type of VPN access is called a client-to-gateway tunnel. The computer is the client, and the router is the gateway. To use the VPN feature, you must do the following:

- Log in to the router to enable and configure OpenVPN (see [Enable OpenVPN service in the router](#) on page 197).
- Install OpenVPN client software and configuration files on your device from which you want to use VPN (see [Install OpenVPN software on a VPN client](#) on page 198).
- Run the OpenVPN client software on your device when you want to use a VPN connection.

Enabling OpenVPN on your router allows VPN connections between the router and a client, for example your laptop when you are away from your business. The router provides the VPN service and the laptop is the VPN client. Traffic between the router and the laptop is encrypted.

**Note:** The router itself does not function as a VPN client to an external VPN service provider, so it does not encrypt traffic passing between your business network and the Internet.

VPN can use either Dynamic DNS (DDNS) or a static IP address to connect with your router:

- To use a DDNS service, register for a DDNS account with a host name. You use the host name to access your business network. The router supports these DDNS accounts: NETGEAR, No-IP, and Dyn. For more information, see [Dynamic DNS](#) on page 128.
- If your Internet service provider (ISP) assigned a static WAN IP address that never changes, the VPN can use that IP address to connect to your business network.

## LAN IP addressing in VPN networks

For the VPN connection to work, your computer or device (the VPN client) must be connected to a network that uses a different LAN IP address scheme than your router.

The default LAN IP address scheme for the router is 192.168.1.x. (The most common IP schemes are 192.168.x.x, 172.x.x.x, and 10.x.x.x.) If you experience a conflict, change the IP scheme either for your business network or for the network where your VPN client device is connected.

If both networks use the same LAN IP scheme, when the VPN tunnel is established, you cannot access your business router or your business network with the OpenVPN software. For information about changing the LAN settings on the router, see [Manage the LANs](#) on page 107.

## Enable OpenVPN service in the router

You must enable the OpenVPN service settings in the router before you can use a VPN connection.

### To enable the OpenVPN service:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > VPN Service**.

The VPN Service page displays.

**Note:** The OpenVPN configuration software packages that you can download on the page are for the VPN client devices (see [Install OpenVPN software on a VPN client](#) on page 198).

5. Select the **Enable VPN Service** check box.

We recommend that you use the default TUN mode and TAP mode settings. (These settings determine how VPN information is transferred.) If you know that you need other settings, you can change the TUN mode and TAP mode settings, but you must do so *before* you download and install the OpenVPN configuration software packages on client devices (see [Install OpenVPN software on a VPN client](#) on page 198).

6. To change the TUN mode settings, do the following:

- To change the TUN mode service type, select the **UDP** or **TCP** radio button.

The default protocol for TUN mode is UDP.

- To change the TUN mode service port, type the port number that you want to use in the field.

The default port number for TUN mode is 12973. The TUN port number is used in the `.ovpn` file of the OpenVPN configuration software package for Mac and non-Windows clients.

7. To change the TAP mode settings, do the following:

- To change the TAP mode service type, select the **UDP** or **TCP** radio button. The default protocol for TAP mode is UDP.

- To change the TAP mode service port, type the port number that you want to use in the field.

The default port number for TAP mode is 12974. The TAP port number is used in the `.ovpn` file of the OpenVPN configuration software package for Windows clients.

8. Click the **Apply** button.

Your changes are saved. VPN is enabled in the router, but you must install and set up OpenVPN software on your device before you can use a VPN connection.

## Install OpenVPN software on a VPN client

You must install OpenVPN software on each Windows-based computer, Mac computer, iOS device, and Android device that you plan to use for VPN connections to your router. Each computer or device is called a VPN client.

The software consists of the application software and the configuration files:

- Download and install the application software from the link that is provided in each client-specific section.
- Download and install the configuration files from the router as described in each client-specific section. The configuration files provide the correct router configuration information for the client utility. You must download the configuration files *after* you enable and configure OpenVPN service in the router (see [Enable OpenVPN service in the router](#) on page 197).

**Note:** If you later change the OpenVPN configuration in the router (for example, you change the TUN or TAP port number), you must download and install the `.ovpn` configuration file again on each client, depending on its operating system. If you change the TUN port number in the router, the `.ovpn` configuration file for Mac and non-Windows clients changes. If you change the TAP port number in the router, the `.ovpn` configuration file for Windows clients changes.

## Install OpenVPN software on a Windows-based computer

You must install both the OpenVPN client utility and OpenVPN configuration files on each Windows-based computer where you want to use a VPN connection to your router.

### **To download and install the OpenVPN client utility and OpenVPN configuration files on a Windows-based computer:**

1. To download the OpenVPN client utility on your Windows-based computer, visit [openvpn.net/community-downloads/](https://openvpn.net/community-downloads/).
2. Select the Windows package with the installer files.  
In most situations, you can download the Windows 32-bit or Windows 64-bit installer files, depending on your Windows operating system.
3. Download and install the OpenVPN client utility on your computer.  
You need to have administrative privileges.
4. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
5. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
6. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
7. Select **ADVANCED > Advanced Setup > VPN Service**.  
The VPN Service page displays.
8. Make sure that the **Enable VPN Service** check box is selected.

For more information about the VPN configuration for the router, see [Enable OpenVPN service in the router](#) on page 197.

9. Click the **FOR WINDOWS** button to download the OpenVPN configuration files to your Windows-based computer.
10. Unzip the OpenVPN configuration files and copy them to the folder in which you installed the OpenVPN client utility.
11. Modify the VPN interface name to **NETGEAR-VPN**:
  - a. If your computer is running Windows 10, select **Control Panel > Network and Sharing Center > Change adapter settings**.  
If your computer is running another Windows version, find the page that lets you change the adapter settings.
  - b. In the local area connection list, find the local area connection with the device name **TAP-Windows Adapter**.
  - c. Select the local area connection and change its name (*not* its device name) to **NETGEAR-VPN**.  
If you do not change the VPN interface name, the VPN tunnel connection will fail.

You can now open a VPN tunnel to the router.

For more information about installing and using OpenVPN on your Windows-based computer, visit <https://openvpn.net/community-resources/how-to/#quick>.

## Install OpenVPN software on a Mac computer

You must install both the Tunnelblick OpenVPN client utility and OpenVPN configuration files on each Mac computer where you want to use a VPN connection to your router.

### **To download and install the Tunnelblick OpenVPN client utility and OpenVPN configuration files on a Mac computer:**

1. To download the Tunnelblick OpenVPN client utility on your Mac computer, visit <https://tunnelblick.net/downloads.html>.
2. Download and install the Tunnelblick OpenVPN client utility on your Mac computer. You need to have administrative privileges.
3. Launch a web browser from the Mac computer, which must be connected to your Orbi network.
4. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

5. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
6. Select **ADVANCED > Advanced Setup > VPN Service**.  
The VPN Service page displays.
7. Make sure that the **Enable VPN Service** check box is selected.  
For more information about the VPN configuration for the router, see [Enable OpenVPN service in the router](#) on page 197.
8. Click the **FOR MAC OS X** button to download the OpenVPN configuration files to your Mac computer.
9. Unzip the OpenVPN configuration files and copy them to the folder in which you installed the Tunnelblick OpenVPN client utility.

You can now open a VPN tunnel to the router.

For more information about installing and using OpenVPN on your Mac computer, visit <https://openvpn.net/vpn-server-resources/installation-guide-for-openvpn-connect-client-on-macos/>.

## Install OpenVPN software on an iOS device

You must install both the OpenVPN Connect app and OpenVPN configuration files on each iOS device where you want to use a VPN connection to your router.

### **To download and install the OpenVPN Connect app and OpenVPN configuration files on an iOS device:**

1. On your iOS device, download and install the OpenVPN Connect app from the Apple app store.
2. Launch a web browser from a computer or your iOS device that is connected to the router network.
3. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

4. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > VPN Service**.  
The VPN Service page displays.
6. Make sure that the **Enable VPN Service** check box is selected.  
For more information about the VPN configuration for the router, see [Enable OpenVPN service in the router](#) on page 197.
7. Click the **FOR SMART PHONE** button to download the router's OpenVPN configuration files to your computer or iOS device.  
If you download the configuration files to your computer, unzip the files, and send them your iOS device.
8. On your iOS device, do the following:
  - a. Open the .ovpn file.
  - b. If the OpenVPN Connect app does not start automatically, a list of apps might display: Select the OpenVPN Connect app.
  - c. Install the .ovpn file.

You can now open a VPN tunnel to the router.

For more information about installing and using OpenVPN on your iOS device, visit [https://www.vpngate.net/en/howto\\_openvpn.aspx#ios](https://www.vpngate.net/en/howto_openvpn.aspx#ios).

## Install OpenVPN software on an Android device

You must install both the OpenVPN Connect app and OpenVPN configuration files on each Android device where you want to use a VPN connection to your router.

### **To download and install the OpenVPN Connect app and OpenVPN configuration files on an Android device:**

1. On your Android device, download and install the OpenVPN Connect app from the Google Play Store.
2. Launch a web browser from a computer or your Android device that is connected to the router network.
3. Enter **orbilogin.com**.  
A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

4. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > VPN Service**.

The VPN Service page displays.

6. Make sure that the **Enable VPN Service** check box is selected.

For more information about the VPN configuration for the router, see [Enable OpenVPN service in the router](#) on page 197.

7. Click the **FOR SMART PHONE** button to download the router's OpenVPN configuration files to your computer or Android device.

If you download the configuration files to your computer, unzip the files, and send them your Android device.

8. On your Android device, open the `.ovpn` file and import it into the OpenVPN Connect app.

You can now open a VPN tunnel to the router.

For more information about using OpenVPN on your Android device, visit [https://www.vpngate.net/en/howto\\_openvpn.aspx#android](https://www.vpngate.net/en/howto_openvpn.aspx#android).

## Use VPN to access your Internet service at your business

When you are away from your business and you access the Internet, you usually use a local Internet service provider. For example, in a hotel you might be given a code that lets you use the hotel's Internet service account to access the web.

Orbi Pro lets you use a VPN connection to access your own Internet service when you are away from your business. You might want to do this if you travel to a geographic location that does not support all the Internet services that you use at your business. For example, you might have Internet subscriptions to applications that work at your business location but not in a different country.

## Allow VPN client Internet access in the router

By default, the router is set up to allow VPN connections only to your business network (referred as the home network in the following procedure), but you can change the settings to allow Internet access. Accessing the Internet remotely through a VPN might be slower than accessing the Internet directly.

### To allow VPN clients to use your business Internet service:

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.  
The VPN Service page displays.
5. Make sure that the **Enable VPN Service** check box is selected.  
For more information about the VPN configuration for the router, see [Enable OpenVPN service in the router](#) on page 197.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **All sites on the Internet & Home Network** radio button.  
When you access the Internet with the VPN connection, instead of using a local Internet service, you use the Internet service from your business network.
7. Click the **Apply** button.  
Your settings are saved.

## Block VPN client Internet access in the router

By default, the router is set up to allow VPN connections only to your business network (referred as the home network in the following procedure), not to the Internet service for your business network. If you changed this setting to allow Internet access, you can change it back.

**To allow VPN clients to access *only* your business network and block them from using your business Internet service:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
2. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
3. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.  
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.  
The VPN Service page displays.
5. Make sure that the **Enable VPN Service** check box is selected.  
For more information about the VPN configuration for the router, see [Enable OpenVPN service in the router](#) on page 197.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **Home Network only** radio button.  
This is the default setting. The VPN connection is only to your business network, not to the Internet service for your business network.
7. Click the **Apply** button.  
Your settings are saved.

# 13

## Troubleshooting

---

This chapter provides information to help you diagnose and solve problems you might experience with your Orbi router or satellite. If you do not find the solution here, check the NETGEAR support site at [support.netgear.com](http://support.netgear.com) for product and contact information.

This chapter includes the following sections:

- [Quick tips](#)
- [The router and satellite do not sync](#)
- [You cannot log in to the router](#)
- [You cannot access the Internet](#)
- [Troubleshoot Internet browsing](#)
- [Troubleshoot PPPoE](#)
- [Troubleshoot WiFi connectivity](#)
- [Troubleshoot your network using the ping utility](#)

## Quick tips

This section describes tips for troubleshooting some common problems.

### Sequence to restart your network

When you restart your network, follow this sequence:

1. Turn off *and* unplug the modem.
2. Turn off the router.
3. Plug in the modem and turn it on. Wait two minutes.
4. Turn on the router and wait two minutes.

### WiFi settings

Make sure that the WiFi settings in the WiFi-enabled computer or mobile device and the router match.

The WiFi network name (SSID) and WiFi security settings must match exactly.

If you set up an access list, you must add each WiFi-enabled computer or mobile device's MAC address to the router's access list.

### Network settings

Make sure that the network settings of the computer are correct. Wired and wirelessly connected computers must use network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP.

Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address on the Attached Devices page.

## The router and satellite do not sync

If you experience difficulty syncing the router and the satellite, we recommend that you move the satellite into the same room as the router during the sync. Then move the satellite to a different location.

### To sync the router and the satellite:

1. Place the satellite in the same room as the Orbi Pro router.  
Use this satellite location only during the sync process.
2. Connect the satellite to a power source.
3. If the Power LED on the back of the satellite does not light and your satellite provides a **Power On/Off** button, press the button.  
Some models provide a **Power On/Off** button.
4. Wait for the satellite's bar LED to light solid white or magenta.
5. Press the **Sync** button on the router and then within two minutes, press the **Sync** button on the satellite.
6. Wait for the satellite to sync with the router.  
The satellite's bar LED pulses white while it attempts to sync with the router. After the LED bar pulses white, it lights one of the following colors for about three minutes and then turns off:
  - **Blue:** The Orbi router and satellite successfully synced, and the connection between the router and satellite is good.
  - **Amber:** The Orbi router and satellite successfully synced, but the connection between the router and satellite is only fair. Consider moving the Orbi satellite closer to the Orbi router.
  - **Magenta:** The Orbi router and satellite did not sync.
7. Do one of the following:
  - **The sync failed:** If the sync failed, try to sync again by repeating [Step 5](#) and [Step 6](#). If the sync keeps failing, try a different location or position.
  - **The sync is successful:** If the sync is successful, move the satellite to the location where you want to install it and continue with [Step 8](#).
8. At the new location, connect the satellite to a power source.
9. At the new location, resync the satellite with the router by repeating [Step 5](#) and [Step 6](#).  
If the satellite's bar LED lights blue or amber, the satellite synced successfully. If the satellite's bar LED lights blue, the connection is good. If the satellite's bar LED lights amber, consider moving the satellite closer to the router so that you can get a good connection instead of a fair connection.

10. If the satellite's bar LED lights magenta, the satellite did not resync with the router. If they successfully synced when they were placed in the same room, do one of the following:
- Move the satellite closer to the router and try again. The router must be within the satellite's WiFi coverage area for a good or fair connection to the satellite.
  - Place another satellite between the router and the satellite that you are trying to sync. Then try to sync between the two satellites. With daisy chain networking, your satellites can connect to each other or to the router, depending on which connection is best.

## You cannot log in to the router

Make sure that your computer or mobile device is connected to the Orbi WiFi network. If you do not want to use a WiFi connection, you can connect your computer to the Orbi router with an Ethernet cable.

If you changed the admin password and you forgot what it is, see [Reset the admin password](#) on page 149.

## You cannot access the Internet

Check your network and Internet connections:

1. Make sure that your WiFi-enabled computer or mobile device is connected to the Orbi network.
2. If you are connected to Orbi but you cannot access the Internet, check to see if your Internet connection is working.
3. Launch a web browser from a computer or mobile device that is connected to your Orbi network.
4. Enter **orbilogin.com**.  
A login window displays.  
If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.
5. Enter the admin user name and password.  
The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

6. Click the **ADVANCED** tab.

The ADVANCED Home page displays.

7. Check that an IP address is shown for the Internet port.

If 0.0.0.0 is shown, your router did not obtain an IP address from your Internet service provider (ISP).

If your router cannot obtain an IP address from the ISP, you can force your cable or DSL modem to recognize your new router by restarting your network. For more information, see [Sequence to restart your network](#) on page 207.

If your router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your Internet service provider (ISP) might require a login program. Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- 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 on the Internet Setup page.
- If your ISP allows only one Ethernet MAC address to connect to 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 your router to clone your computer's MAC address.

## Troubleshoot Internet browsing

If your router can obtain an IP address but your computer is unable to load any web pages from the Internet, it might be for one of the following reasons:

- The traffic meter is enabled, and the limit was reached.  
By configuring the traffic meter not to block Internet access when the traffic limit is reached, you can resume Internet access (see [Unblock the traffic meter after the traffic limit is reached](#) on page 161). If your ISP sets a usage limit, they might charge you for the overage.
- Your computer might not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses.

Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, restart your computer. Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.

- The router might not be configured as the default gateway on your computer. Reboot the computer and verify that the router address (orbilogin.com) is listed by your computer as the default gateway address.
- You might be running login software that is no longer needed. If your ISP provided a program to log you in to the Internet, you no longer need to run that software after installing your router.

## Troubleshoot PPPoE

If you are using PPPoE, try troubleshooting your Internet connection.

### **To troubleshoot a PPPoE connection:**

1. Launch a web browser from a computer or mobile device that is connected to your Orbi network.

2. Enter **orbilogin.com**.

A login window displays.

If your browser does not display a login window but displays a security warning and does not let you proceed, see [What to do if you get a browser security warning](#) on page 29.

3. Enter the admin user name and password.

The user name is **admin**. The password is the one that you set the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Click the **ADVANCED** tab.

The ADVANCED Home page displays.

5. In the Internet Port pane, click the **Connection Status** button.

The Connection Status window opens.

6. Check the Connection Status window to see if your PPPoE connection is active and working.

If the router is not connected, click the **Connect** button.

The router continues to attempt to connect indefinitely.

7. If you cannot connect after several minutes, the router might be set up with an incorrect service name, user name, or password, or your ISP might be experiencing a provisioning problem.

Unless you connect manually, the router does not authenticate using PPPoE until data is transmitted to the network.

## Troubleshoot WiFi connectivity

If you are experiencing trouble connecting to the Orbi WiFi network, try to isolate the problem:

- Does the WiFi-enabled computer or mobile device that you are using find your WiFi network?  
If you disabled the router's SSID broadcast, then your WiFi network is hidden and does not display in the list of networks that your computer or WiFi device finds. (By default, SSID broadcast is enabled.)
- Does your WiFi-capable device support the security that you are using for your WiFi network (WPA2 or WPA3)?
- To view the WiFi settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router, and select **BASIC > Wireless**.

**Note:** Be sure to click the **Apply** button if you change settings.

- If you are trying to connect to the 5 GHz band, does your WiFi-enabled computer or mobile device support this standard?
- Did your computer or WiFi device automatically connect to a different WiFi network in your area, such as a WiFi hotspot?

## Troubleshoot your network using the ping utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a network using the ping utility in your computer or workstation.

## 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 toolbar, click the **Start** button and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

**ping orbilogin.com**

3. Click the **OK** button.

You should see a message like this one:

```
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, you might be experiencing one of the following problems:

- Wrong physical connections  
For a wired connection, make sure that the numbered LAN port LED is lit for the port to which you are connected.  
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 address for your router and your computer are correct and that the addresses are on the same subnet.

## Test the path from your computer to a remote device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

### To test the path from a Windows-based computer to a remote device:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the Windows Run window, type:

**ping -n 10** <IP address>

where <IP address> is the IP address of a remote device such as your ISP DNS server.

If the path is functioning correctly, messages display that are similar to those shown in [Test the LAN path to your router](#) on page 213.

If you do not receive replies, check the following:

- Check to see that the IP address of your router is listed as the default gateway for your computer. If DHCP assigns the IP configuration of your computers, this information is not visible in your computer Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
- Check to see that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name on the Internet Setup page.
- Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers.

Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem. Some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If your ISP does this, configure your router to “clone” or “spoof” the MAC address from the authorized computer.

# A

## How to Use VLANs in Your Network

---

On an Orbi Pro WiFi 6 router, you can manually configure a VLAN by creating a VLAN profile (basically, and VLAN ID with a VLAN name) and assigning the VLAN to one or more network interfaces, such as WiFi networks (also referred to as WLAN or SSIDs) and Ethernet ports. Or, you can use an Orbi Pro WiFi 6 preset VLAN for which you can edit the settings to suit your network needs.

The following table shows the preset VLANs and their designated uses.

Table 8. Preset VLAN profiles and their designated uses

| VLAN ID | VLAN Profile Name | LAN ID | Ethernet Ports                 | WLAN Name    | WLAN Usage      |
|---------|-------------------|--------|--------------------------------|--------------|-----------------|
| 1       | Default           | LAN 1  | All LAN ports and the WAN port | Wireless 1   | admin access    |
| 20      | Employee          | LAN 2  | None assigned                  | Wireless 2   | Employee access |
| 30      | IoT               | LAN 3  | None assigned                  | Wireless 3   | IoT access      |
| 40      | Guest             | LAN 4  | None assigned                  | Guest Portal | Guest access    |

If you need a different type of VLAN, you can create your own VLAN profile according to your requirements.

This appendix includes two use cases for VLAN configuration:

- [VLAN use case 1: Orbi Pro WiFi 6 router in a home environment](#)
- [VLAN use case 2: Orbi Pro WiFi 6 router in a business environment](#)

# VLAN use case 1: Orbi Pro WiFi 6 router in a home environment

This use case describes how to configure the VLANs on an Orbi Pro WiFi 6 router and satellite in a home environment. Almost all settings that you need for this configuration are already preset on the Orbi Pro WiFi 6 router and satellite. The satellite is connected to the router over a WiFi backhaul.

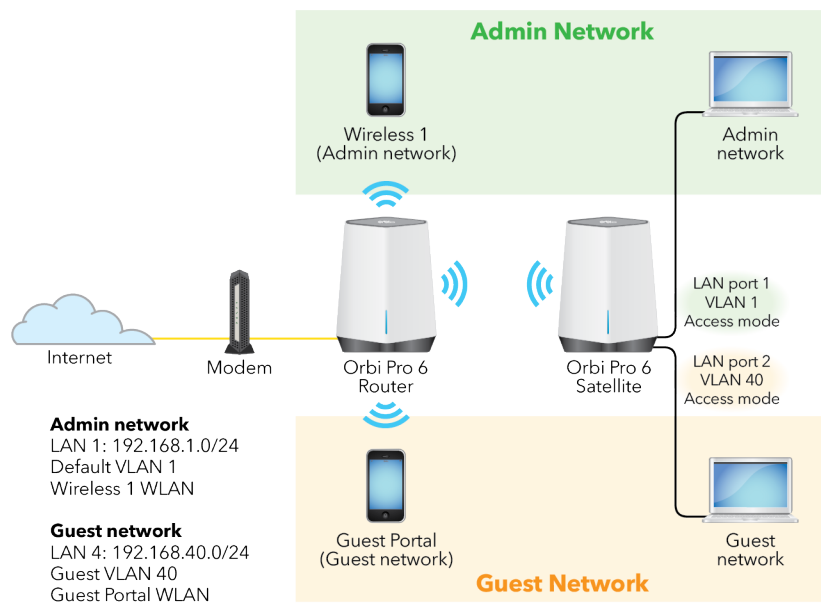


Figure 8. Orbi Pro WiFi 6 router as a router in a home environment

The procedure in this section does the following:

- Uses the LAN 1, preset Default VLAN 1, Wireless 1 WLAN, and the satellite's LAN 1 port for the Admin network.
- Sets the LAN 4, preset Guest VLAN 40, Guest Portal WLAN, and the satellite's LAN 2 port for the Guest network.
- Sets the port mode for the following LAN ports to Access mode:
  - **Satellite's LAN port 1.** This port is cabled to a desktop that is used for admin tasks such as accessing the router web interface.
  - **Satellite's LAN port 2.** This port is cabled to a desktop that is available to guests.

**Note:** LANs (networks) and LAN *ports* are two different concepts. By default, all LAN ports and the WAN port on the router and all LAN ports on any connected satellites are Ethernet ports in the same physical network segment (LAN 1) and members of VLAN 1. However, you can assign a LAN port to a different VLAN.

**To configure your Orbi Pro WiFi 6 router and satellite with a guest network that is separate from your admin network:**

1. Configure the VLANs on the router.

If you use the preset VLANs, you do not need to configure any VLANs. This sample configuration uses the Default VLAN with ID 1 and the Guest VLAN with ID 40, both of which are preset VLANs.

If you prefer to use custom VLANs, create the VLANs on the router (see [Add a new VLAN profile](#) on page 74).

2. Configure the WiFi networks on the router.

If you use the preset WiFi networks, you do not need to configure any WiFi networks. This sample configuration uses the Wireless 1 WLAN (assigned to VLAN 1) and the Guest Portal WLAN (assigned to VLAN 40), both of which are default WLANs.

If you prefer to use other WLAN names or assign WLANs to other VLANs, change the configuration for one or more existing WLANs (see [Manage the WiFi Networks](#) on page 85).

**Note:** The router and satellite share the same WiFi settings. After you configure or change these settings on the router, the settings are automatically synced with the satellite.

3. Change the VLAN for the LAN 2 port on the satellite.

In this sample configuration, the satellite's LAN 2 port is cabled to a desktop that is used for guest access. For the LAN port 2, change the VLAN to the Guest VLAN with ID 40 (see [Change the VLAN profile for an Ethernet port](#) on page 82).

By default, all LAN ports are assigned to VLAN 1, the default VLAN. That means that you do not need to change the VLAN for the satellite's LAN 1 port. In this sample configuration, this port is part of the Admin network.

4. Change the port mode for the satellite's LAN 1 and LAN 2 ports.

By default, the port mode for any LAN port is Trunk mode. In this sample configuration, the satellite's LAN 1 and LAN 2 ports are cabled to end devices (desktops). Therefore, change the port mode for these ports to Access mode (see [Port mode: Trunk mode or Access mode](#) on page 83).

## VLAN use case 2: Orbi Pro WiFi 6 router in a business environment

This use case describes how to configure the VLANs on an Orbi Pro WiFi 6 router and satellite in a business environment. Many of the settings that you need for this configuration are already preset on the Orbi Pro WiFi 6 router and satellite, but not on your network router and switch. In this use case, the Orbi Pro 6 satellite is connected to the Orbi Pro WiFi 6 router over an Ethernet cable, but you could also use a WiFi backhaul.

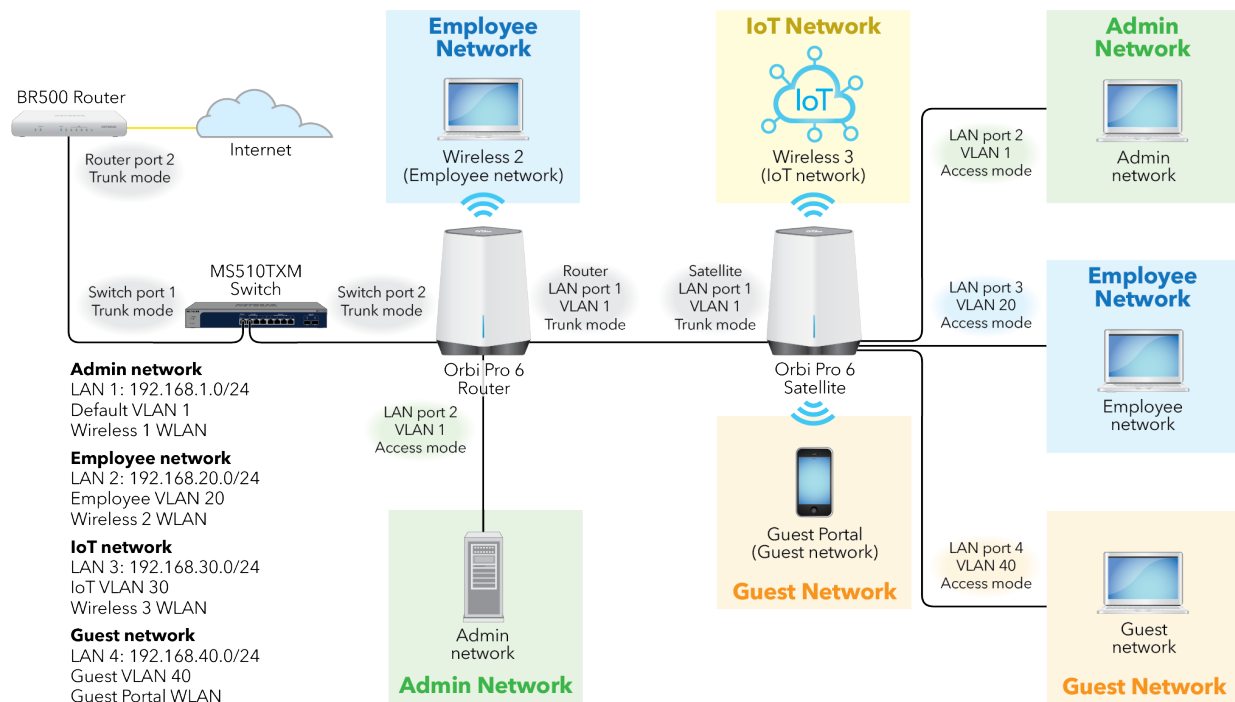


Figure 9. Orbi Pro WiFi 6 router in a business environment

The procedure in this section configures the network router and switch with the VLANs and LANs that you use on the Orbi Pro WiFi 6 system, and then does the following on the Orbi Pro WiFi 6 router and satellite:

- Uses the LAN 1, preset Default VLAN 1, Wireless 1 WLAN, the router's LAN 2 port, and the satellite's LAN 2 port for the Admin network.
- Sets the LAN 2, preset Employee VLAN 20, Wireless 2 WLAN, and the satellite's LAN 3 port for the Employee network.
- Uses the LAN 3, preset IoT VLAN 30, and Wireless 3 WLAN for the Internet of things (IoT) network.
- Sets the LAN 4, preset Guest VLAN 40, Guest Portal WLAN, and the satellite's LAN 4 port for the Guest network.

- Sets the port mode for the following LAN ports to Access mode:
  - **Router LAN port 2.** This port is cabled to a desktop that is used for admin tasks such as accessing the router web interface.
  - **Satellite LAN port 2.** This port is cabled to a desktop that is also used for admin tasks.
  - **Satellite LAN port 3.** This port is cabled to a desktop that is used by an employee.
  - **Satellite LAN port 4.** This port is cabled to a desktop that is available to guests.

**Note:** LANs (networks) and LAN *ports* are two different concepts. By default, all LAN ports and the WAN port on the router and all LAN ports on any connected satellites are Ethernet ports in the same physical network segment (LAN 1) and members of VLAN 1. However, you can assign a LAN port to a different VLAN.

### **To configure your network router and switch and your Orbi Pro WiFi 6 router and satellite with secure employee, IoT, and guest networks:**

1. Create the following VLANs on your network router:
  - Add VLAN 20 with the name Employee, and add all ports as tagged members.
  - Add VLAN 30 with the name IoT, and add all ports as tagged members.
  - Add VLAN 40 with the name Guest, and add all ports as tagged members.
2. Create the following LAN subnets on your network router:
  - Add LAN 2 with subnet 192.168.20.0/24, make LAN 2 a member of VLAN 20 (the Employee VLAN), and enable the DHCP server for LAN 2.
  - Add LAN 3 with subnet 192.168.30.0/24, make LAN 3 a member of VLAN 30 (the IoT VLAN), and enable the DHCP server for LAN 3.
  - Add LAN 4 with subnet 192.168.40.0/24, make LAN 4 a member of VLAN 40 (the Guest VLAN), and enable the DHCP server for LAN 4.
3. Create the following VLANs on your network switch:
  - Add VLAN 20 with the name Employee. As tagged members of VLAN 20, add the switch port (port 1 in the diagram) that is cabled to the network router as a trunk port, and do the same for the switch port (port 2 in the diagram) that is cabled to the Orbi Pro WiFi 6 router.
  - Add VLAN 30 with the name IoT. As tagged members of VLAN 30, add the switch port (port 1 in the diagram) that is cabled to the network router as a trunk port, and do the same for the switch port (port 2 in the diagram) that is cabled to the Orbi Pro WiFi 6 router.

- Add VLAN 40 with the name Guest. As tagged members of VLAN 40, add the switch port (port 1 in the diagram) that is cabled to the network router as a trunk port, and do the same for the switch port (port 2 in the diagram) that is cabled to the Orbi Pro WiFi 6 router.

4. Configure the VLANs on the Orbi Pro WiFi 6 router.

If you use the preset VLANs, you do not need to configure any VLANs. This sample configuration uses the Default VLAN with ID 1, the Employee VLAN with ID 20, the IoT VLAN with ID 30, and the Guest VLAN with ID 40, all of which are preset VLANs.

If you prefer to use custom VLANs, create the VLANs on the router (see [Add a new VLAN profile](#) on page 74).

5. Configure the WiFi networks on the Orbi Pro WiFi 6 router.

If you use the preset WiFi networks, you do not need to configure any WiFi networks. This sample configuration uses the Wireless 1 WLAN (assigned to VLAN 1), the Wireless 2 WLAN (assigned to VLAN 20), the Wireless 3 WLAN (assigned to VLAN 30), and the Guest Portal WLAN (assigned to VLAN 40), all of which are default WLANs.

If you prefer to use other WLAN names or assign WLANs to other VLANs, change the configuration for one or more existing WLANs (see [Manage the WiFi Networks](#) on page 85).

**Note:** The router and satellite share the same WiFi settings. After you configure or change these settings on the router, the settings are automatically synced with the satellite.

6. Change the VLANs for LAN ports on the Orbi Pro WiFi 6 satellite.

In this sample configuration, change the VLANs for the following satellite's LAN ports:

- **Satellite LAN 3 port:** Assign to the Employee VLAN with ID 20 because this port is cabled to a desktop that is used for employee access.
- **Satellite LAN 4 port:** Assign to the Guest VLAN with ID 40 because this port is cabled to a desktop that is used for guest access.

For more information, see [Change the VLAN profile for an Ethernet port](#) on page 82.

By default, all LAN ports are assigned to VLAN 1, the default VLAN. That means that you do not need to change the VLAN for the router's LAN 1 and LAN 2 ports and the satellite's LAN 1 and LAN 2 ports. In this sample configuration, all these ports are part of the Admin network (the default network):

- **Router LAN port 1:** Cabled to the satellite's LAN 1 port.
- **Router LAN port 2:** Cabled to a desktop that is used for admin access.

- **Satellite LAN port 1:** Cabled to the router's LAN 1 port.
  - **Satellite LAN port 2:** Cabled to a desktop that is used for admin access.
7. Change the port mode for LAN ports on the Orbi Pro WiFi 6 router and the satellite. By default, the port mode for any LAN port is Trunk mode. In this sample configuration, the router's LAN 2 port and the satellite's LAN 2, LAN 3, and LAN 4 ports are cabled to end devices (desktops). Therefore, change the port mode for these ports to Access mode (see [Port mode: Trunk mode or Access mode](#) on page 83).

Troubleshooting tips:

- If a WiFi device cannot get an IP address from the Orbi Pro WiFi 6 system, verify that the WiFi network is assigned to the correct VLAN.
- If a wired device cannot get an IP address from the Orbi Pro WiFi 6 system, verify that the Ethernet port is assigned to the correct VLAN and that LAN is assigned to the correct VLAN:

**Note:** If your Orbi Pro WiFi 6 router is in AP mode (the default operation mode is Router mode), only the LAN 1 settings work. The other LAN subnets do not work. However, in AP mode, the VLAN settings still apply to the WLANs, you can still assign an Ethernet port to another VLAN, and you can still change the port mode for an Ethernet port.

# B

## Supplemental Information

---

This appendix covers the following topics:

- [Factory settings](#)
- [Technical specifications](#)

# Factory settings

The following factory settings information are for the Orbi Pro WiFi 6 AX5400 router (model SXR50) and the Orbi Pro WiFi 6 AX5400 satellite (model SXS50).

You can return the Orbi Pro WiFi 6 AX5400 router or satellite to its factory settings. Use the end of a paper clip or a similar object to press and hold the **Reset** button on the back of the router or satellite for at least seven seconds. The router or satellite resets, and returns to the factory settings.

## Factory settings for Orbi Pro WiFi 6 AX5400 router model SXR50

The following table shows the factory default settings for the Orbi Pro WiFi 6 AX5400 router.

Table 9. Factory default settings for the router

| Feature                                     | Default Setting  |
|---|--|
| <b>Router web interface login</b>           |  |
| Login URL                                   | orbilogin.com  |
| Loign user name (case-sensitive)            | admin  |
| Default login password (case-sensitive)     | password   |
| <b>Internet connection</b>                  |  |
| WAN MAC address                             | Use default hardware address                                 |
| WAN MTU size                                | 1500   |
| Port speed                                  | AutoSensing  |
| DMZ   | Disabled   |
| Time zone                                   | GMT for WW, except NA and GR<br>GMT+1 for GR<br>GMT-8 for NA |
| Time zone adjusted for daylight saving time | Disabled   |
| <b>Local network 1 (LAN 1)</b>              |  |
| LAN 1 IP                                    | 192.168.1.1  |
| LAN 1 subnet mask                           | 255.255.255.0  |

Table 9. Factory default settings for the router (Continued)

| Feature                        | Default Setting                |
|--------------------------------|--------------------------------|
| LAN 1 DHCP server              | Enabled                        |
| LAN 1 DHCP range               | 192.168.1.2 to 192.168.1.254   |
| LAN 1 DHCP starting IP address | 192.168.1.2                    |
| LAN 1 DHCP ending IP address   | 192.168.1.254                  |
| <b>Local network 2 (LAN 2)</b> |                                |
| LAN 2 IP                       | 192.168.20.1                   |
| LAN 2 subnet mask              | 255.255.255.0                  |
| LAN 2 DHCP server              | Enabled                        |
| LAN 2 DHCP range               | 192.168.20.2 to 192.168.20.254 |
| LAN 2 DHCP starting IP address | 192.168.20.2                   |
| LAN 2 DHCP ending IP address   | 192.168.20.254                 |
| <b>Local network 3 (LAN 3)</b> |                                |
| LAN 3 IP                       | 192.168.30.1                   |
| LAN 3 subnet mask              | 255.255.255.0                  |
| LAN 3 DHCP server              | Enabled                        |
| LAN 3 DHCP range               | 192.168.30.2 to 192.168.30.254 |
| LAN 3 DHCP starting IP address | 192.168.30.2                   |
| LAN 3 DHCP ending IP address   | 192.168.30.254                 |
| <b>Local network 4 (LAN 4)</b> |                                |
| LAN 4 IP                       | 192.168.40.1                   |
| LAN 4 subnet mask              | 255.255.255.0                  |
| LAN 4 DHCP server              | Enabled                        |
| LAN 4 DHCP range               | 192.168.40.2 to 192.168.40.254 |
| LAN 4 DHCP starting IP address | 192.168.40.2                   |
| LAN 4 DHCP ending IP address   | 192.168.40.254                 |
| <b>Local network 5 (LAN 5)</b> |                                |
| LAN 5 IP                       | 192.168.50.1                   |

Table 9. Factory default settings for the router (Continued)

| Feature  | Default Setting  |
|--|--|
| LAN 5 subnet mask                                    | 255.255.255.0  |
| LAN 5 DHCP server                                    | Enabled  |
| LAN 5 DHCP range                                     | 192.168.50.2 to 192.168.50.254                         |
| LAN 5 DHCP starting IP address                       | 192.168.50.2   |
| LAN 5 DHCP ending IP address                         | 192.168.50.254   |
| <b>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)  |
| Source MAC filtering                                 | Disabled   |
| <b>WiFi</b>  |  |
| WiFi communication                                   | Enabled  |
| SSID name  | See router label                                       |
| Security   | WPA2-PSK (AES)   |
| Broadcast SSID                                       | Enabled  |
| Transmission speed                                   | Auto <sup>1</sup>                                      |
| Country/region                                       | United States in the US<br>Otherwise, varies by region |
| RF channel 2.4 GHz fronthaul                         | Auto   |
| RF channel 2.4 GHz backhaul                          | Auto   |
| RF channel 5 GHz fronthaul                           | Channel 48 for NA, AU, and CA<br>Channel 36 for EU     |
| RF channel 5 GHz backhaul                            | Channel 48 for NA, AU, and CA<br>Channel 36 for EU     |

<sup>1</sup> Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

## Factory settings for Orbi Pro WiFi 6 AX5400 satellite model SXS50

The satellite has the same factory settings as the router. The following table shows the default satellite web interface login settings.

Table 10. Factory default settings for the satellite

| Satellite Web Interface Login Settings  | Default Setting |
|---|-----------------|
| Default IP address (login URL)          | 192.168.1.250   |
| Login user name (case-sensitive)        | admin           |
| Default login password (case-sensitive) | password        |

## Technical specifications

The following are the technical specifications for Orbi Pro WiFi 6 AX5400 router (model SXR50) and Orbi Pro WiFi 6 AX5400 satellite (SXS50).

### Technical specifications for Orbi Pro WiFi 6 AX5400 router model SXR50

The following table shows the technical specifications for the router.

Table 11. Technical specifications for the router

| Feature                    | Description   |
|----------------------------|---|
| Data and routing protocols | TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, DDNS, and UPnP   |
| Power adapter              | North America: 120V, 60 Hz, input<br>UK, Australia: 240V, 50 Hz, input<br>Europe: 230V, 50 Hz, input<br>All regions (output): 12V, 3.5A DC output |
| Dimensions                 | 6.7 x 2.9 x 8.8 in (170 x 75.6 x 224.5 mm)  |
| Weight                     | 1.6 lb (0.72 kg)  |
| Operating temperature      | 0° to 40°C (32° to 104°F)   |
| Operating humidity         | 90% maximum relative humidity, noncondensing  |

Table 11. Technical specifications for the router (Continued)

| Feature  | Description  |
|--|--|
| WAN  | 1 Ethernet WAN port with an RJ-45 receptacle. The port supports 10BASE-T, 100BASE-TX, and 1000BASE-T.  |
| LAN  | 3 Ethernet LAN ports with RJ-45 receptacles. The ports support 10BASE-T, 100BASE-TX, and 1000BASE-T.   |
| WiFi   | Maximum wireless signal rate complies with the IEEE 802.11 standard. <sup>2</sup>  |
| Radio data rates                                 | 2.4 GHz: Max. 600 Mbps<br>5 GHz Low band: Max. 2400 Mbps<br>5 GHz High band: Max. 2400 Mbps  |
| Data encoding standards                          | Simultaneous Tri-band WiFi with QAM support:<br>Radio 1: IEEE 802.11b/g/n/ax 2.4 GHz - 256 QAM<br>Radio 2: IEEE 802.11a/n/ac/ax 5 GHz - 1024 QAM<br>Radio 3: IEEE 802.11a/n/ac/ax 5 GHz - 1024 QAM |
| Maximum number of computers per wireless network | Limited by the amount of WiFi network traffic generated by each node (typically 50-70 nodes)<br>2.4 GHz: 127<br>5 GHz (front haul): 127  |
| Operating frequency range 2.4 GHz (US)           | 2.412-2.462  |
| Operating frequency range 2.4 GHz (Europe ETSI)  | 2.412-2.472 GHz  |
| Operating frequency range 5 GHz (US)             | 5.18 GHz-5.24 GHz<br>5.745 GHz-5.825 GHz   |
| Operating frequency range 5 GHz (EU)             | 5.18 GHz-5.24 GHz<br>5.26 GHz-5.32 GHz<br>5.5 GHz-5.7 GHz  |
| 802.11 security                                  | WPA2-PSK [AES]<br>WPA-PSK [TKIP] + WPA2-PSK [AES]<br>WPA2-Enterprise<br>WPA3-Personal [SAE]<br>WPA3-Enterprise   |
| Electromagnetic emissions                        | FCC Part 15 Class B<br>VCCI Class B<br>EN 55 022 (CISPR 22), Class B C-Tick N10947   |

<sup>2</sup>Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

## Technical specifications for Orbi Pro WiFi 6 AX5400 satellite model SXS50

The following table shows the technical specifications for the satellite.

Table 12. Technical specifications for the satellite

| Feature  | Description  |
|--|--|
| Data and routing protocols                       | TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, DDNS, and UPnP  |
| Power adapter                                    | North America: 120V, 60 Hz, input<br>UK, Australia: 240V, 50 Hz, input<br>Europe: 230V, 50 Hz, input<br>All regions (output): 12V, 3.5A DC output  |
| Dimensions                                       | 6.7 x 2.9 x 8.8 in (170 x 75.6 x 224.5 mm)   |
| Weight   | 1.6 lb (0.72 kg)   |
| Operating temperature                            | 0° to 40°C (32° to 104°F)  |
| Operating humidity                               | 90% maximum relative humidity, noncondensing   |
| LAN  | 4 Ethernet LAN ports with RJ-45 receptacles.<br>The ports support 10BASE-T, 100BASE-TX, and 1000BASE-T.  |
| WiFi   | Maximum wireless signal rate complies with the IEEE 802.11 standard. <sup>3</sup>  |
| Radio data rates                                 | 2.4 GHz: Max. 600 Mbps<br>5 GHz Low band: Max. 2400 Mbps<br>5 GHz High band: Max. 2400 Mbps  |
| Data encoding standards                          | Simultaneous Tri-band WiFi with QAM support:<br>Radio 1: IEEE 802.11b/g/n/ax 2.4 GHz - 256 QAM<br>Radio 2: IEEE 802.11a/n/ac/ax 5 GHz - 1024 QAM<br>Radio 3: IEEE 802.11a/n/ac/ax 5 GHz - 1024 QAM |
| Maximum number of computers per wireless network | Limited by the amount of WiFi network traffic generated by each node (typically 50-70 nodes)<br>2.4 GHz: 127<br>5 GHz (front haul): 127  |
| Operating frequency range 2.4 GHz (US)           | 2.412-2.462  |
| Operating frequency range 2.4 GHz (Europe ETSI)  | 2.412-2.472 GHz  |
| Operating frequency range 5 GHz (US)             | 5.18 GHz-5.24 GHz<br>5.745 GHz-5.825 GHz   |

Table 12. Technical specifications for the satellite (Continued)

| Feature                              | Description  |
|--------------------------------------|--|
| Operating frequency range 5 GHz (EU) | 5.18 GHz-5.24 GHz<br>5.26 GHz-5.32 GHz<br>5.5 GHz-5.7 GHz  |
| 802.11 security                      | WPA2-PSK [AES]<br>WPA-PSK [TKIP] + WPA2-PSK [AES]<br>WPA2-Enterprise<br>WPA3-Personal [SAE]<br>WPA3-Enterprise |
| Electromagnetic emissions            | FCC Part 15 Class B<br>VCCI Class B<br>EN 55 022 (CISPR 22), Class B C-Tick N10947                             |

<sup>3</sup> *Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.*