Cisco Start
SIMPLE SMART SECURE

Cisco RV340 Series Security Router

Easy Setup Guide

You can easily set up
your RV340 Series Security Router
in this step-by-step guide

1. Connecting Equipment
2. Logging in & Changing Password
3. Using Initial Setup Wizard
4. Using VPN Setup Wizard
5. Using Application Control Wizard
6. Applying Configuration

1 Connecting Equipment

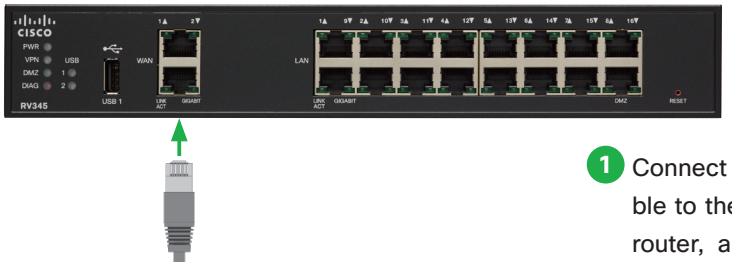
1-1 Before You Begin

Before you begin the installation, make sure that you have the following equipment:

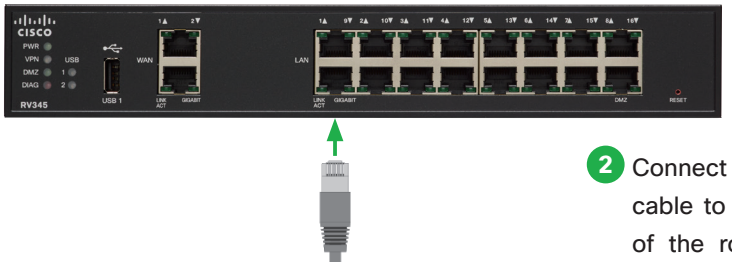
- RV340 Router (the router)
- Ethernet Cable x 2
- Power Adapter
- PC

Make sure that nothing is connected to the router and your PC settings are configured to use DHCP. And power off all equipment, including the cable or DSL modem, the computer, and the router.

1-2 Connecting Equipment

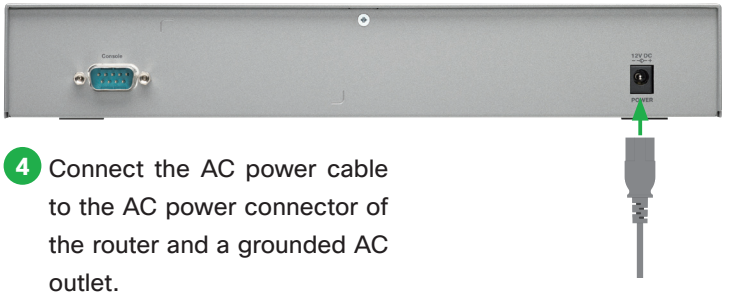


1 Connect the first Ethernet cable to the WAN port #1 of the router, and the other end of the cable to the Ethernet port of your WAN device.



2 Connect the second Ethernet cable to one of the LAN port of the router, and the other end of the cable to the Ethernet port of your PC.

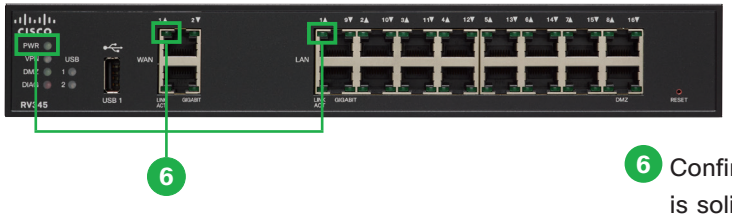
3 Power on the WAN device and wait until the connection is active.



4 Connect the AC power cable to the AC power connector of the router and a grounded AC outlet.

The power switch is on by default. The power light on the front panel is solid green when the power adapter is connected properly and the device is finished booting.

5 Power on the PC that you connected to one of the LAN port in step 2.



6 Confirm that the PWR LED is solid green and the port LEDs that you connected to the WAN device and the PC are green or blinking green.

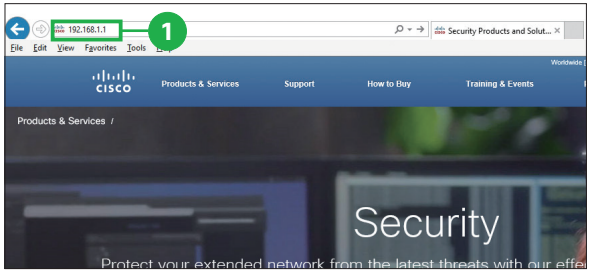
MEMO

During the system boot up, the PWR LED will progressively keep flashing until the system has fully booted. At start up, the PWR, LINK/ACT and GIGIBIT LEDs of LAN #1 will flash. At 25 % boot up, the PWR, LINK/ACT and GIGIBIT LEDs of LAN #1 and 2 will flash. At 50 % boot up, the PWR, LINK/ACT and GIGIBIT LEDs of LAN #1, #2 and #3 will flash. At 75% boot up, the PWR, LINK/ACT and GIGIBIT LEDs of LAN #1, #2, #3 and #4 will flash. The system boot time will be less than 3 minutes typically. If the router is fully configured with all feature configuration settings set to a maximum, it may take up to 7 minutes to fully boot the system.

2 Logging in & Changing Password

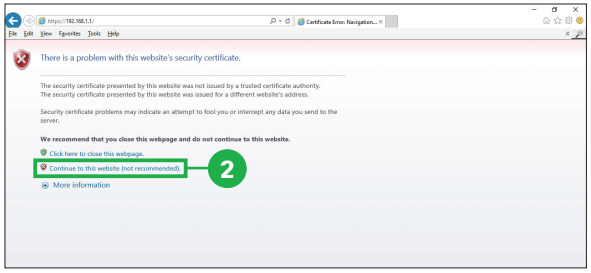
The router comes with default settings. However, your internet service provider (ISP) might require you to modify the settings. You can modify the settings using the Setup Wizard and Device Manager on your web browser such as Internet Explorer (version 10 and higher), Firefox, or Chrome (for PC) or Safari (for Mac).

Launch a web browser.



1 Launch a Web browser and enter the IP address "https://192.168.1.1" into the address bar, then press Enter key.

Depending on your environment, the security certificate page appears.

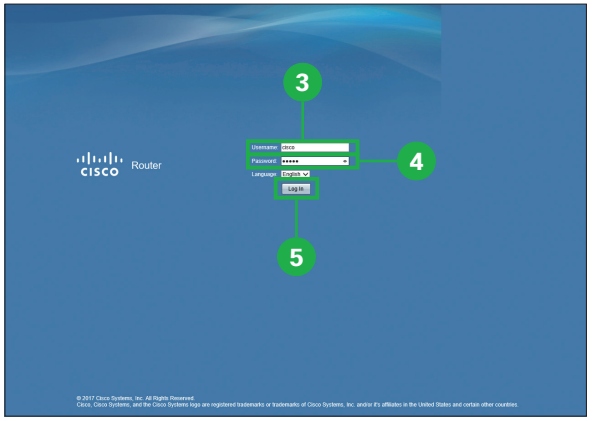


2 Click [Continue to this website (not recommended)].

Caution

If the log in page does not appear, make sure that:

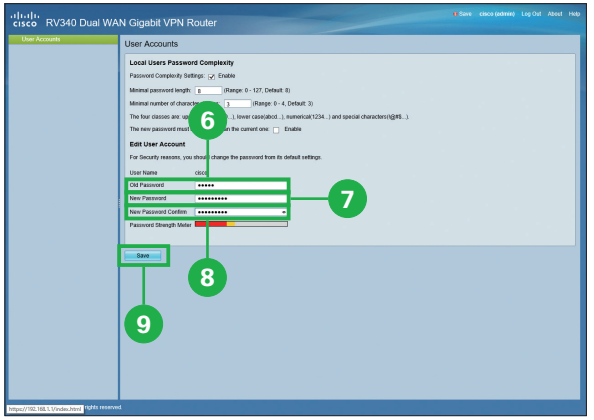
- The PWR LED is solid green and the port LEDs are green or blinking green.
- You connect a straight-through cable to an Ethernet port on the router.
- Any pop-up blockers or proxy settings on your browser are disabled and that any wireless client is disabled on your PC or laptop.
- Your PC settings use DHCP. The router acts as a DHCP server. If your PC has a static IP address, temporarily configure your PC settings to use DHCP.



3 Enter "cisco" in the [Username].

4 Enter "cisco" in the [Password].

5 Click [Log In].

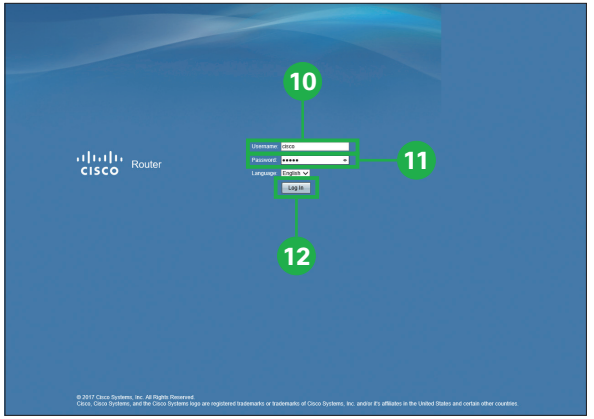


6 Enter "cisco" in the [Old Password].

7 Enter a password in the [New Password].

8 Enter it again in the [New Password Confirm].

9 Click [Save].



10 Enter "cisco" in the [Username].

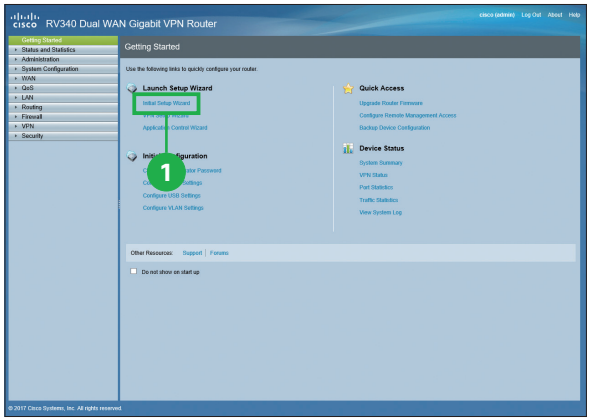
11 Enter a password in the [Password].

12 Click [Log In].

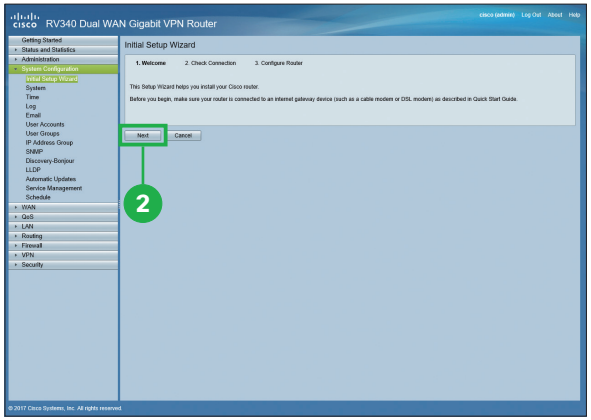
The Device Manager Getting Started page appears.

3 Using Initial Setup Wizard

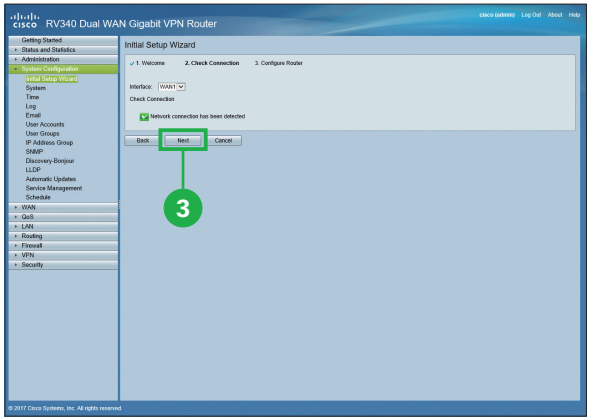
You can check the connection and configure the basic router settings on the Initial Setup Wizard page. Refer to your ISP for the information required to setup your Internet connection.



1 From the Getting Started page, Click [Initial Setup-Wizard].

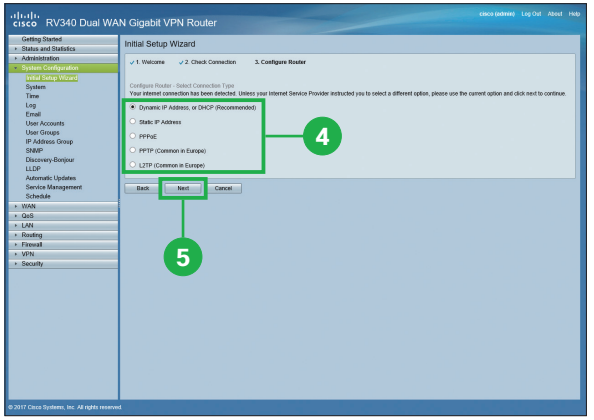


2 Click [Next].



3 Click [Next].

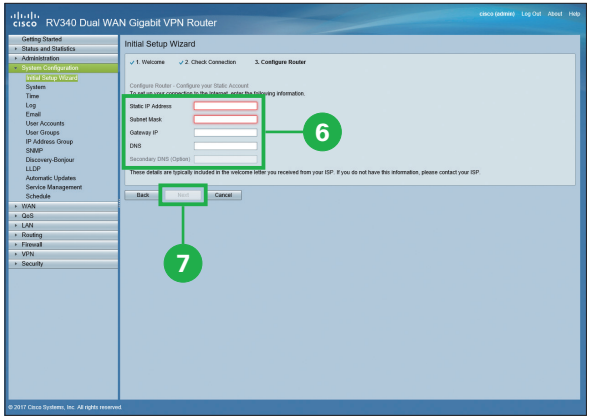
If your router has detected a connection, the connection details are displayed on this page.



4 Select your internet connection type.

5 Click [Next].

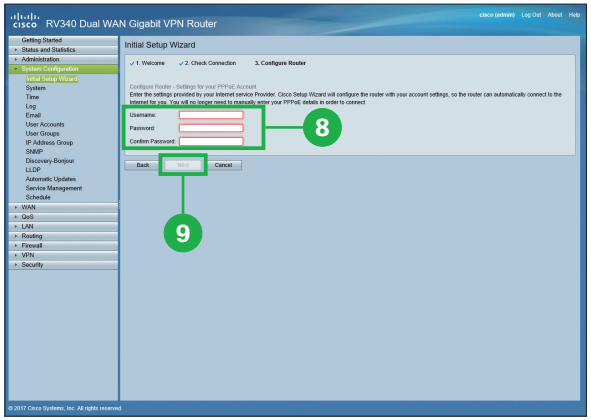
If you select [Dynamic IP Address, or DHCP (Recommended)], skip to 14.



6 If you select [Static IP Address], enter the required information.

7 Click [Next] and skip to 14.

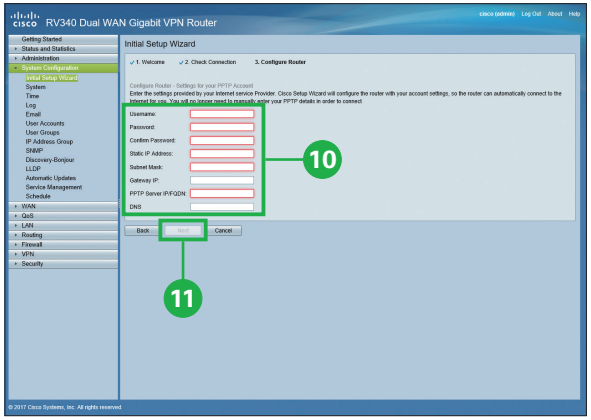
These details are typically included in the welcome letter you received from your ISP. If you do not have this information, please contact your ISP.



8 If you select [PPPoE], enter the required information.

9 Click [Next] and skip to **14**.

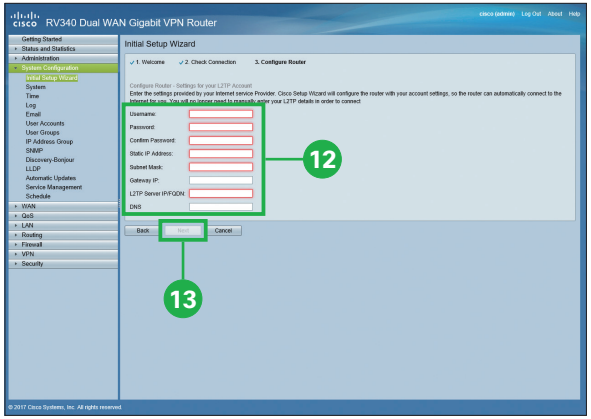
These details are typically included in the welcome letter you received from your ISP. If you do not have this information, please contact your ISP.



10 If you select [PPTP (Common in Europe)], enter the required information.

11 Click [Next] and skip to **14**.

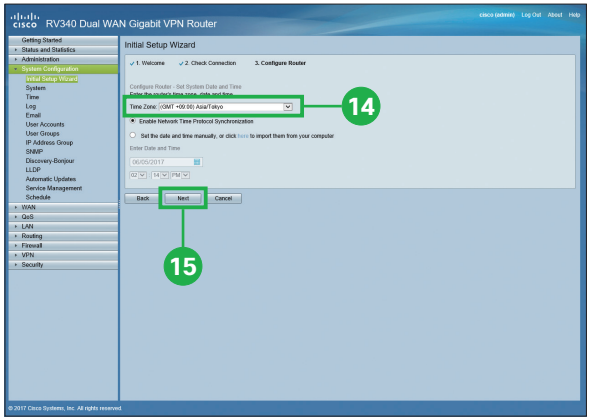
These details are typically included in the welcome letter you received from your ISP. If you do not have this information, please contact your ISP.



12 If you select [L2TP (Common in Europe)], enter the required information.

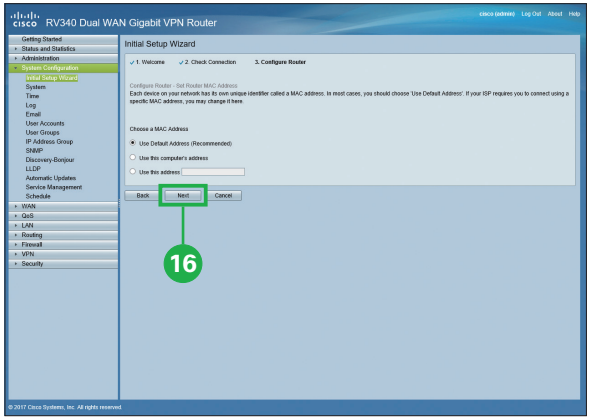
13 Click [Next].

These details are typically included in the welcome letter you received from your ISP. If you do not have this information, please contact your ISP.

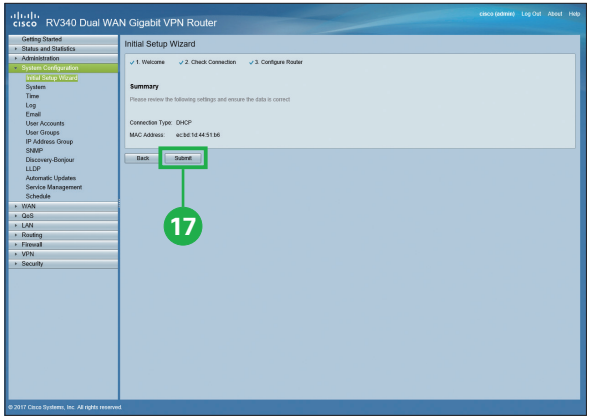


14 Select the router's time zone from the [Time Zone] drop down list.

15 Click [Next].



16 Click [Next].

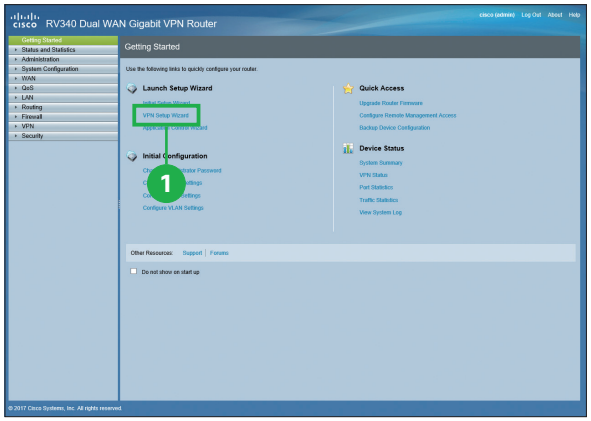


17 Click [Submit].

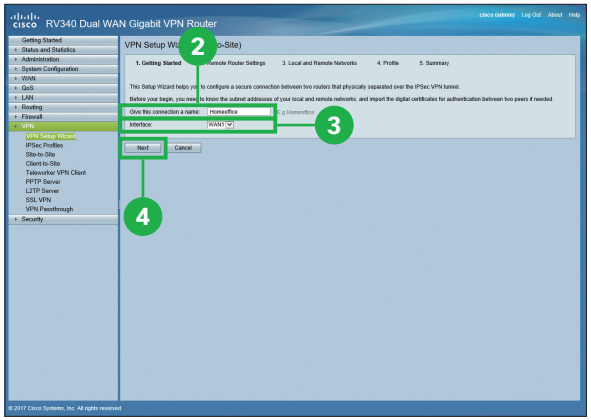
If you need to configure additional WAN settings, proceed to "Appendix 1, Additional WAN Settings".

4 Using VPN Setup Wizard

The VPN allows a remote host to act as if they were located on the same local network. The router supports 50 tunnels. The VPN Setup Wizard guides in configuring a secure connection for site-to-site IPSec tunnel. This simplifies the configuration by avoiding complex and optional parameters, so any user can set up the IPSec tunnel in a fast and efficient manner.



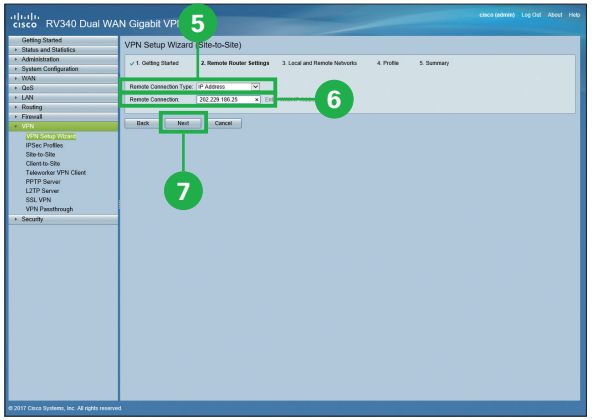
1 From the Getting Started page, Click [VPN Setup-Wizard].



2 Enter a connection name in the [Give this connection a name] field.

3 Select an interface from the drop-down list.

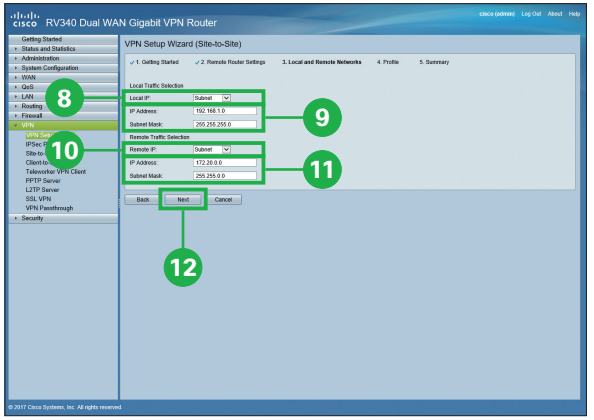
4 Click [Next].



5 Select the [Remote Connection Type] from the drop-down list.

6 If you select [IP Address], enter the IP Address, or if you select a [FQDN], enter the name.

7 Click [Next].



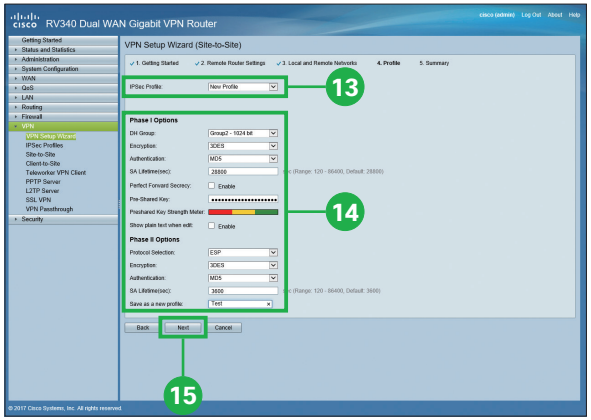
8 Select the [Local IP] from the drop-down list.

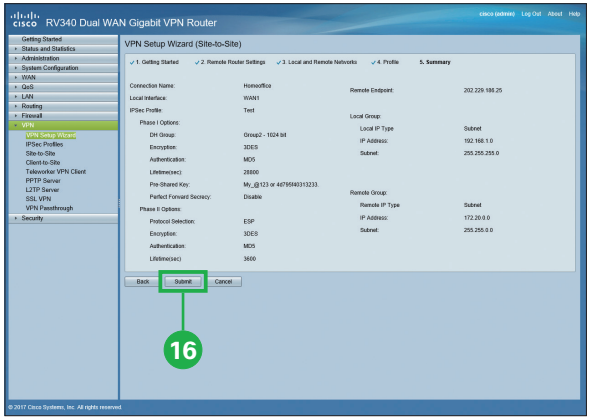
9 If you select [IP Address], enter the IP address, or if you select [Subnet], enter the IP address and subnet mask.

10 Select the [Remote IP] from the drop-down list.

11 If you select [IP Address], enter the IP address, or if you select [Subnet], enter the IP address and subnet mask.

12 Click [Next].





13 Select the [IPSec profile] from the drop-down list.

If you select [Default], skip to **15**.

14 If you select [New Profile], enter the required information.

Refer to the MEMO.

15 Click [Next].

16 Click [Submit].

MEMO: Phase 2 Options

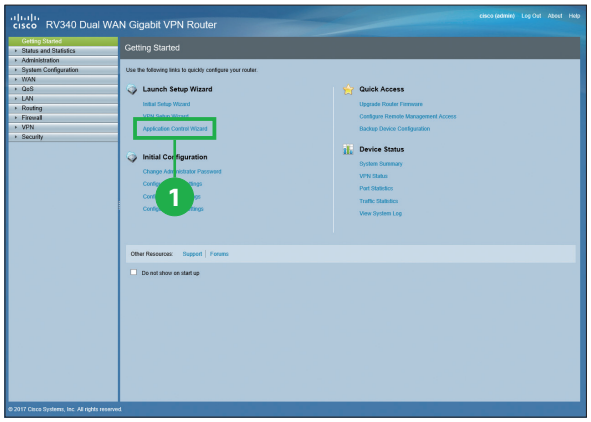
- **Diffie-Hellman (DH) Group**
  Select a DH group from the drop-down list. This is enabled only when Perfect Forward secrecy is enabled under Phase 1 Options.
- **Protocol Selection**
  Select a protocol from the drop-down list.
- **Encryption**
  Select an encryption option from the drop-down list.
- **Authentication**
  Select an authentication.
- **SA Lifetime (Sec)**
  Amount of time a VPN tunnel (IPSec SA) is active in this phase. The default value for Phase 2 is 3600 seconds.

MEMO: Phase 1 Options

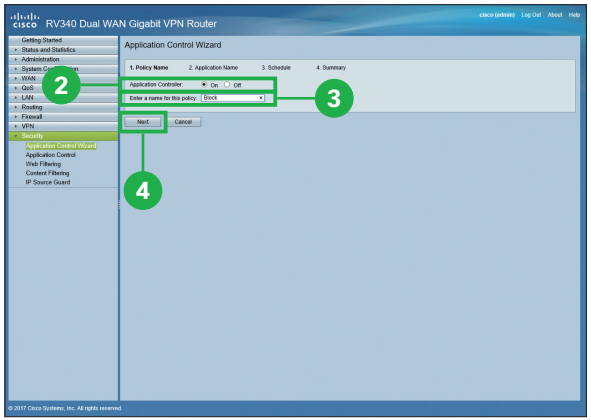
- **Diffie-Hellman (DH) Group**
  Select a DH group (**Group 2** or **Group 5**) from the drop-down list. DH is a key exchange protocol, with two groups of different prime key lengths: Group 2 has up to 1,024 bits, and Group 5 has up to 1,536 bits.
  For faster speed and lower security, choose Group 2. For slower speed and higher security, choose Group 5. Group 2 is selected by default.
- **Encryption**
  Select an encryption option (**3DES**, **AES-128**, **AES-192**, or **AES-256**) from the drop-down list. This method determines the algorithm used to encrypt or decrypt ESP/ISAKMP packets.
- **Authentication**
  The authentication method determines how the Encapsulating Security Payload Protocol (ESP) header packets are validated. The MD5 is a one-way hashing algorithm that produces a 128-bit digest. The SHA1 is a one-way hashing algorithm that produces a 160-bit digest. The SHA1 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method. Select an authentication (**MD5**, **SHA1** or **SHA2-256**).
- **SA Lifetime (Sec)**
  Amount of time an IKE SA is active in this phase. The default value for Phase 1 is 28,800 seconds.
- **Perfect Forward Secrecy (PFS)**
  Check **Enable** to enable PFS and enter the lifetime in seconds, or uncheck Enable to disable. When the PFS is enabled, the IKE Phase 2 negotiation generates a new key for the IPSec traffic encryption and authentication. Enabling this feature is recommended.
- **Pre-Shared Key**
  Pre-shared key to use to authenticate the remote IKE peer. You can enter up to 30 keyboard characters or hexadecimal values, such as **My_@123 or 4d795f40313233**. Both ends of the VPN tunnel must use the same Pre-shared Key.
  We recommend that you change the Pre-shared Key periodically to maximize VPN security.

5 Using Application Control Wizard

The application control enables you to restrict access to clients from certain designated unwanted applications. It can permit and log, or block access to applications based on the categories and names. It is also possible to schedule when the application control should be active.



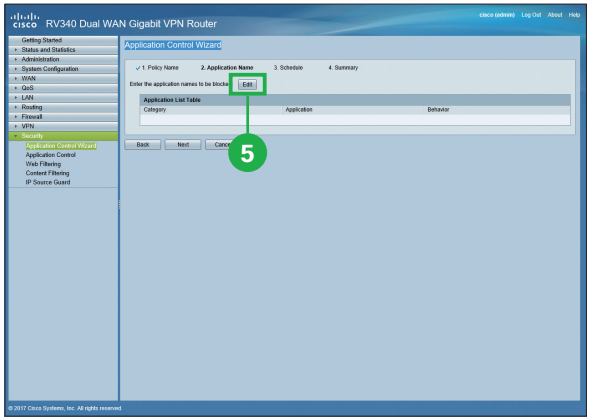
1 From the Getting Started page, Click [Application Control Wizard].



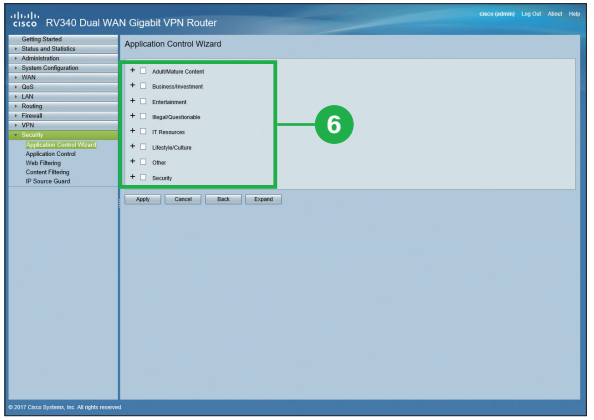
2 Select [On].

3 Enter a policy name in the [Enter a name of this policy] field.

4 Click [Next].

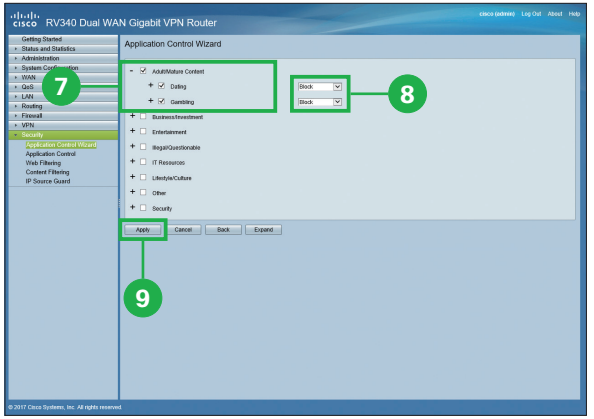


5 Click [Edit].



6 Select one or more category names or click + icons to expand to sub categories to be filtered.

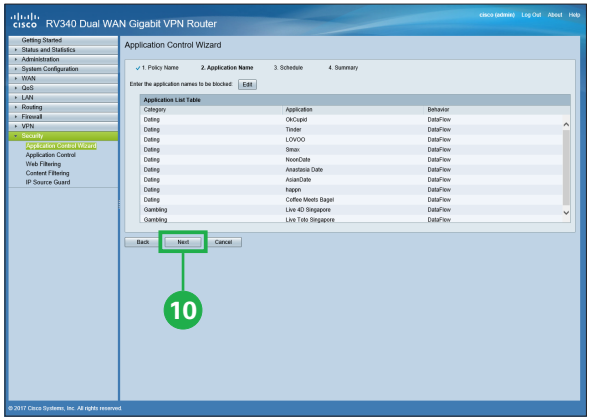
You can click + icons to expand to applications to be filtered.



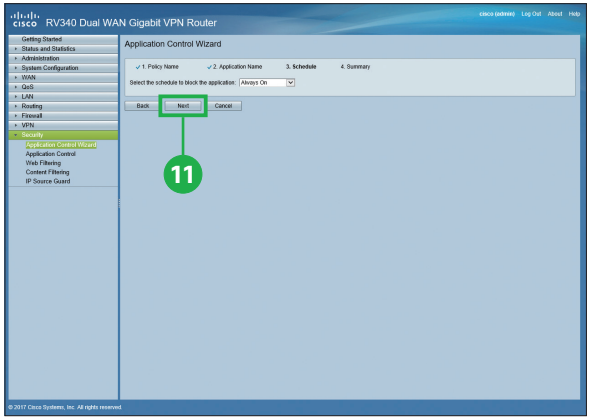
7 Select one or more category names, sub category names, or applications to be filtered.

8 Select an action (Permiet or Block, etc) from the drop-down list to each sub category names or applications.

9 Click [Apply].

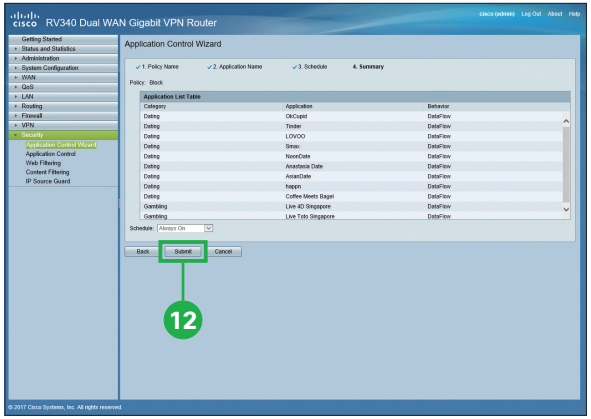


10 Click [Next].



11 Click [Next].

You can select the schedule to block the application from the [Select the schedule to block the application] drop-down list.

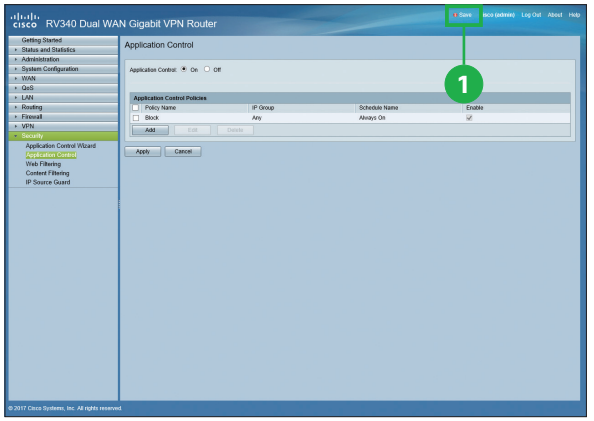


12 Click [Submit].

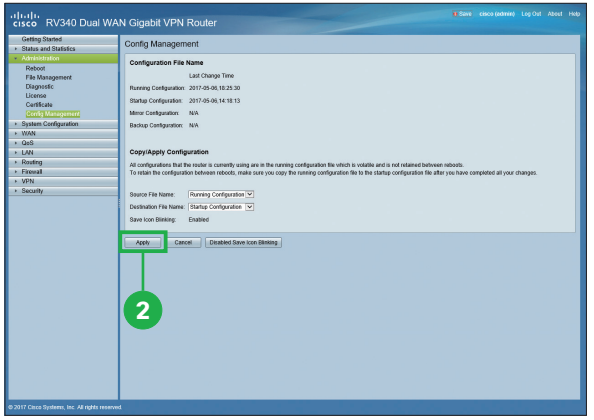
You can set separate application control policies to take different actions for different application categories or applications. If you want to do so, repeat the steps.

6 Applying Configuration

All configurations that the router is currently using are in the running configuration file which is volatile and is not retained between reboots.
To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.



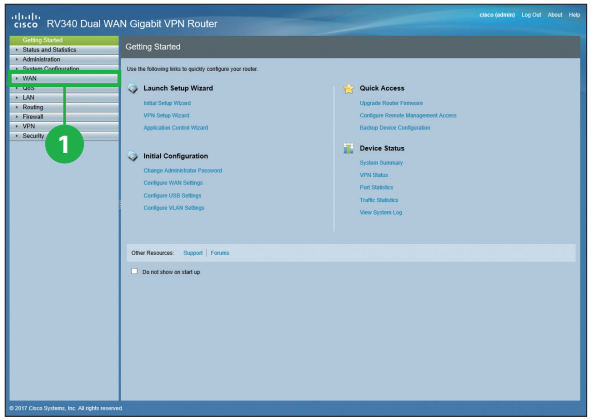
1 Click blinking [Save].



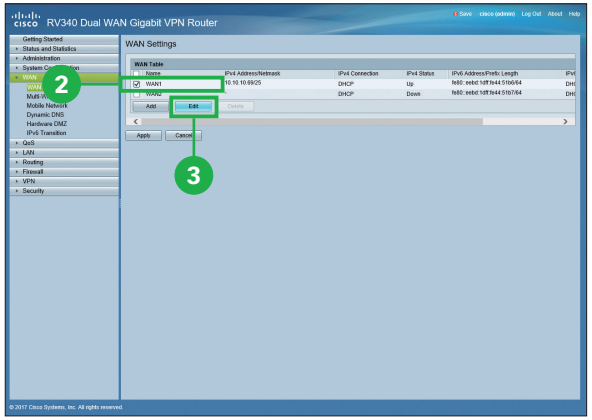
2 Click [Apply].

Appendix 1 Additional WAN Settings

If you need to configure additional WAN settings, follow these steps.

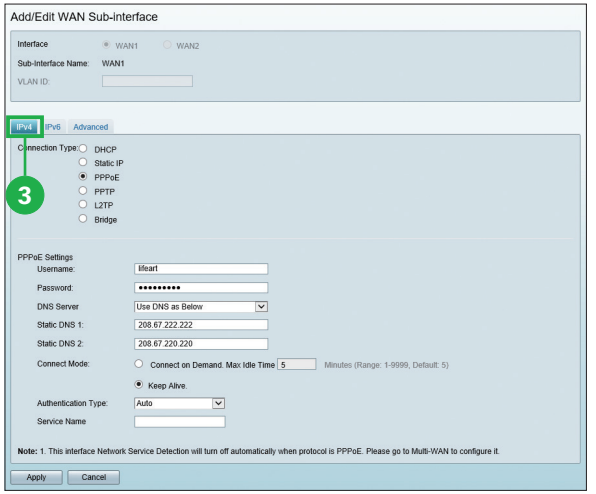


1 Click [WAN].



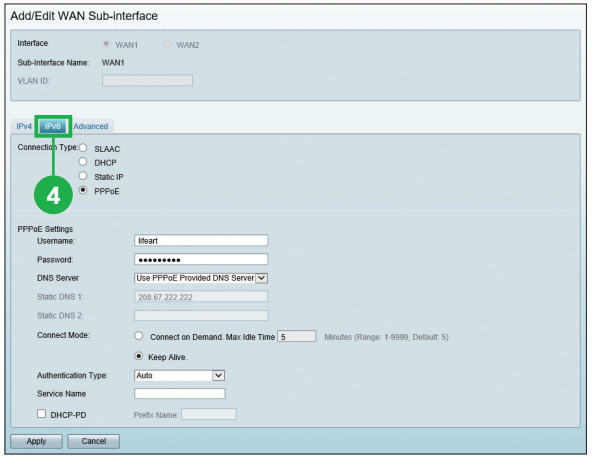
2 Select the Interface.

3 Click [Edit].



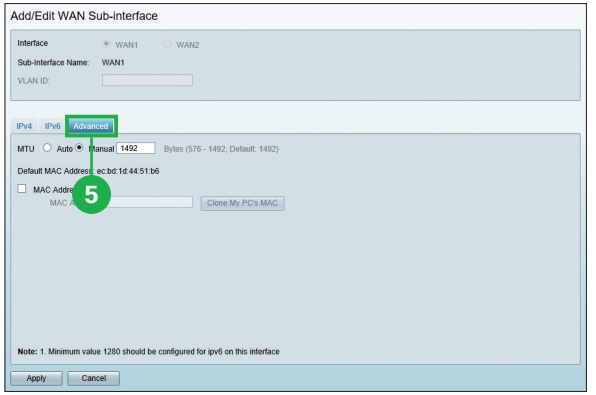
3 Click [IPv4] tab to configure additional settings for IPv4.

For example, you can configure [DNS Server] manually.



4 Click [IPv6] tab to configure additional settings for IPv6.

For example, you can configure [DHCP-PD].



5 Click [Advanced] tab to configure additional advanced settings.

For example, you can configure [MTU] manually.

Appendix 2 Where to Go From Here

Support

- **Cisco Support Community**
  http://www.cisco.com/go/smallbizsupport

- **Cisco Support and Resources**
  http://www.cisco.com/go/smallbizhelp

- **Phone Support Contacts**
  http://www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html

- **Cisco Firmware Downloads**
  http://www.cisco.com/go/smallbizfirmware

- **Cisco Open Source Requests**
  http://www.cisco.com/go/smallbiz_opensource_request

- **Cisco Partner Central**
  http://www.cisco.com/web/partners/sell/smb

- **Cisco Online Device Emulators**
  http://www.cisco.com/go/onlinedevicemanagers

Product Documentation

- **Cisco RV340 Series Security Router Administration Guide**
  http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/RV340/Administration/EN/b_RV340_AG.pdf