

Total Network Configuration: RV345P and Cisco Business Wireless using the Web UI

Objective

This guide will show you how to configure a wireless mesh network using an RV345P router, a CBW140AC access point, and two CBW142ACM mesh extenders.

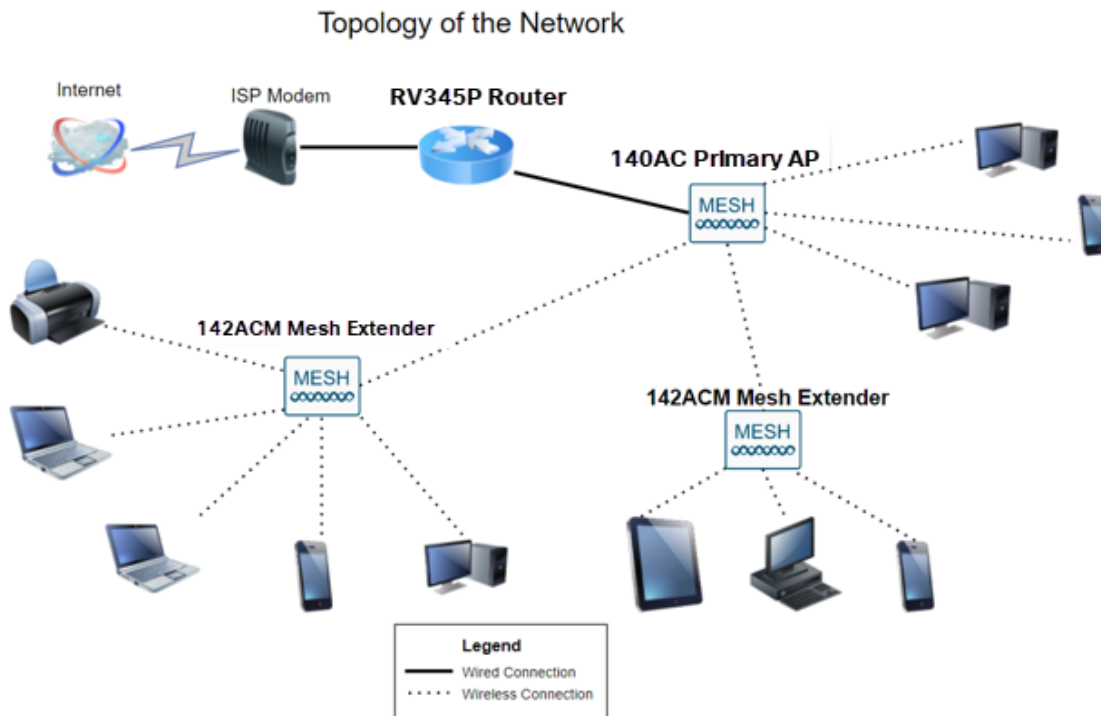
This article uses the Web User Interface (UI) to set up the mesh wireless network. If you prefer to use the mobile application, which is recommended for easy wireless setup, [click to jump to the article that uses the mobile application](#).

Table of Contents

- [Prerequisites](#)
 - [Prepare the Router](#)
 - [Obtain a Cisco.com Account](#)
- [Configure the RV345P Router](#)
 - [RV345P Out of the Box](#)
 - [Set Up the Router](#)
 - [Troubleshooting the Internet Connection](#)
 - [Initial Configuration](#)
 - [Edit an IP address If Necessary \(Optional\)](#)
 - [Upgrade Firmware if Needed](#)
 - [Configure Automatic Updates on the RV345P Series Router](#)
- [Security Options](#)
 - [RV Security License \(Optional\)](#)
 - [Web Filtering on the RV345P Router](#)
 - [Umbrella RV Branch License \(Optional\)](#)
 - [Other Security Options](#)
- [VPN Options](#)
 - [VPN Passthrough](#)
 - [AnyConnect VPN](#)
 - [Shrew Soft VPN](#)
 - [Other VPN Options](#)
- [Supplemental Configurations on the RV345P Router](#)
 - [Configure VLANs \(Optional\)](#)
 - [Assign VLANs to Ports \(Optional\)](#)
 - [Add a Static IP \(Optional\)](#)
 - [Managing Certificates \(Optional\)](#)
 - [Configure a Mobile Network Using a Dongle and an RV345P Series Router \(Optional\)](#)
- [Configure the CBW140AC](#)
 - [CBW140AC Out of the Box](#)
 - [Set Up the 140AC Primary Wireless Access Point on the Web UI](#)

- [Wireless Troubleshooting Tips](#)
- [Configure the CBW142ACM Mesh Extenders Using the Web UI](#)
- [Check and Update Software Using the Web UI](#)
- [Create WLANs on the Web UI](#)
- [Optional Wireless Configurations](#)
 - [Create a Guest WLAN using the Web UI \(Optional\)](#)
 - [Application Profiling using the Web UI \(Optional\)](#)
 - [Client Profiling using the Web UI \(Optional\)](#)

Topology



Introduction

All of your research has come together and you have purchased your Cisco equipment, how exciting! In this scenario, we are using an RV345P router. This router provides Power over Ethernet (PoE) which allows you to plug the CBW140AC into the router instead of a switch. The CBW140AC and the CBW142ACM mesh extenders will be used to create a wireless mesh network.

This advanced router also gives the option for additional features.

1. Application control allows you to control traffic. This feature can be configured to allow traffic but to log it, block traffic and log it, or simply to block traffic.
2. Web Filtering is used to prevent web traffic to insecure or inappropriate web sites. There is no logging with this feature.
3. AnyConnect is a Secure Sockets Layer (SSL) Virtual Private Network (VPN) that is available from Cisco. VPNs allow remote users and sites to connect to your company office or datacenters by making a secure tunnel through the Internet.

If you want to use these features, you will need to purchase a license. Routers and licenses are registered online, which will be covered in this guide.

If you are unfamiliar with some of the terms used in this document or want more details about Mesh Networking, check out the following articles:

- [Cisco Business: Glossary of New Terms](#)
- [Welcome to Cisco Business Wireless Mesh Networking](#)
- [Frequently Asked Questions \(FAQ\) for a Cisco Business Wireless Network](#)

Applicable Devices | Software Version

- RV345P | 1.0.03.21
- CBW140AC | 10.4.1.0
- CBW142ACM | 10.4.1.0 (at least one mesh extender is needed for the mesh network)

Prerequisites

Prepare the Router

1. Make sure you have a current Internet connection for setup.
2. Contact your Internet Service Provider (ISP) to find out any special instructions they have when using your RV345P router. Some ISPs offer gateways with built-in routers. If you have a gateway with an integrated router, you may have to disable the router and pass the Wide Area Network (WAN) IP address (the unique Internet protocol address that the Internet provider assigns to your account) and all network traffic through to your new router.
3. Decide where to place the router. You will want an open area if possible. This may not be easy because you must connect the router to the broadband gateway (modem) from your Internet Service Provider (ISP).

Obtain a Cisco.com Account

Now that you own Cisco equipment, you need to get a Cisco.com Account, sometimes referred to as a Cisco Connection Online Identification (CCO ID). There is no charge for an account.

If you already have an account, you can [jump to the next section of this article](#).

Step 1

Go to [Cisco.com](#). Click the **person icon** and then **Create an account**.



2 Primary AP Information

User : admin (ReadWrite) Logout

Step 2

Enter the required details to create the account and click **Register**. Follow the instructions to complete the registration process.

1

Create Account

Already have an account? [Sign In](#)

Email

First Name

Last Name

Country

Select a country or start typing for suggestions

Company

Password

Create a password

Confirm Password

Re-enter your password

Would you like updates about Cisco promotions, products and services?

Email Yes No

2 Register

If you have any issues, [click to jump to the Cisco.com Account Registration Help Page](#).

Configure the RV345P Router

A router is essential in a network because it routes packets. It enables a computer to communicate with other computers that are not on the same network or subnet. A

router accesses a routing table to determine where packets should be sent. The routing table lists destination addresses. Static and dynamic configurations can both be listed on the routing table in order to get packets to their specific destination.

Your RV345P comes with default settings that are optimized for many small businesses. However, your network demands, or Internet Service Provider (ISP) might require you to modify a few of these settings. After you contact your ISP for the requirements, you can make changes using the Web User Interface (UI).

Are you ready? Let's get to it!

RV345P Out of the Box

Step 1

Connect the Ethernet cable from one of the RV345P LAN (Ethernet) ports to the Ethernet port on the computer. You will need an adapter if your computer doesn't have an Ethernet port. The terminal must be in the same wired subnetwork as the RV345P to perform the initial configuration.

Step 2

Be sure to use the power adapter that is supplied with the RV345P. Using a different power adapter could damage the RV345P or cause USB dongles to fail. The power switch is on by default.

Connect the power adapter to the 12VDC port of the RV345P, but don't plug it into power yet.

Step 3

Make sure the modem is turned off.

Step 4

Use an Ethernet cable to connect your cable or DSL modem to the WAN port on the RV345P.

Step 5

Plug the other end of the RV345P adapter into an electrical outlet. This will power on the RV345P. Plug the modem back in so it can power up as well. The power light on the front panel is solid green when the power adapter is connected properly, and the RV345P is finished booting.

Set Up the Router

The prep work is done, now it's time to get to some configurations! To launch the Web

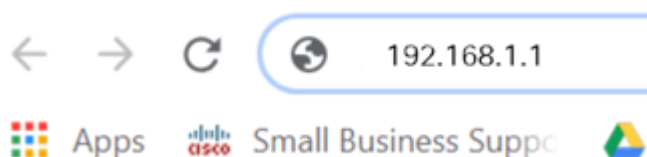
UI, follow these steps.

Step 1

If your computer is configured to become a Dynamic Host Configuration Protocol (DHCP) client, an IP address in the 192.168.1.x range is assigned to the PC. DHCP automates the process of assigning IP addresses, subnet masks, default gateways, and other settings to computers. Computers must be set to participate in the DHCP process to obtain an address. This is done by selecting to obtain an IP address automatically in the properties of TCP/IP on the computer.

Step 2

Open a web browser such as Safari, Internet Explorer, or Firefox. In the address bar, enter the default IP address of the RV345P, 192.168.1.1.



Step 3

The browser might issue a warning that the website is untrusted. Continue to the website. If you are not connected, jump down to [Troubleshooting the Internet Connection](#).



Your connection is not private

Attackers might be trying to steal your information from [ciscobusiness.cisco](#) (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. [Privacy policy](#)

Advanced

Back to safety

Step 4

When the sign-in page appears, enter the default username *cisco* and the default password *cisco*.

Click **Login**.

For detailed information, click [How to access the web-based setup page of Cisco RV340 series VPN routers](#).



Router

1

2

English ▾

3

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Step 5

Click **Login**. The *Getting Started* page appears. If the navigation pane isn't open, you can open it by clicking on the **menu icon**.



Now that you have confirmed the connection and logged in to the router, jump to the [Initial Configuration](#) section of this article.

Troubleshooting the Internet Connection

Dang it, if you are reading this you are probably having trouble connecting to the Internet or the Web UI. One of these solutions should help.

On your connected Windows OS, you can test your network connection by opening the command prompt. Enter **ping 192.168.1.1** (the default IP address of the router). If the request times out, you are not able to communicate with the router.

If connectivity is not happening, you can check out this [Troubleshooting](#) article.

Some other things to try:

1. Verify that your web browser is not set to Work Offline.
2. Check the local area network connection settings for your Ethernet adapter. The PC should obtain an IP address through DHCP. Alternatively, the PC can have a static IP address in the 192.168.1.x range with the default gateway set to 192.168.1.1 (the default IP address of the RV345P). To connect, you may need to modify the network settings of the RV345P. If you are using Windows 10, check out [Windows 10 directions to modify the network settings](#).

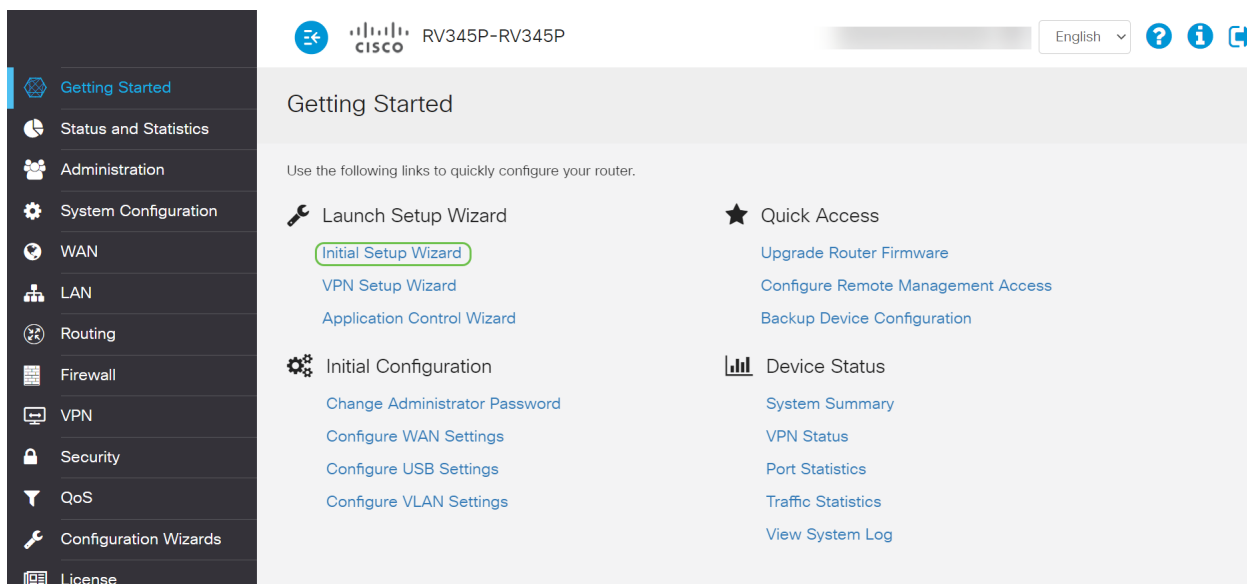
3. If you have existing equipment occupying the 192.168.1.1 IP address, you'll need to resolve this conflict for the network to operate. More on this at the end of this section, or [click here to be taken there directly](#).
4. Reset the modem and the RV345P by powering off both devices. Next, power on the modem and let it sit idle for about 2 minutes. Then power on the RV345P. You should now receive a WAN IP address.
5. If you have a DSL modem, ask your ISP to put the DSL modem into bridge mode.

Initial Configuration

We recommend that you go through the *Initial Setup Wizard* steps listed in this section. You can change these settings at any time.

Step 1

Click **Initial Setup Wizard** from the *Getting Started* Page.

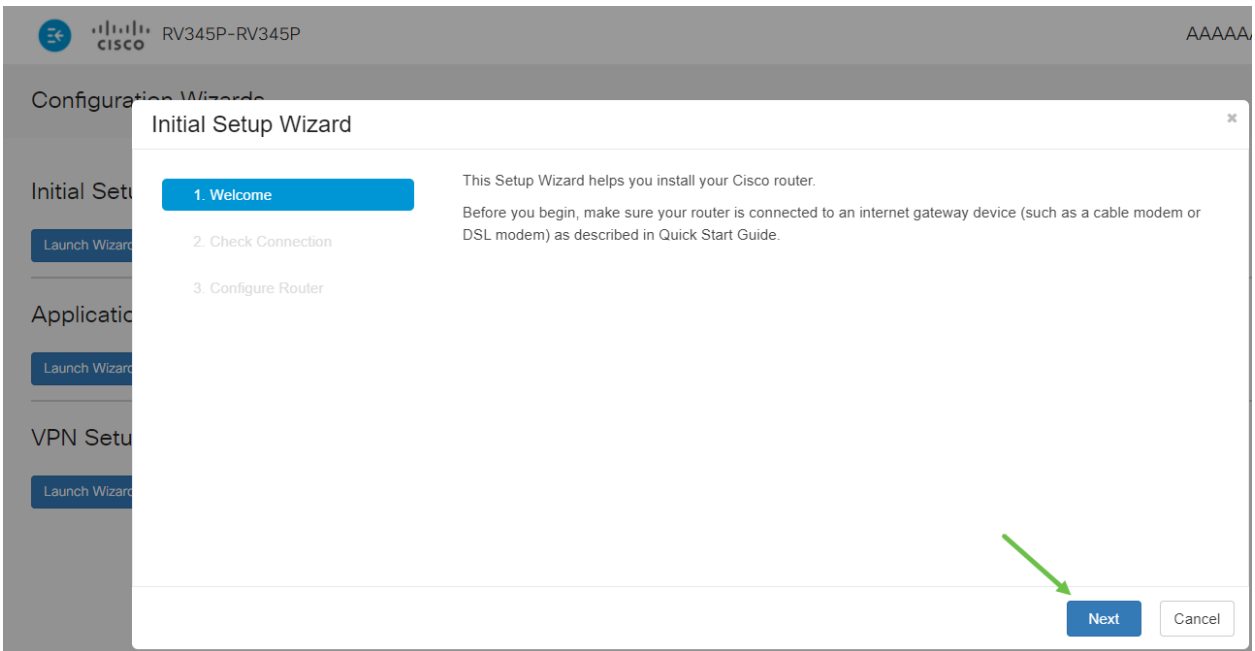


The screenshot shows the Cisco RV345P web interface. The top navigation bar includes the Cisco logo, the device model 'RV345P-RV345P', a language dropdown set to 'English', and help icons. The left sidebar lists various configuration categories: Getting Started, Status and Statistics, Administration, System Configuration, WAN, LAN, Routing, Firewall, VPN, Security, QoS, Configuration Wizards, and License. The main content area is titled 'Getting Started' and contains the following sections:

- Launch Setup Wizard**
 - [Initial Setup Wizard](#) (highlighted with a green box)
 - [VPN Setup Wizard](#)
 - [Application Control Wizard](#)
- Initial Configuration**
 - [Change Administrator Password](#)
 - [Configure WAN Settings](#)
 - [Configure USB Settings](#)
 - [Configure VLAN Settings](#)
- Quick Access**
 - [Upgrade Router Firmware](#)
 - [Configure Remote Management Access](#)
 - [Backup Device Configuration](#)
- Device Status**
 - [System Summary](#)
 - [VPN Status](#)
 - [Port Statistics](#)
 - [Traffic Statistics](#)
 - [View System Log](#)

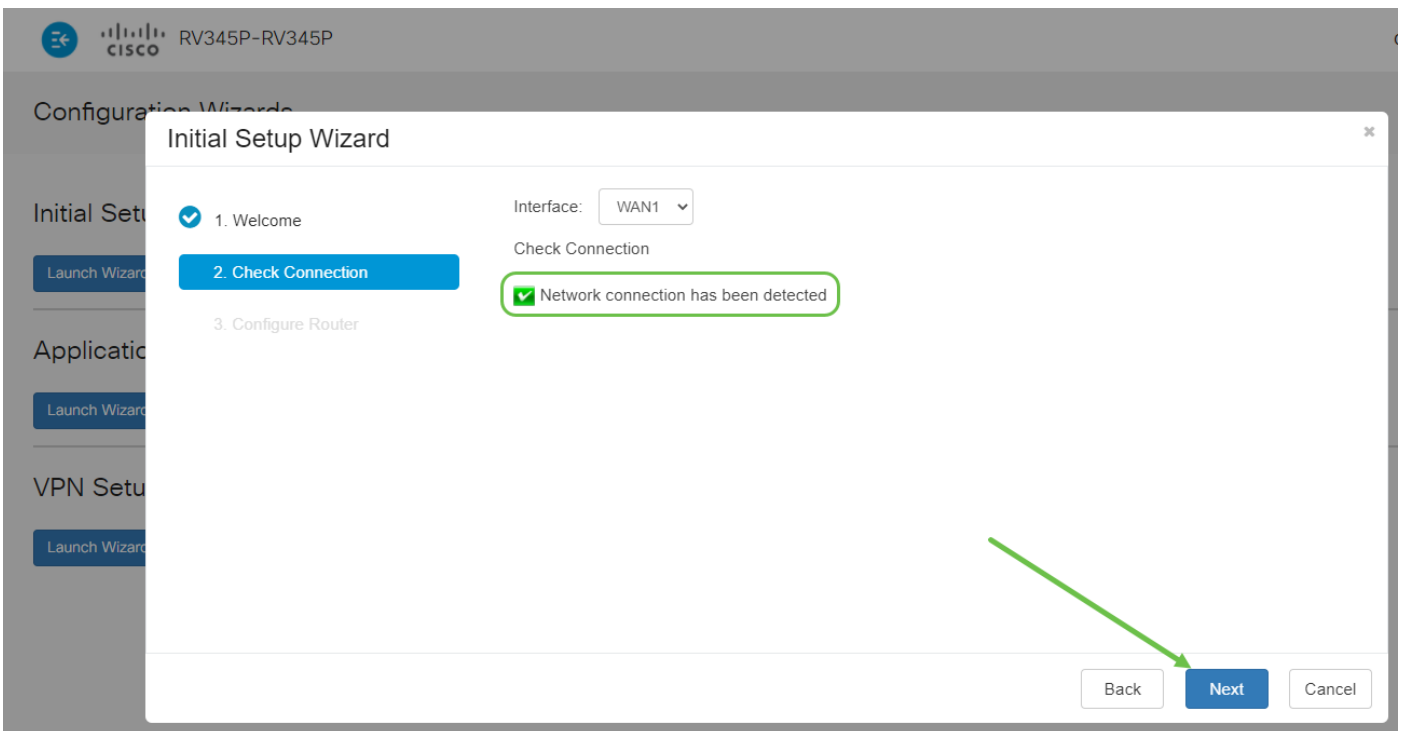
Step 2

This step confirms the cables are connected. Since you confirmed this already, click **Next**.



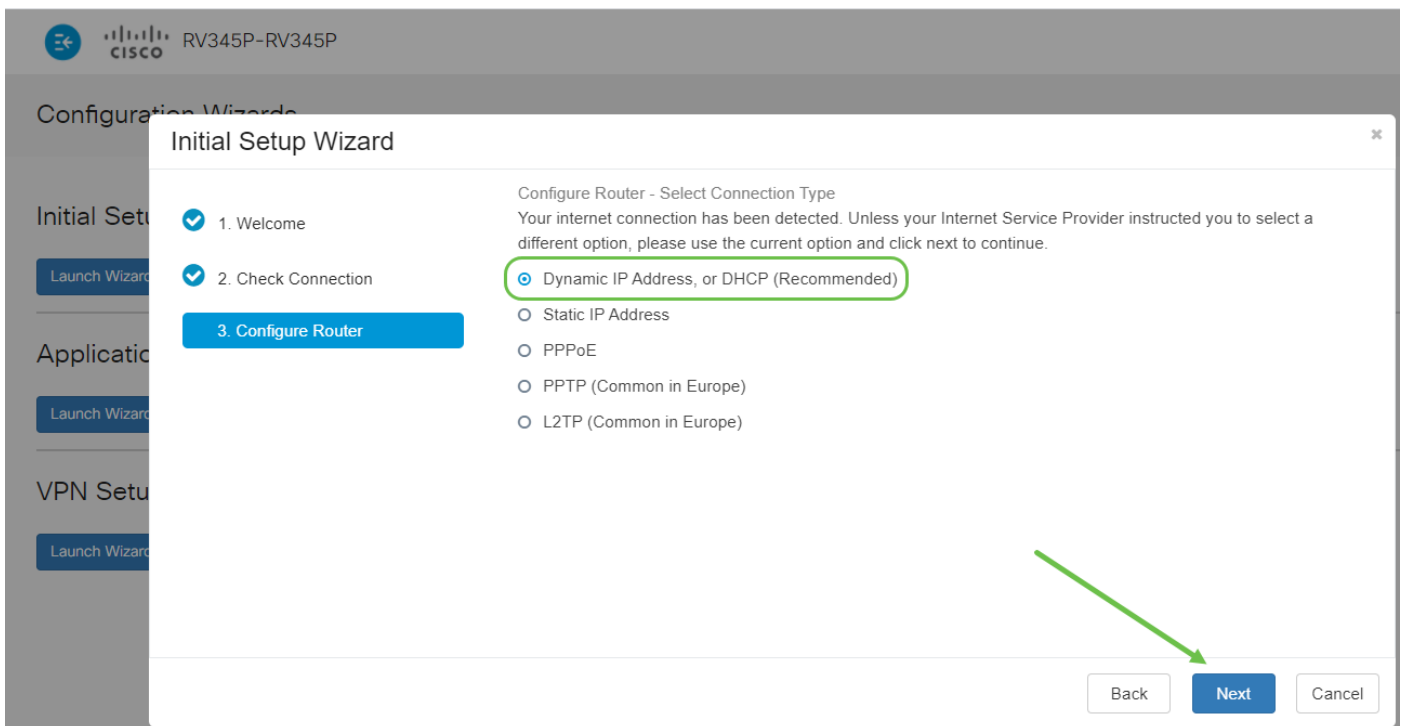
Step 3

This step covers basic steps to make sure your router is connected. Since you have already confirmed this, click **Next**.



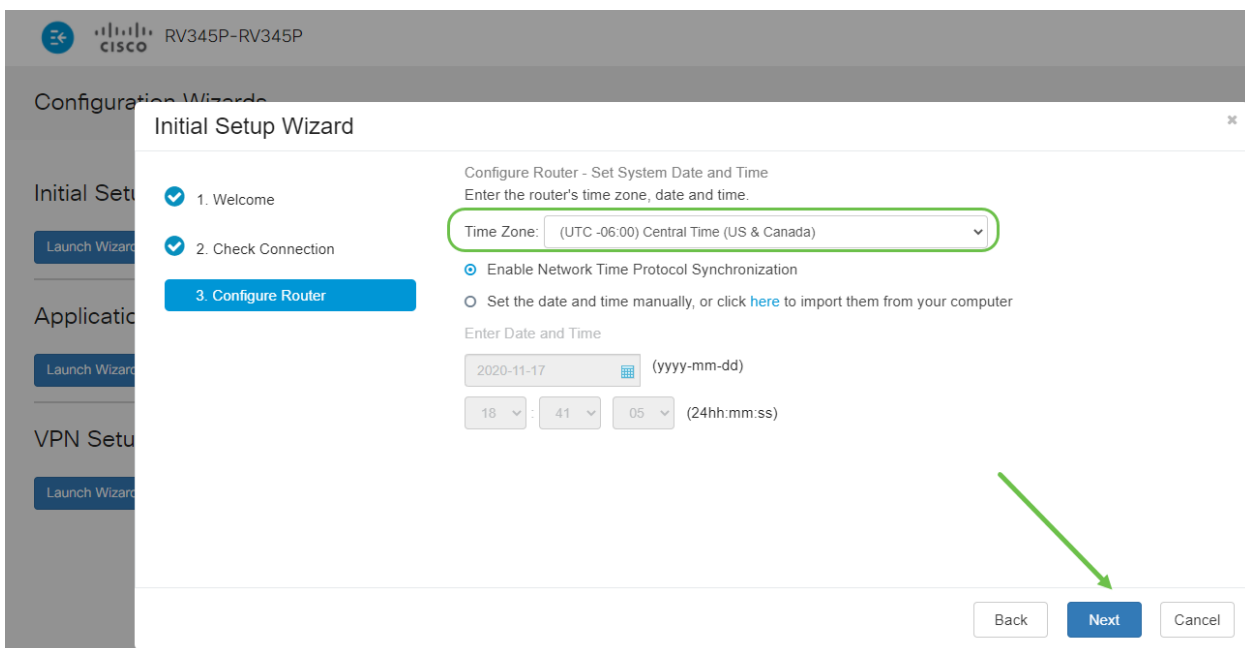
Step 4

The next screen displays your options for assigning IP addresses to your router. You need to select DHCP in this scenario. Click **Next**.



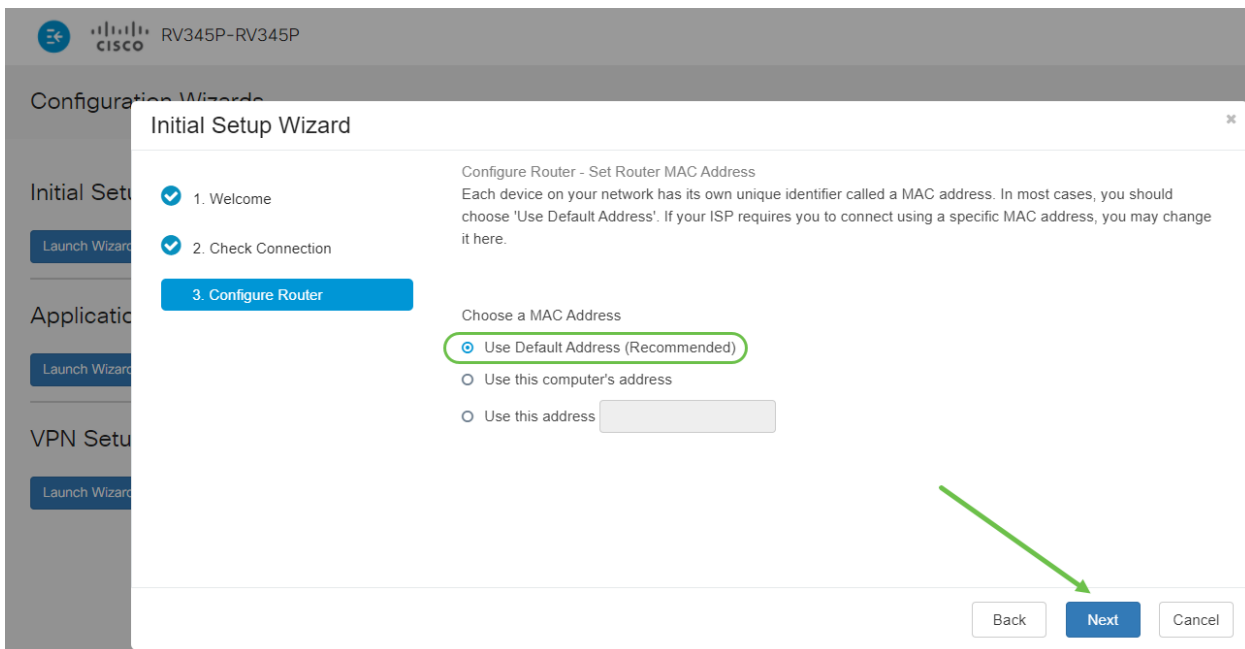
Step 5

You will be prompted to set your router time settings. This is important because it enables precision when reviewing logs or troubleshooting events. Select your **Time Zone** and then click **Next**.



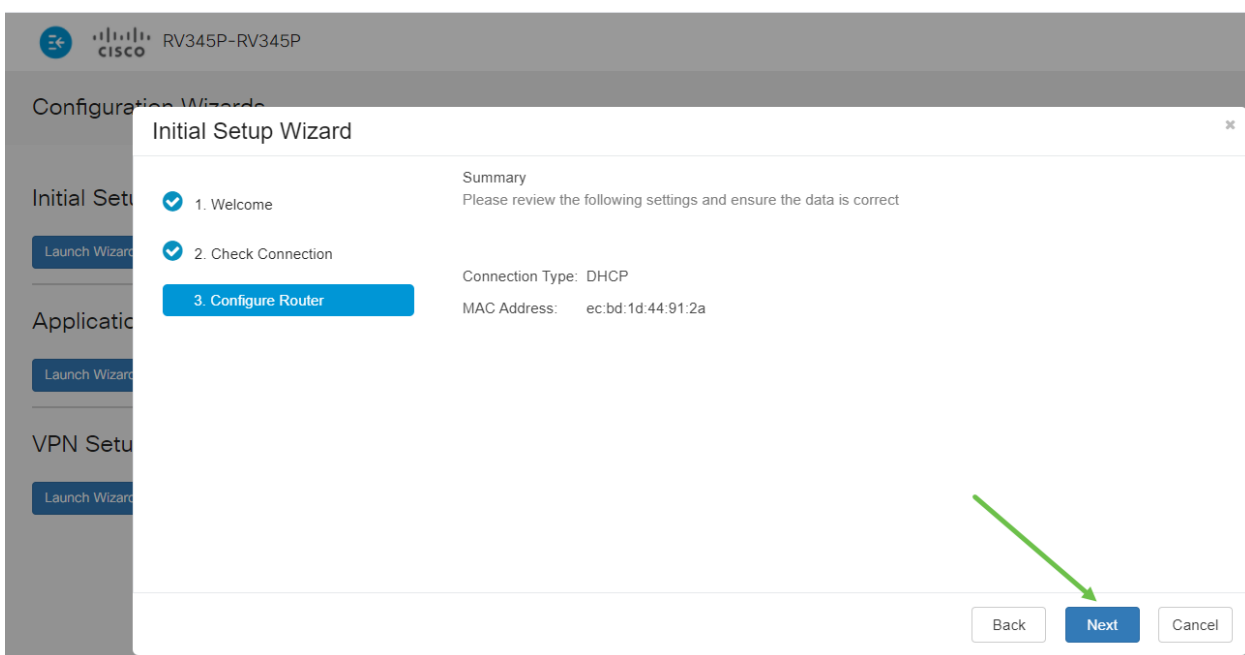
Step 6

You will select what MAC addresses to assign to devices. Most often, you will use the default address. Click **Next**.



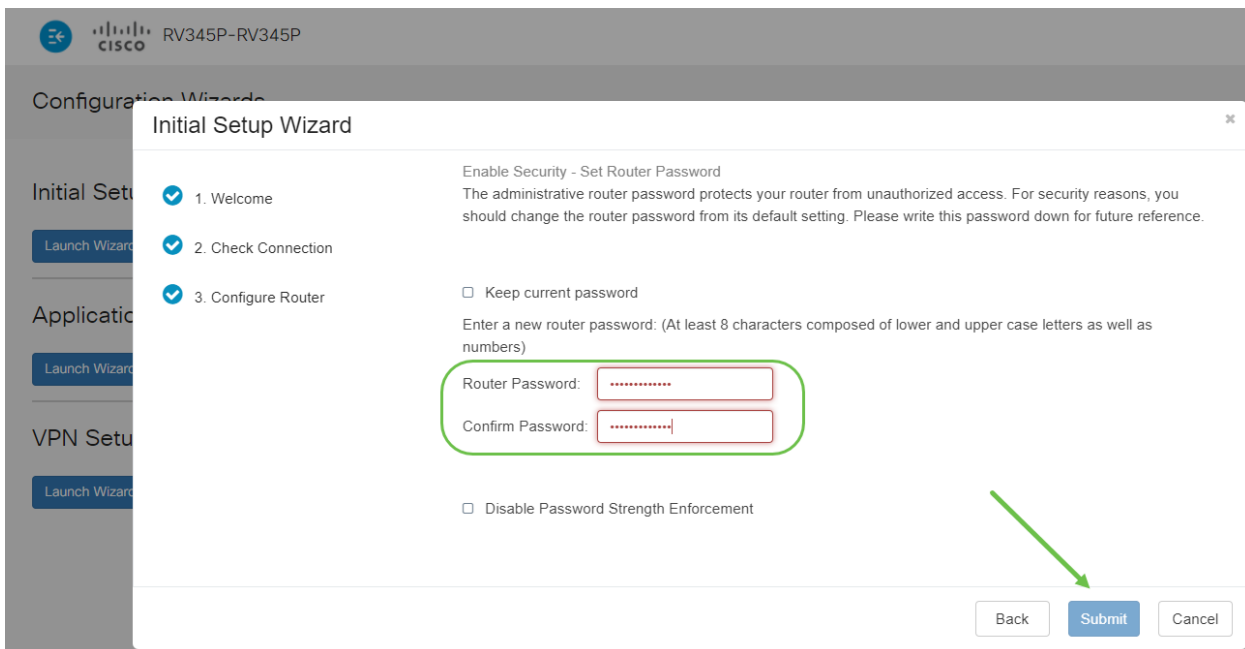
Step 7

The following page is a summary of the selected options. Review and click **Next** if satisfied.



Step 8

For the next step, you will select a password to use when logging into the router. The standard for passwords is to contain at least 8 characters (both upper and lower case) and include numbers. **Enter a password** that conforms with the strength requirements. Click **Next**. Take note of your password for future logins.



It is *not* recommended that you select *Disable Password Strength Enforcement*. This option would let you select a password as simple as 123, which would be as easy as 1-2-3 for malicious actors to crack.

Step 9

Click the **save icon**.



If you want more information on these settings, you can read [Configure DHCP WAN Settings on the RV34x Router](#).

Your RV345P has Power over Ethernet (PoE) enabled by default, but you have the ability to make some adjustments to them. If you need to customize the settings, check out [Configure Power over Ethernet \(PoE\) Settings on the RV345P Router](#).

Edit an IP address If Necessary (Optional)

After completing the *Initial Setup Wizard*, you can set a static IP address on the router by editing the VLAN settings.

This process is only needed if your router IP address needs to be assigned a specific address in your existing network. If you don't need to edit an IP address, you can move to the [next section](#) of this article.

Step 1




On the left-hand menu, click **LAN > VLAN Settings**.




Step 2

Select the **VLAN** that contains your routing device, then click the **edit icon**.

VLAN Table

| <input checked="" type="checkbox"/> | VLAN ID | Name | Inter-VLAN Routing | Device Management | IPv4 Address/Mask |
|-------------------------------------|---------|-------|-------------------------------------|---|---|
| <input checked="" type="checkbox"/> | 1 | VLAN1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/>  | 192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149 |

Step 3

Enter your desired **static IP address** and click **Apply** in the upper-right hand corner.

| <input type="checkbox"/> | VLAN ID | Name | Inter-VLAN Routing | Device Management | IPv4 Address/Mask | IPv6 Address/Prefix Length |
|-------------------------------------|---------|---------|-------------------------------------|-------------------------------------|---|--|
| <input checked="" type="checkbox"/> | 1 | Default | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | IP Address: 192.168.1.1/24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input type="radio"/> Server <input checked="" type="radio"/> Relay | Prefix: <input checked="" type="radio"/> fec0: <input type="radio"/> Prefix from DHCP-PD Prefix Length: 64 Preview: [fec0::1] Interface Identifier: <input type="radio"/> EUI-64 <input checked="" type="radio"/> 1 DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server |

Step 4 (Optional)

If your router is not the DHCP server/device assigning IP addresses, you can use the DHCP Relay feature to direct DHCP requests to a specific IP address. The IP address is likely to be the router connected to the WAN/Internet.

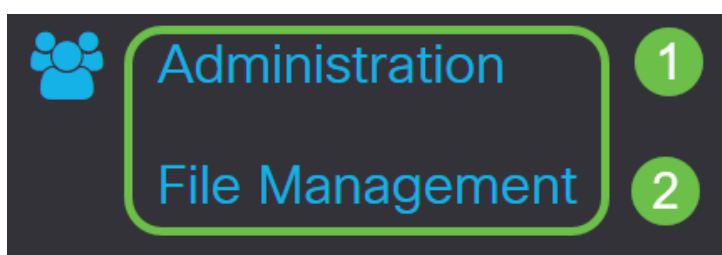
| | |
|---|---|
| DHCP Type: <input type="radio"/> Disabled <input type="radio"/> Server <input checked="" type="radio"/> Relay | Prefix Length: 64 Preview: [fec0::1] Interface Identifier: <input type="radio"/> EUI-64 <input checked="" type="radio"/> 1 DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server |
|---|---|

Upgrade Firmware if Needed

This is an important step, don't skip it!

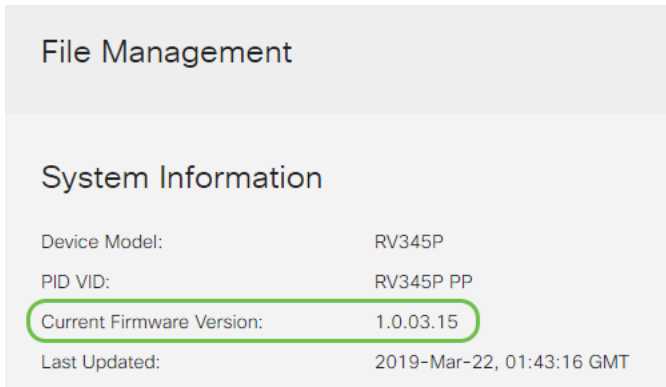
Step 1

Choose **Administration > File Management**.



In the *System Information* area, the following sub-areas describe the following:

- Device Model - Displays the model of your device.
- PID VID - Product ID and Vendor ID of the router.
- Current Firmware Version - Firmware that is currently running on the device.
- Latest Version Available on Cisco.com - Latest version of the software available on the Cisco website.
- Firmware last updated - Date and time of the last firmware update made on the router.



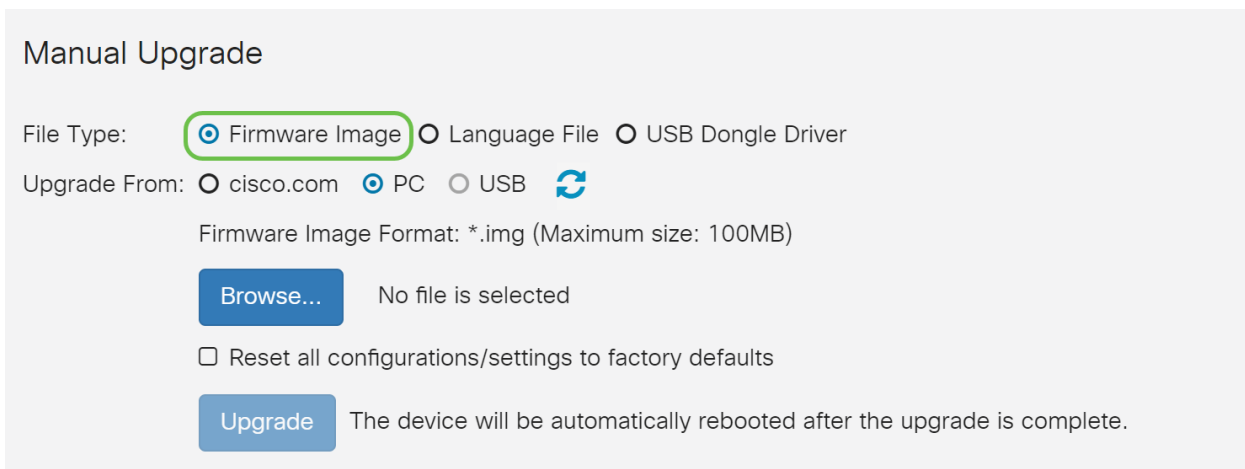
File Management

System Information

| | |
|---------------------------|---------------------------|
| Device Model: | RV345P |
| PID VID: | RV345P PP |
| Current Firmware Version: | 1.0.03.15 |
| Last Updated: | 2019-Mar-22, 01:43:16 GMT |


Step 2

Under the *Manual Upgrade* section, click on the **Firmware Image** radio button for *File Type*.



Manual Upgrade

File Type: Firmware Image Language File USB Dongle Driver

Upgrade From: cisco.com PC USB 

Firmware Image Format: *.img (Maximum size: 100MB)

No file is selected

Reset all configurations/settings to factory defaults

The device will be automatically rebooted after the upgrade is complete.

Step 3

On the *Manual Upgrade* page, click on the radio button to select *cisco.com*. There are a few other options for this, but this is the easiest way to do an upgrade. This process installs the latest upgrade file directly from the Cisco Software Downloads webpage.

If your device is not connected to the Internet or is suffering from Internet disconnections you will not be able to upgrade from cisco.com. If this pertains to you, alternative options can be found [here](#).

Manual Upgrade

File Type: Firmware Image Language File USB Dongle Driver

Upgrade From: cisco.com PC USB 

Reset all configurations/settings to factory defaults

Upgrade

The device will be automatically rebooted after the upgrade is complete.


Download to USB

Step 4

Click **Upgrade**.

Manual Upgrade

File Type: Firmware Image Language File USB Dongle Driver

Upgrade From: cisco.com PC USB 

Reset all configurations/settings to factory defaults

Upgrade

The device will be automatically rebooted after the upgrade is complete.

Download to USB

Step 5

Click **Yes** in the confirmation window to continue.

File Management

Latest Ve

Firmware

Confirm



Are you sure you want to upgrade the firmware right now?

Yes

No

The update process needs to run without interruption. You will get the following message on the screen while the upgrade is in progress.

File Management

Latest Version Available:

Firmware Last Updated:



Upgrade is in progress. Do not power off or reset the device. It may take a few minutes to complete.

Current Version:

Once the upgrade has been completed, a notification window will pop-up to inform you that the router will be *Restarting* with a countdown of the estimated time for the process to finish. Following this, you will be logged out.

File Management

Latest Version Available:

Firmware Last Updated:



Restarting

Please wait for 176 seconds...

Step 6

Log back into the web-based utility to verify that the router firmware has been upgraded, scroll to *System Information*. The *Current Firmware Version* area should now display the upgraded firmware version.

File Management

System Information

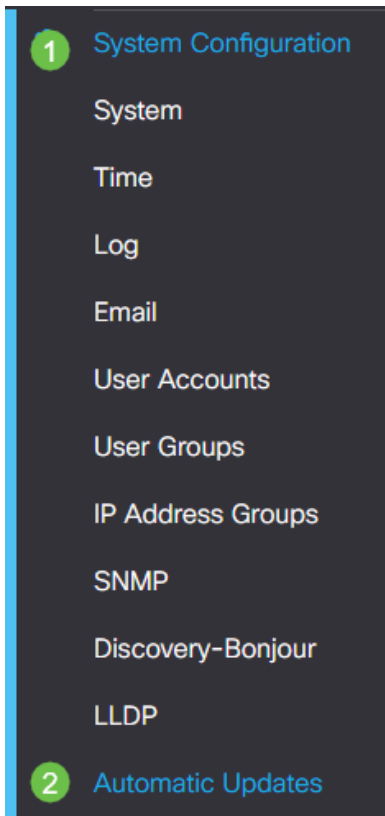
| | |
|--------------------------------------|---------------------------|
| Device Model: | RV345P |
| PID VID: | RV345P-K9 V01 |
| Current Firmware Version: | 1.0.03.20 |
| Last Updated: | 2020-Oct-02, 11:10:50 GMT |
| Last Version Available on Cisco.com: | 1.0.03.20 |
| Last Checked: | 2020-Nov-11, 14:16:01 GMT |

Configure Automatic Updates on the RV345P Series Router

Since updates are so important and you are a busy person, it makes sense to configure automatic updates from here on out!

Step 1

Log into the web-based utility and choose **System Configuration > Automatic Updates**.



Step 2

From the *Check Every* drop-down list, choose how often the router should check for updates.

The screenshot shows the 'Automatic Updates' configuration page. At the top, the title 'Automatic Updates' is displayed. Below it, there is a 'Check Every:' label followed by a dropdown menu currently set to 'Week' and a blue 'Check Now' button. Underneath, the 'Notify via:' section has a checked checkbox for 'Admin GUI' and an unchecked checkbox for 'Email to' followed by an empty text input field. To the right of the 'Email to' field, there is a note: 'Notifications will not be sent unless an email server is configured. Click [here](#) to manage email server settings.'

Step 3

In the *Notify via* area, check the **Email to** checkbox to receive updates through email. The *Admin GUI* checkbox is enabled by default and cannot be disabled. A notification will appear in the web-based configuration once an update is available.

If you want to set up email server settings, click [here](#) to learn how.

Automatic Updates

Check Every:

Notify via: Admin GUI

Email to

Notifications will not be sent unless an email server is configured. Click [here](#) to manage email server settings.

Step 4

Enter an email address in the *Email to* address field.

It is highly recommended to use a separate email account instead of using your personal email to maintain privacy.

Automatic Updates

Check Every:

Notify via: Admin GUI

Email to

Notifications will not be sent unless an email server is configured. Click [here](#) to manage email server settings.

Step 5

Under the *Automatically Update* area, check the **Notify** checkboxes of the kind of updates you want to be notified about. The options are:

- System Firmware — The main control program for the device.
- USB Modem Firmware — The control program or driver for the USB port.
- Security Signature — This will contain signatures for Application Control to identify applications, device types, operating systems, and so on.

Automatic Updates

Check Every:

Notify via: Admin GUI

Email to

Notifications will not be sent unless an email server is configured. Click [here](#) to manage email server settings.

Automatic Update

| | Notify <input type="checkbox"/> | Update (hh:mm) <input type="text"/> | Status <input type="text"/> |
|--------------------|-------------------------------------|-------------------------------------|-----------------------------|
| System Firmware | <input checked="" type="checkbox"/> | <input type="text" value="Never"/> | Version 1.0.03.20 |
| USB Modem Firmware | <input checked="" type="checkbox"/> | <input type="text" value="Never"/> | Version 1.0.00.02 |
| Security Signature | <input checked="" type="checkbox"/> | <input type="text" value="23:00"/> | Version 2.0.0.0015 |

Step 6

From the *Automatic Update* drop-down list, choose a time of the day you want the automatic update to be done. Some options may vary according to the type of update you have chosen. Security Signature is the only option to have an immediate update. It is recommended that you set a time when your office is closed so service isn't interrupted at an inconvenient time.

The screenshot shows the 'Automatic Updates' configuration page for a Cisco RV345P-RV345P device. The page includes a 'Check Every' dropdown set to 'Week' and a 'Check Now' button. Under 'Notify via', 'Admin GUI' and 'Email to' (with the address 'terizepnick@gmail.com') are checked. Below is a table of update settings:

| Automatic Update | Notify | Time |
|--------------------|-------------------------------------|-------|
| System Firmware | <input checked="" type="checkbox"/> | Never |
| USB Modem Firmware | <input checked="" type="checkbox"/> | Never |
| Security Signature | <input checked="" type="checkbox"/> | 23:00 |

The status displays the currently running version of the firmware or security signature.

Step 7

Click **Apply**.

The screenshot shows two buttons: 'Apply' and 'Cancel'. The 'Apply' button is highlighted with a green border.

Step 8

To save the configuration permanently, go to the Copy/Save Configuration page or click the **save icon** at the upper portion of the page.



Awesome, your basic settings on your router are complete! Now you have some configuration options to explore.

Security Options

Of course, you want your network to be safe. There are some simple options, such as having a complex password, but if you want to take steps for an even more secure network check out this section on security.

RV Security License (Optional)

This RV Security License features protect your network from attacks from the Internet:

- **Intrusion Prevention System (IPS):** Inspects network packets, logs, and/or blocks a wide range of network attacks. It delivers increased network availability, faster remediation, and comprehensive threat protection.
- **Antivirus:** Protection from viruses by scanning the applications for various protocols like HTTP, FTP, SMTP Email attachments, POP3 Email attachments, and IMAP Email attachments going through the router.
- **Web Security:** Enables business efficiency and security while connecting to the Internet, allows Internet access policies for end devices and Internet applications to help ensure performance and security. It is cloud-based and contains more than 80 categories with more than 450 million domains classified.
- **Application Identification:** Identify and assign policies to Internet applications. 500 unique applications are automatically identified.
- **Client Identification:** Identify and categorizes clients dynamically. The ability to assign policies based on end-device category and operating system.

The RV Security License provides Web Filtering. Web Filtering is a feature that allows you to manage access to inappropriate websites. It can screen a client's web access requests to determine whether to allow or deny that website.

The licensed security features can be trialed at no cost for 90 days. Should you wish to continue using the advanced security features on your router after the evaluation period, then you must acquire and activate a license.

Another Security option is Cisco Umbrella. [Click here if you would like to jump to the Umbrella section instead.](#)

If you don't want either security license, [click to jump to the VPN section of this document.](#)

Introduction to Smart Accounts

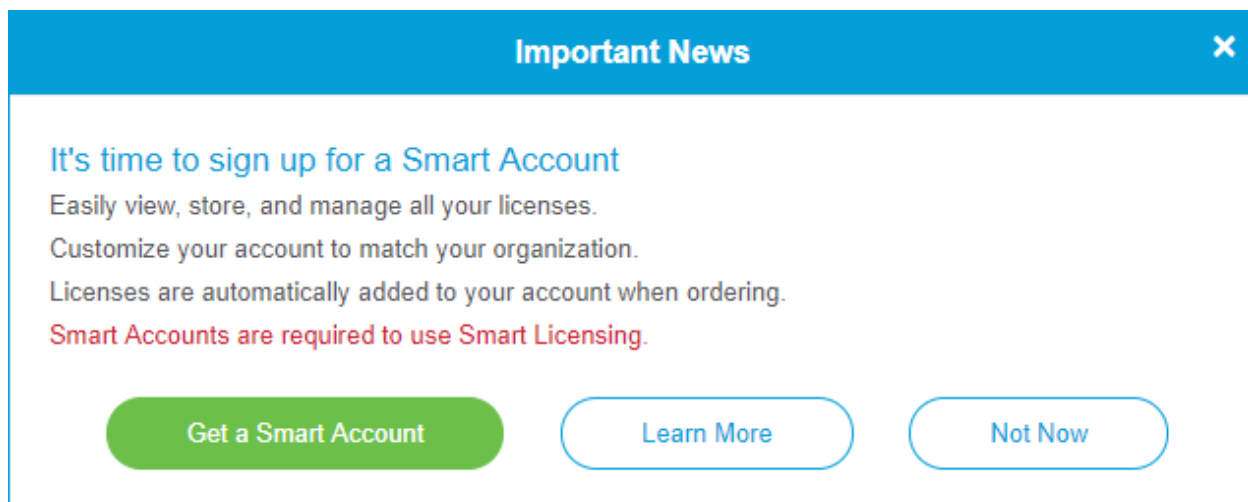
To purchase the RV Security License, you need a Smart Account.

By authorizing the activation of this Smart Account, you agree that you are authorized to create accounts and manage product and service entitlements, license agreements, and user access to accounts on behalf of your organization. Cisco Partners may not authorize account creation on behalf of customers.

The creation of a new Smart Account is a one-time event and management from that point forward is provided through the tool.

Create a Smart Account

When you access your general Cisco account using your Cisco.com Account, or CCO ID (the one you created at the beginning of this document), you may be greeted by a message to create a Smart Account.



Important News ✕

It's time to sign up for a Smart Account
Easily view, store, and manage all your licenses.
Customize your account to match your organization.
Licenses are automatically added to your account when ordering.
Smart Accounts are required to use Smart Licensing.

[Get a Smart Account](#) [Learn More](#) [Not Now](#)

If you haven't seen this pop-up, you can click to be taken to the [Smart Account creation page](#). You may need to log in with your Cisco.com Account credentials.

For additional detail on the steps involved in requesting your Smart Account, click [here](#).

Be sure to take note of your account name along with other registration details.

Quick Tip: If you are required to enter a domain and you do not have one, you can enter your email address in the form of *name@domain.com*. Common domains are gmail, yahoo, etc. depending on your company or provider.

It is very important that you have a Cisco.com (CCO ID) Account and a Cisco Smart Account before purchasing the RV Security License.

Purchase RV Security License

You must purchase a license from your Cisco distributor or your Cisco partner. To locate a Cisco partner, click [here](#).

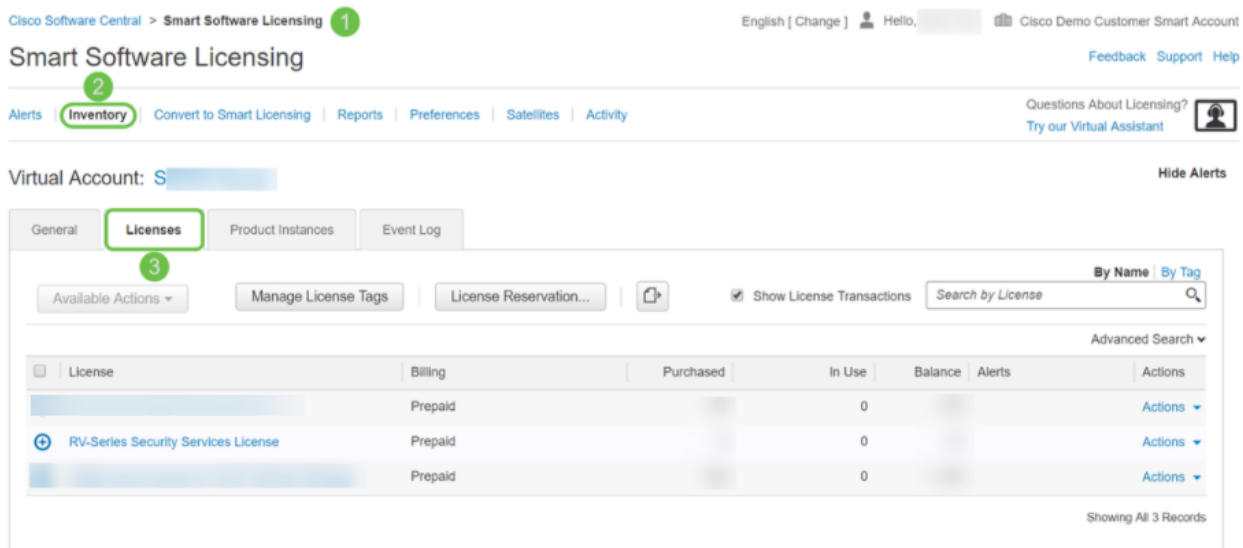
The table below displays the part number for the license.

| Type | Product ID | Description |
|---------------------|-------------------|--|
| RV Security License | LS-RV34X-SEC-1YR= | RV Security: 1 year: Dynamic Web Filter, Application Visibility, Client Identification and Statistics, Gateway Antivirus, and Intrusion Prevention System IPS. |

The license key is not entered into your router directly but will be assigned to your Cisco Smart Account after you order the license. The amount of time it takes for the license to show up on your account depends on when the partner accepts the order and when the reseller links the licenses to your account, which is usually 24-48 hours.

Confirm License is in Smart Account

Navigate to your Smart License account page, then click **Smart Software License page > Inventory > Licenses**.

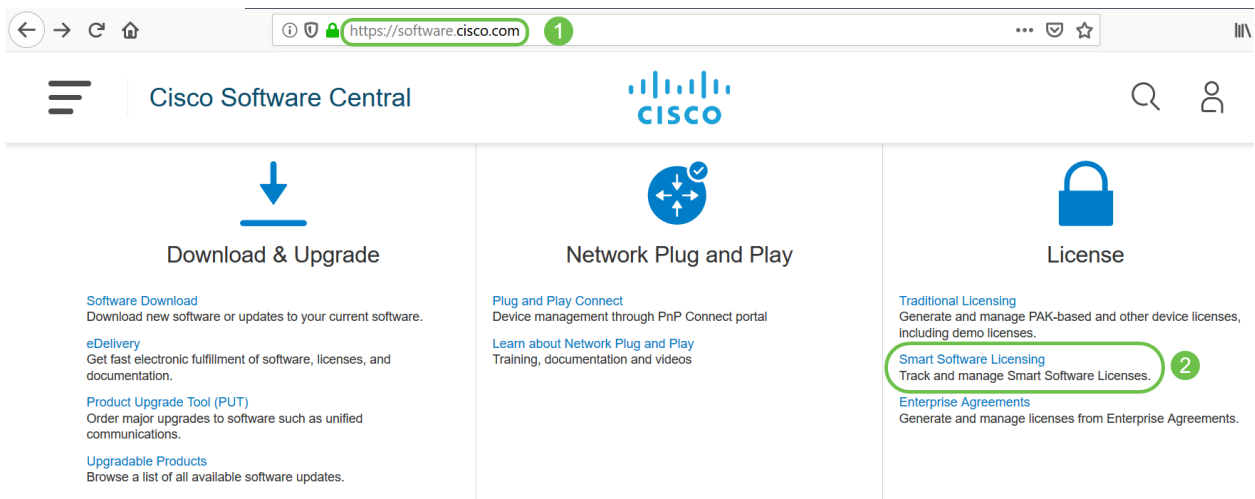


If you do not see your license in your Smart Account, contact your Cisco partner.

Configure the RV Security License on the RV345P Series Router

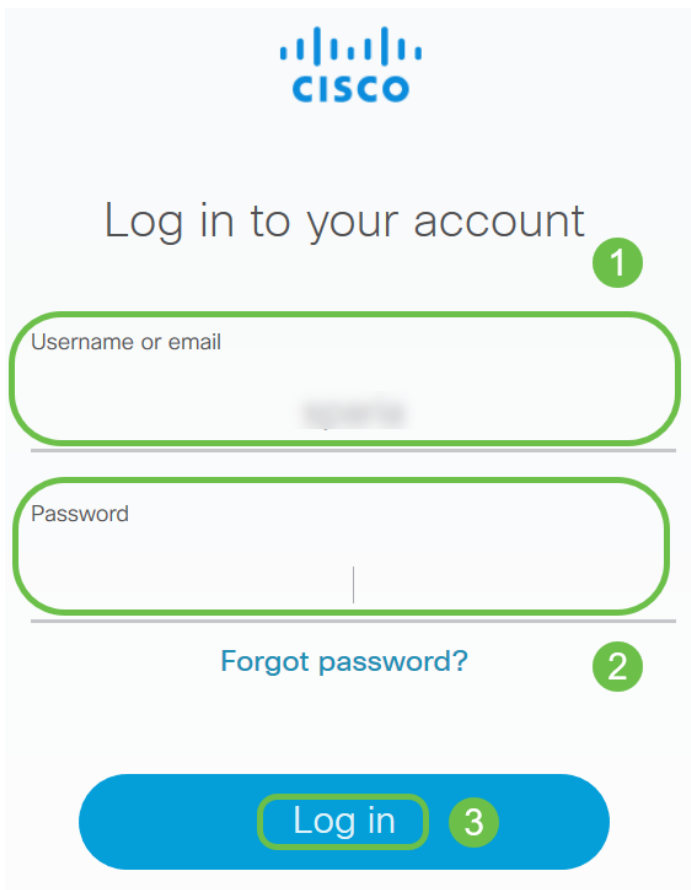
Step 1

Access [Cisco Software](#) and navigate to **Smart Software Licensing**.



Step 2

Enter your *Username or email* and *Password* to log into your Smart Account. Click **Log in**.

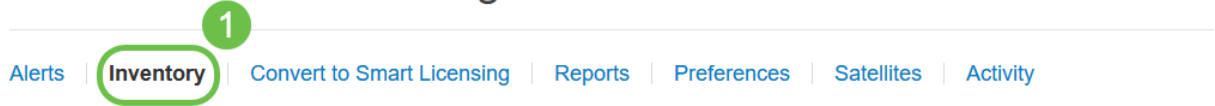


Step 3

Navigate to **Inventory > Licenses** and verify that the *RV-Series Security Services License* is listed on your Smart Account. If you do not see the license listed, contact your Cisco partner.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing



Step 4

Navigate to **Inventory > General**. Under *Product Instance Registration Tokens* click on **New Token**.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts | **Inventory** | Convert to Smart Licensing | Reports | Preferences | Satellites | Activity

1

Virtual Account: [blurred]

General

Licenses

Product Instances

Event Log

2

Virtual Account

Description:

Default Virtual Account:

No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

3

Step 5

A Create Registration Token window will appear. The *Virtual Account* area displays the virtual account under which the registration token will be created. On the *Create Registration Token* page, complete the following:

- In the Description field, enter a unique description for the token. In this example, security license – web filtering is entered.
- In the Expire After field enter a value between 1 to 365 days. Cisco recommends the value 30 days for this field; however, you may edit the value to fit your needs.
- In the Max. Number of Uses field enter a value to define the number of times you want to use that token. The token will expire when either the amount of days or the maximum number of uses is reached.
- Check the Allow export-controlled functionality on the products registered with this token checkbox to enable the export-controlled functionality for tokens of a product instance in your virtual account. Uncheck the checkbox if you do not want to allow the export-controlled functionality to be made available for use with this token. Use this option only if you are compliant with the export-controlled functionality. Some export-controlled features are restricted by the United States Department of Commerce. These

features are restricted for products registered using this token when you uncheck the checkbox. Any violations are subjected to penalties and administrative charges.

- Click **Create Token** to generate the token.

Create Registration Token ? ×

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description : **1**

* Expire After: **2** Days
Between 1 - 365, 30 days recommended

Max. Number of Uses: **3**

The token will be expired when either the expiration or the maximum uses is reached

Allow export-controlled functionality on the products registered with this token **4**

5

You have now successfully generated a product instance registration token.

| Token | Expiration Date | Uses | Export-Controlled | Description | Created By | Actions |
|---|---------------------------------|---------|-------------------|----------------------------------|------------|---------------------------|
| <input type="text" value="ITMGZIN..."/> | 2019-Sep-08 09:46:20 (in 30...) | 0 of 10 | Allowed | security license - web filtering | | Actions ▾ |

The token will be expired when either the expiration or the maximum uses is reached

Step 6

Click the **arrow icon** in the *Token* column, to copy the token to the clipboard press **ctrl + c** on your keyboard.

Token ? ×

Press ctrl + c to copy selected text to clipboard. **2**

1

The token will be expired when either the expiration or the maximum uses is reached

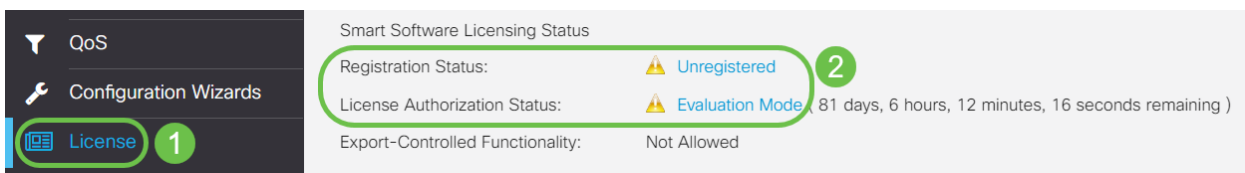
Step 7 (Optional)

Click the **Actions** drop-down menu, choose **Copy** to copy the token to the clipboard or **Download...** to download a text file copy of the token from which you may copy.



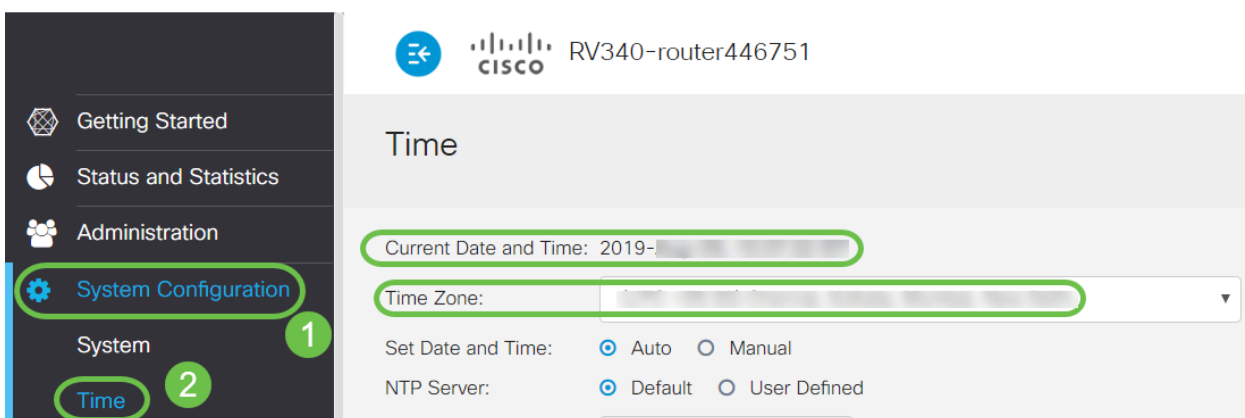
Step 8

Navigate to **License** and verify the *Registration Status* is showing as *Unregistered* and *License Authorization Status* is showing as *Evaluation Mode*.



Step 9

Navigate to **System Configuration > Time** and verify the *Current Date and Time* and *Time Zone* are reflecting correctly as per your time zone.



Step 10

Navigate to **License**. Paste the copied token in step 6 on the text box under the *License* tab by selecting **ctrl + v** on your keyboard. Click **Register**.

Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
Routing
Firewall
VPN
Security
QoS
Configuration Wizards
License 1

License

You are currently running in evaluation mode, to register an account:

- Ensure this product has internet access.
- [Click here](#) to access your Cisco Smart Account.
- Navigate to the Virtual Account section which contains licenses.
- Generate and copy a token for the specific license to be applied to this device.
- Paste the token into the box below.

2

3E4LTE1Njc5MzU5%0AODA4MTh8dFh07

* Click **Register 3**

Learn More about [Smart Software Licensing](#)

Smart Software Licensing Status

Registration Status: ⚠ **Unregistered**

License Authorization Status: ⚠ **Evaluation Mode (81 days, 6 hours, 12 minutes, 14 seconds remaining)**

Export-Controlled Functionality: **Not Allowed**

The registration may take a few minutes. Do not leave the page as the router attempts to contact the license server.

Step 11

You should now have successfully registered and authorized your RV345P Series router with a Smart License. You will get a notification on the screen *Registration completed successfully*. Also, you will be able to see that the *Registration Status* is showing as *Registered* and *License Authorization Status* is showing as *Authorized*.

RV340-router446751

Registration completed successfully

License

To view and manage Smart Software Licenses for your Cisco Smart Account, go to [Smart Licensing Manager](#) **Actions**

Smart Software Licensing Status

Registration Status: ✔ **Registered** (, 2019)

License Authorization Status: ✔ **Authorized** (, 2019)

Smart Account: Cisco Demo Customer Smart Account

Virtual Account: ...

PID: RV340-K9

Export-Controlled Functionality: Allowed

Step 12 (Optional)

To view more detail of the *Registration Status* of the license, hover your pointer over the *Registered* status. A dialog message appears with the following information:

License

To view and manage Smart Software Licenses for your Cisco Smart Account, go to [Smart Licensing Manager](#) **Actions** ▾

Smart Software Licensing Status

Registration Status: **Registered**

License Authorization Status: **Authorized (A)**

Smart Account: [REDACTED]

Virtual Account: [REDACTED]

PID: RV340-K9

Export-Controlled Functionality: Allowed

This product is registered for Smart Software Licensing

Initial Registration: [REDACTED] 2019 11:01:37 (Succeed)

Next Renewal Attempt: [REDACTED] 2020 11:01:36

Registration Expire: [REDACTED] 2020 10:55:01

- Initial Registration — This area indicates the date and time the license was registered.
- Next Renewal Attempt — This area indicates the date and time the router will attempt to renew the license.
- Registration Expire — This area indicates the date and time the registration expires.

Step 13

On the *License* page verify the *Security-License* status is showing *Authorized*. You may also click on the **Choose License** button to verify the *Security-License* is enabled.

If you run into any issues on this step, you may need to reboot your router.

Choose Smart Licenses

Choose Smart Licenses to be used by this product. Ensure you have a sufficient number of licenses in the Virtual Account associated with this product, otherwise it will be out of compliance.

| Enable | Name (Version) | Description | Count |
|-------------------------------------|------------------|--|-------|
| <input checked="" type="checkbox"/> | Security-License | Anti Threat Services: IPS, AppID, Dynamic W... | -- |

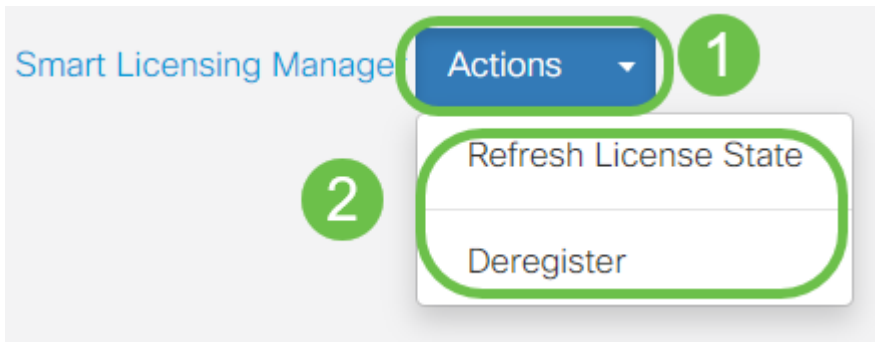
Save and Authorize Cancel

Smart License Usage

| Name | Description | Count | Status |
|------------------|--|-------|------------|
| Security-License | Anti Threat Services: IPS, AppID, Dynamic Web Filter, G... | -- | Authorized |

Step 14 (Optional)

To *Refresh License State* or *Deregister* the license from the router, click on the *Smart Licensing Manager* **Actions** drop-down menu and select an action item.



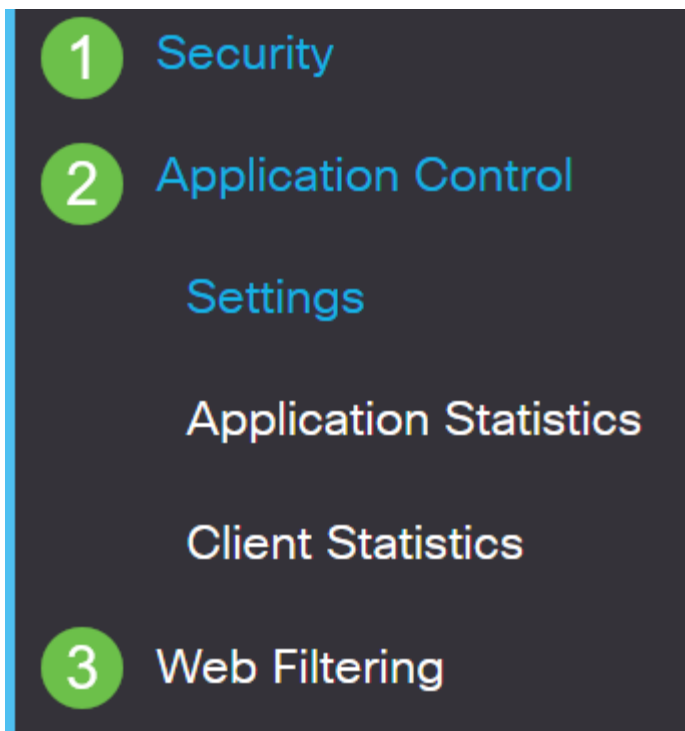
Now that you have your license on the router, you need to complete the steps in the next section.

Web Filtering on the RV345P Router

You have 90 days after activation to use web filtering at no cost. After the free trial, if you want to continue using this feature, you need to purchase a license. [Click to go back to that section.](#)

Step 1

Log into the web-based utility and choose **Security > Application Control > Web Filtering**.



Step 2

Select the **On** radio button.

Web Filtering


Web Filtering: On Off

Step 3

Click the **add icon**.

Web Filtering Policies



Policies 

Step 4

Enter a *Policy Name*, *Description*, and the *Enable* checkbox.

Policy Profile-Add/Edit

Policy Name:

1

Weekdays

Description:

2

Default-High

Enable:

3



If Content Filtering is enabled on your router, a notification will appear to inform you that Content Filtering has been disabled and that the two features cannot be enabled simultaneously. Click **Apply** to proceed with the configuration.

Step 5

Check the Web Reputation checkbox to enable filtering based on a web reputation index.

Web Reputation



Content will be filtered according to the notoriety of a website or URL based on a web reputation index. If the score falls below 40, the website will be blocked. To read more about the web reputation technology, click [here](#) for more details.

Step 6

From the *Device Type* drop-down list, select the source/destination of the packets to be filtered. Only one option can be chosen at a time. The options are:

- ANY — Choose this to apply the policy to any device.
- Camera — Choose this to apply the policy to cameras (such as IP security cameras).
- Computer — Choose this to apply the policy to computers.
- Game_Console — Choose this to apply the policy to Gaming Consoles.
- Media_Player — Choose this to apply the policy to Media Players.
- Mobile — Choose this to apply the policy to mobile devices.
- VoIP — Choose this to apply the policy to Voice over Internet Protocol devices.

Policy Profile-Add/Edit

IP Group:

Any



Device Type:

ANY



OS Type:

ANY

Camera

Computer

Game_Console

Media_Player

Mobile

VoIP

Exclusion List Table



Step 7

From the *OS Type* drop-down list, choose an Operating System (OS) to which the policy should be applicable. Only one option can be chosen at a time. The options are:

- ANY — Applies the policy to any type of OS. This is the default.
- Android — Applies the policy to Android OS only.
- BlackBerry — Applies the policy to Blackberry OS only.
- Linux — Applies the policy to Linux OS only.
- Mac_OS_X — Applies the policy to Mac OS only.
- Other — Applies the policy to an OS that is not listed.
- Windows — Applies the policy to the Windows OS.
- iOS — Applies the policy to iOS OS only.

Application:

Application List Table

Category ⇅

IP Group:

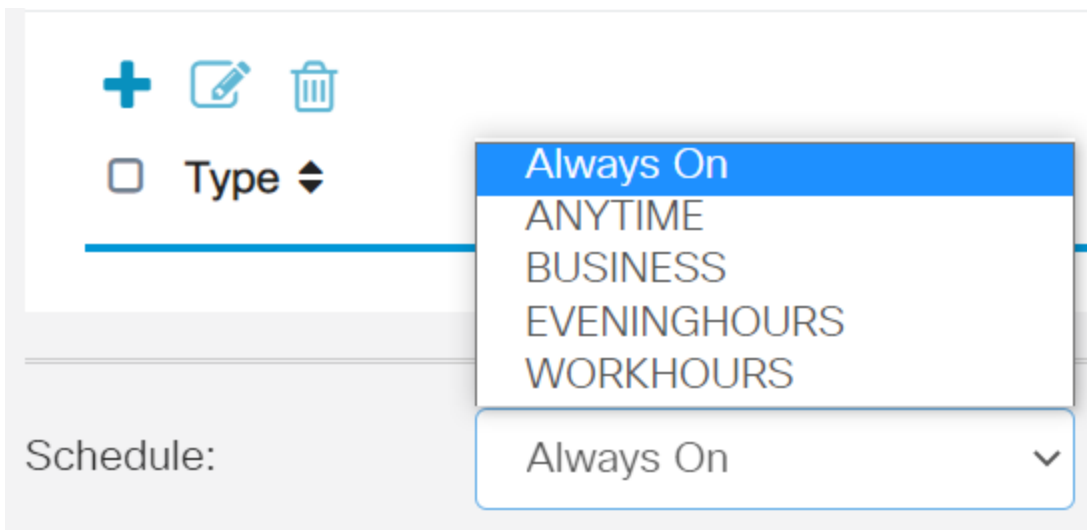
Device Type:

OS Type: ▼

- ANY
- Android
- BlackBerry
- Linux
- Mac_OS_X
- Other
- Windows
- iOS

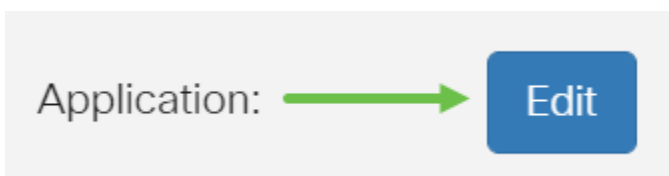
Step 8

Scroll down to the *Schedule* section and select the option that best fits your needs.



Step 9

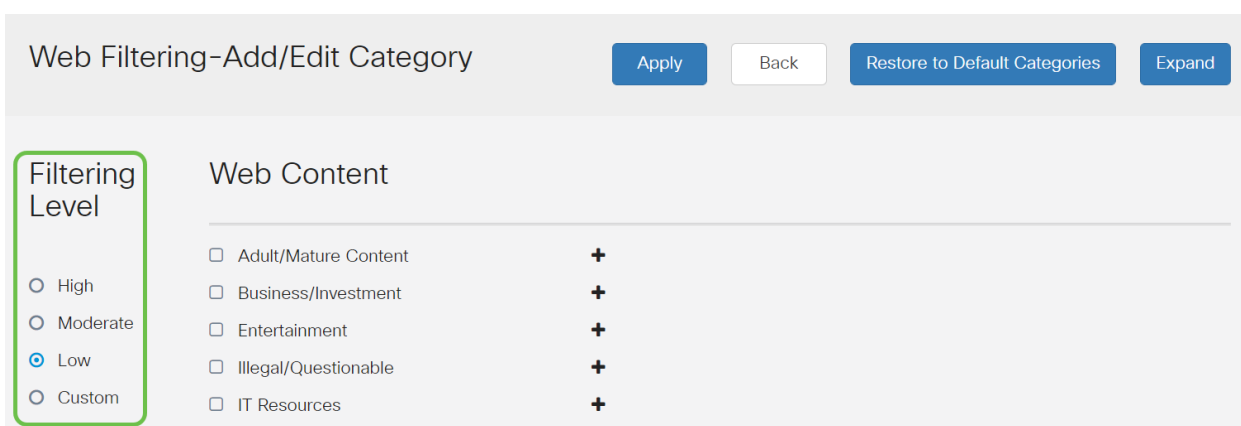
Click the **edit icon**.



Step 10

In the Filtering Level column, click a radio button to quickly define the filtering extent that would best fit the network policies. The options are High, Moderate, Low, and Custom. Click on any of the filtering levels below to know the specific pre-defined sub-categories filtered to each of their enabled Web Content Category. Pre-defined filters cannot be altered any further and are greyed out.

- **Low** — This is the default option. Security is enabled with this option.
- **Moderate** — Adult/Mature Content, Illegal/Questionable, and Security are enabled with this option.
- **High** — Adult/Mature Content, Business/Investment, Illegal/Questionable, IT Resources, and Security are enabled with this option.
- **Custom** — No defaults are set to allow user-defined filters.



Step 11

Enter the web content that you want to filter. Click on the **plus icon** if you want more detail on one section.

Web Filtering-Add/Edit Category

Apply Back Restore to Default Categories Expand

Filtering Level

Web Content

- Adult/Mature Content +
- Business/Investment +
- Entertainment +
- Illegal/Questionable +
- IT Resources +
- Lifestyle/Culture +
- Other +
- Security +

○ High

○ Moderate

● Low

○ Custom

Step 12 (Optional)

To view all Web Content sub-categories and descriptions, you can click the **Expand** button.

Apply Back Restore to Default Categories Expand

Step 13 (Optional)

Click **Collapse** to collapse the sub-categories and descriptions.

Apply Back Restore to Default Categories Collapse

Step 14 (Optional)

To return to the default categories, click **Restore to Default Categories**.

Apply Back Restore to Default Categories Collapse

Step 15

Click **Apply** to save the configuration and to return to the Filter page to continue the setup.

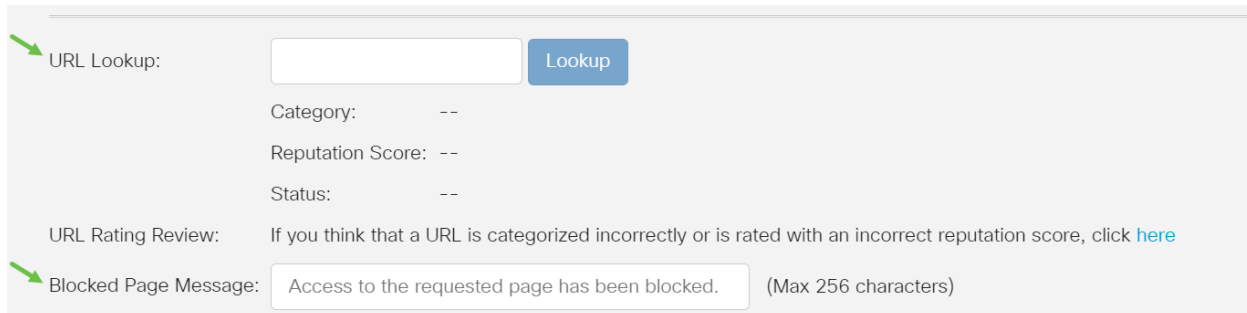
Apply Cancel



In the Application List Table, the corresponding sub-categories based on the chosen filtering level will populate the table.

Step 16 (Optional)

Other options include URL Lookup and the message that shows when a requested page has been blocked.



The screenshot shows a configuration panel with the following elements:

- URL Lookup:** A text input field with a blue "Lookup" button to its right.
- Category:** A dropdown menu showing "--".
- Reputation Score:** A dropdown menu showing "--".
- Status:** A dropdown menu showing "--".
- URL Rating Review:** A text area containing the message: "If you think that a URL is categorized incorrectly or is rated with an incorrect reputation score, click [here](#)".
- Blocked Page Message:** A text input field containing "Access to the requested page has been blocked." with a character count "(Max 256 characters)" to its right.

Step 17 (Optional)

Click **Apply**.



The screenshot shows two buttons: a blue "Apply" button and a white "Cancel" button with a grey border.

Step 18

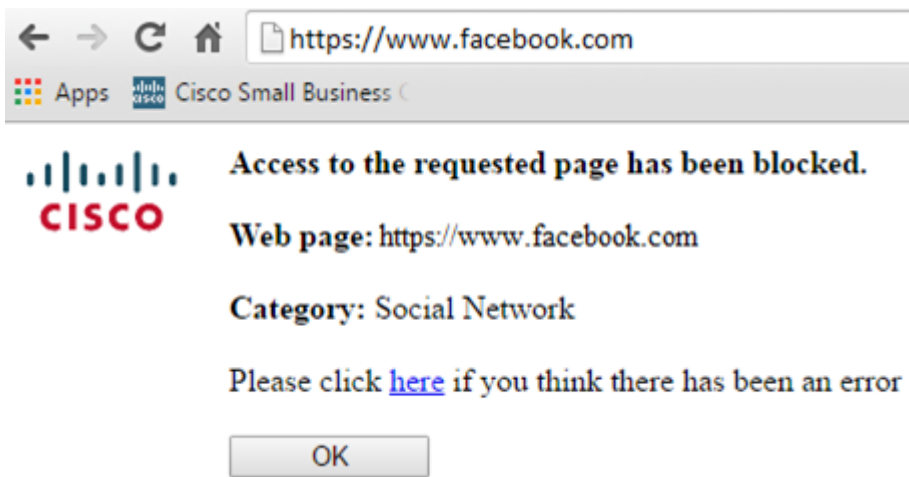
To save the configuration permanently, go to the *Copy/Save Configuration* page or click the **save icon** at the upper portion of the page.



Step 19 (Optional)

To verify that a website or URL has been filtered or blocked, launch a web browser or open a new tab in your browser. Enter the domain name you have block listed or have filtered to be blocked or denied.

In this example, we used www.facebook.com.



You should now have successfully configured web filtering on your RV345P Router. Since you are using the RV Security License for web filtering, you probably don't need Umbrella. If you also want Umbrella, [click here](#). If you have enough security, [click to skip to the next section](#).

Troubleshooting

If you've purchased a license but it is not appearing in your virtual account, you have two options:

1. Follow up with the reseller to request they make the transfer.
2. Reach out to us and we'll get in touch with the reseller.

Ideally, you wouldn't have to do either, but if you arrive at this crossroad we're happy to help! To make the process as expedient as possible, you will need the credentials in the table above as well as those outlined below.

| Information Required | Locating the information |
|---|--|
| License Invoice | This should be emailed to you after completing the purchase of the licenses. |
| Cisco Sales Order number | You may need to go back to the reseller to get this. |
| Screenshot of your Smart Account license page | Taking a screenshot captures the contents of your screen for sharing with our team. If you're unfamiliar with screenshots you can use the below methods. |

Screenshots

Once you have a token, or if you are troubleshooting, it is recommended that you take a screenshot to capture the contents of your screen.

Given the differences in the procedure required to capture a screenshot, see below for links specific to your operating system.

- [Windows](#)

- [MAC](#)
- [iPhone/iPad](#)
- [Android](#)

Umbrella RV Branch License (Optional)

Umbrella is a simple, yet very effective cloud security platform from Cisco.

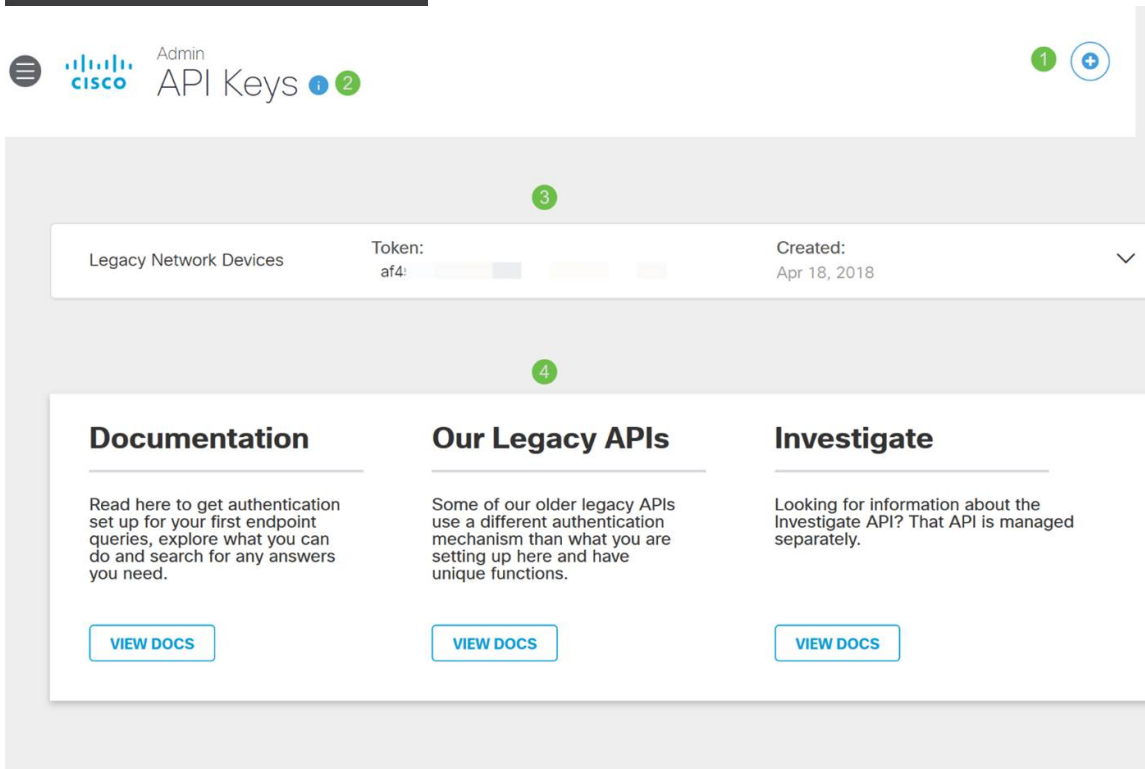
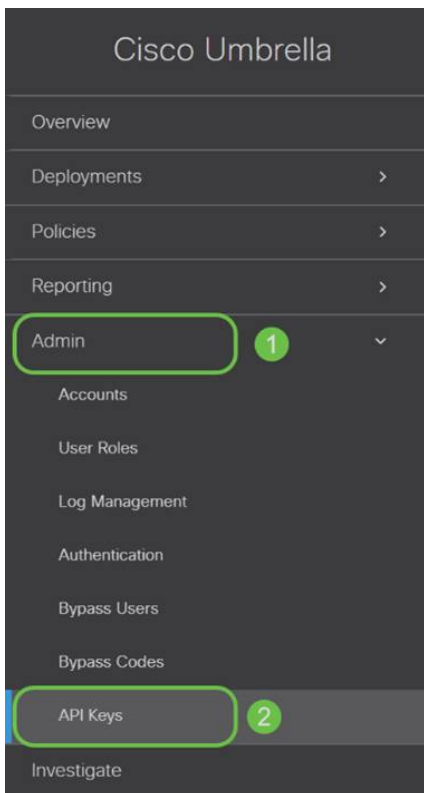
Umbrella operates in the cloud and performs many security-related services. From emergent threat to post-event investigation. Umbrella discovers and prevents attacks across all ports and protocols.

Umbrella uses DNS as its main vector for defense. When users enter a URL in their browser bar and hit *Enter*, Umbrella participates in the transfer. That URL passes to Umbrella's DNS resolver, and if a security warning associates with the domain, the request is blocked. This telemetry data transfers and is analyzed in microseconds, adding nearly no latency. Telemetry data uses logs and instruments tracking billions of DNS requests throughout the world. When this data is pervasive, correlating it across the globe enables rapid response to attacks as they begin. See Cisco's privacy policy here for more information: [full policy](#), [summary version](#). Think of telemetry data as data derived from tools and logs.

Visit [Cisco Umbrella](#) to learn more and to create an account. If you run into any issues, [check here for documentation](#), and [here for Umbrella Support options](#).

Step 1

After logging into your Umbrella Account, from the *Dashboard* screen click on **Admin** > **API Keys**.

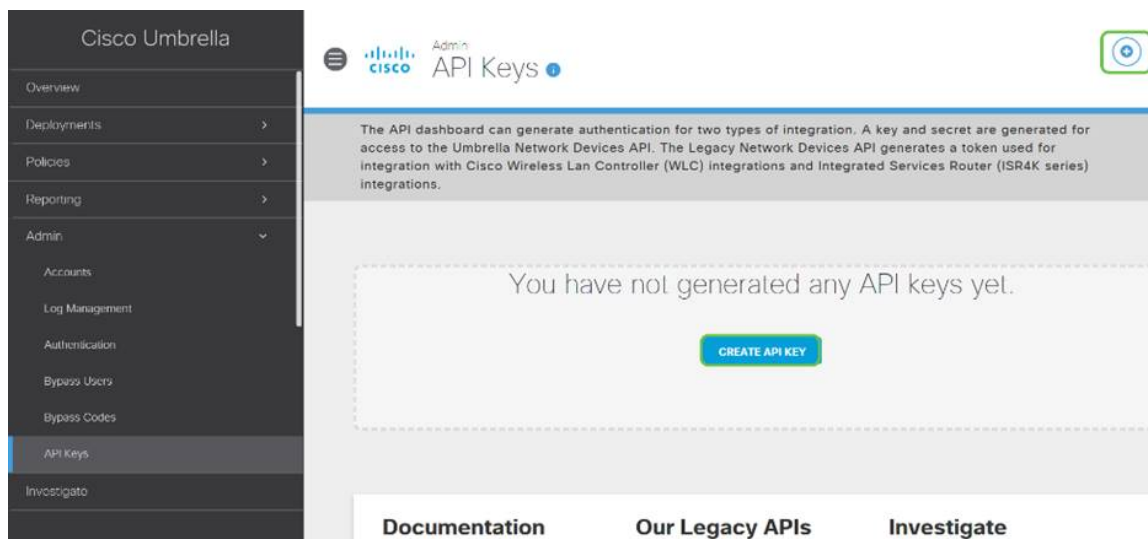


Anatomy of the API Keys Screen (with pre-existing API key)

1. Add API Key – Initiates the creation of a new key for use with the Umbrella API.
2. Additional Info – Slides down/up with an explainer for this screen.
3. Token Well – Contains all keys and tokens created by this account. (Populates once a key has been created)
4. Support Documents – Links to documentation on the Umbrella site pertaining to the topics in each section.

Step 2

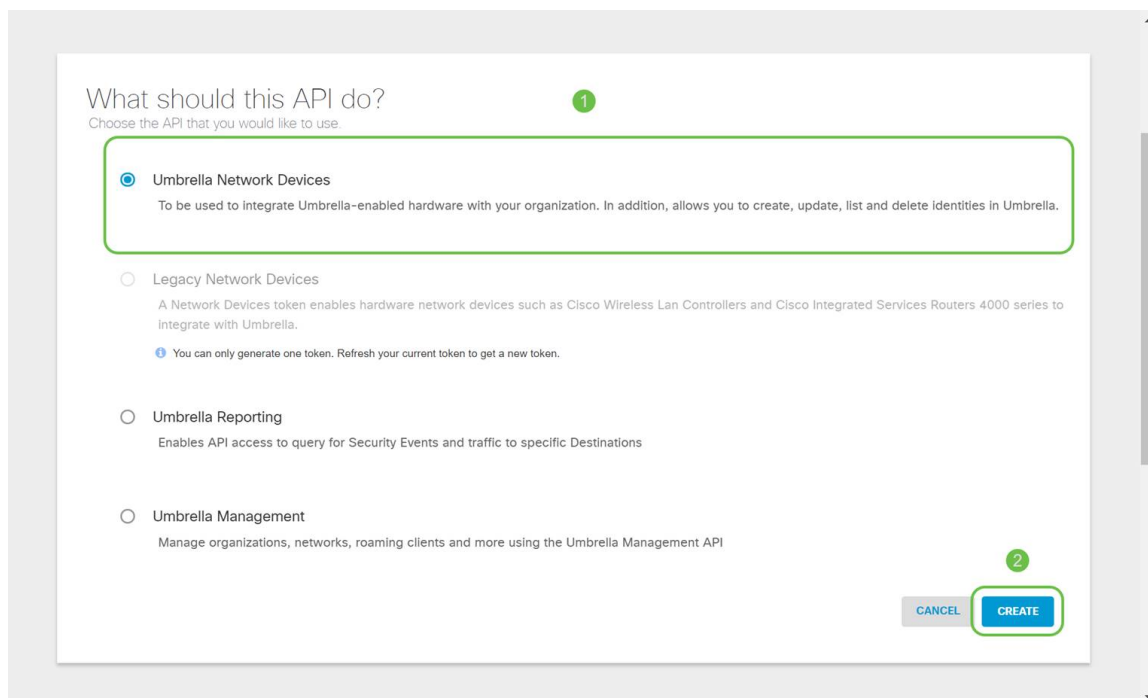
Click on the **Add API Key** button in the upper-right hand corner or click the **Create API Key** button. They both function the same.



The above screenshot would be similar to what you would see opening this menu for the first time.

Step 3

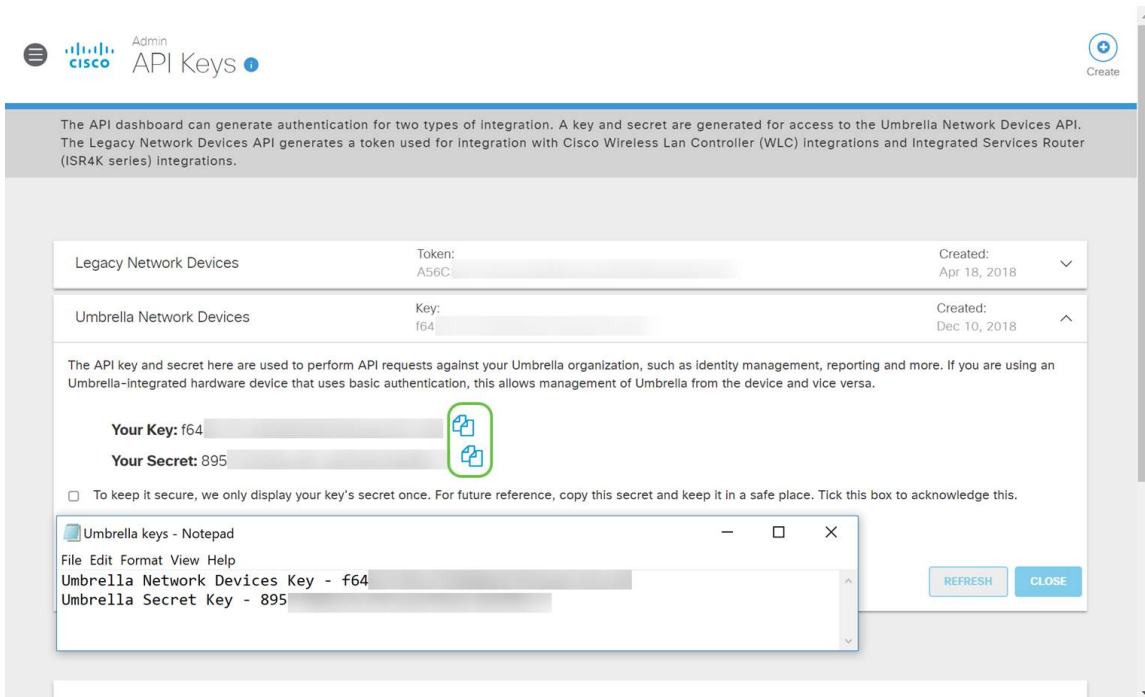
Select **Umbrella Network Devices** and then click the **Create** button.



Step 4

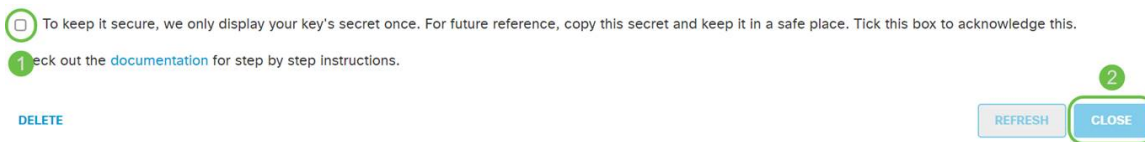
Open a text editor such as notepad then click the **copy icon** to the right of your API and API *Secret Key*, a pop-up notification will confirm the key is copied to your clipboard. One at a time, paste your secret and API key into the document, labeling

them for future reference. In this case, its label is “Umbrella network devices key”. Then save the text file to a secure location that's easy to access later.



Step 5

After you've copied the key and secret key to a safe location, from the *Umbrella API screen* click the **checkbox** to confirm to complete acknowledgment of the temporary viewing of the secret key, then click the **Close** button.



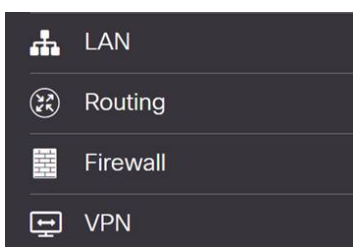
If you lose or accidentally delete the secret key, there is no function or support number to call to retrieve this key. If lost, you will need to delete the key and re-authorize the new API key with each device you wish to protect with Umbrella.

Configuring Umbrella on your RV345P

Now that we've created API keys within Umbrella, you can take those keys and install them on your RV345P.

Step 1

After logging into your RV345P router, click on **Security > Umbrella** in the sidebar menu.



Step 2

The Umbrella API screen has a range of options, begin enabling Umbrella by clicking the **Enable** checkbox.

Cisco Umbrella

Apply Cancel

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

Enable
 Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
 - Go to [DNS-O-MATIC website](#), create an account and add your OpenDNS account to it.
 - Go to [DNS-O-MATIC Settings](#) to enable DNS-O-MATIC so your WAN IP change can be propagated to OpenDNS/Umbrella.

Advanced Configuration

Local Domain To Bypass (Optional): +

DNSCrypt: Enable

Public Key:
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:30C8:D666:8D0C:BED4:BFAB:CA4:

If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Step 3 (Optional)

On by default, the box *Block LAN DNS Queries* is selected. This neat feature automatically creates access control lists on your router which will prevent DNS traffic from going out to the Internet. This feature forces all domain translation requests to be directed through the RV345P and is a good idea for most users.

Step 4

The next step plays out in two different ways. They both depend on the setup of your network. If you use a service like DynDNS or NoIP, you leave the default naming scheme of "Network". You will need to log into those accounts to ensure Umbrella interfaces with those services as it provides protection. For our purposes we're relying on "Network Device", so we click on the bottom radio button.

Cisco Umbrella

Apply Cancel

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

Enable
 Block LAN DNS query

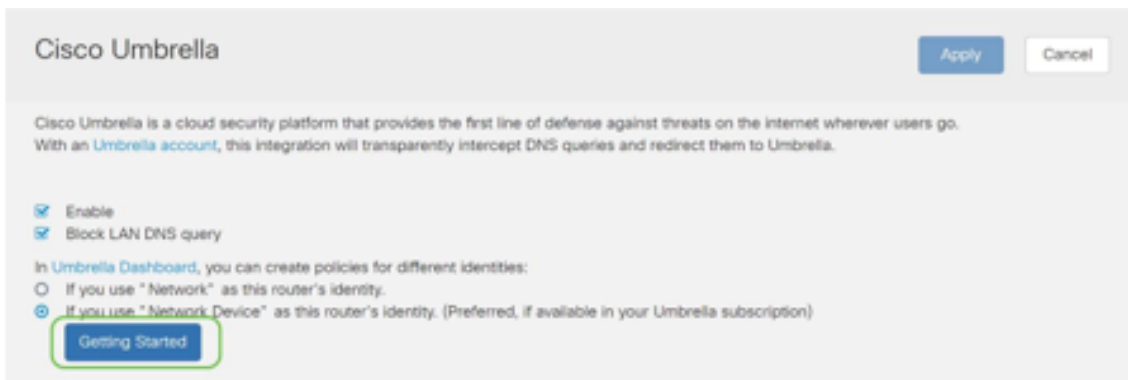
In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Getting Started

Step 5

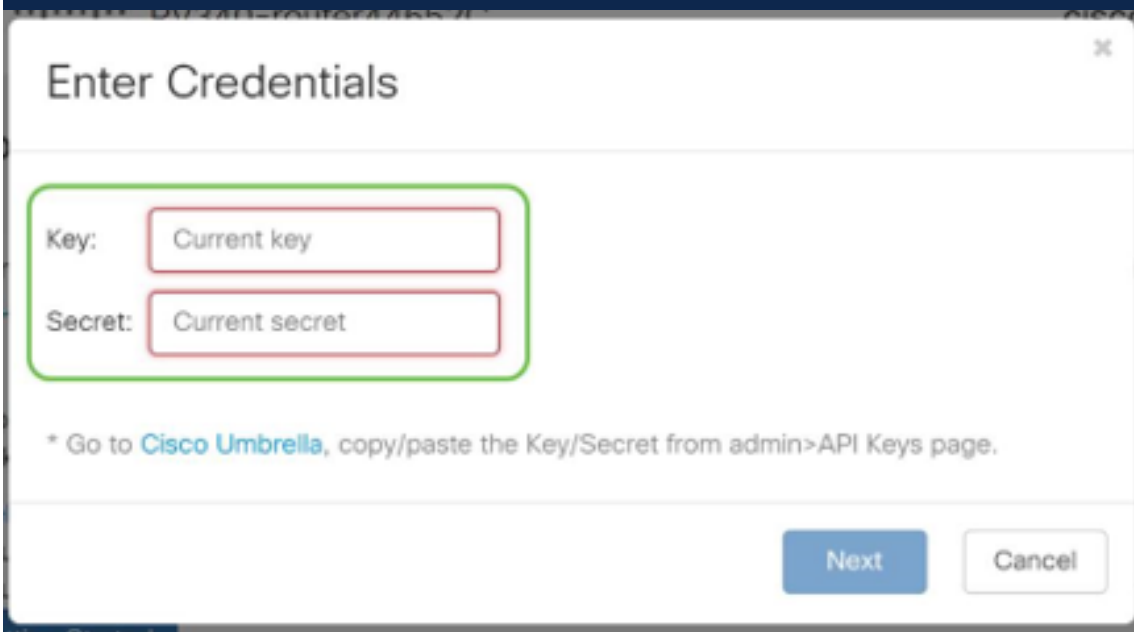
Click **Getting Started**.



Step 6

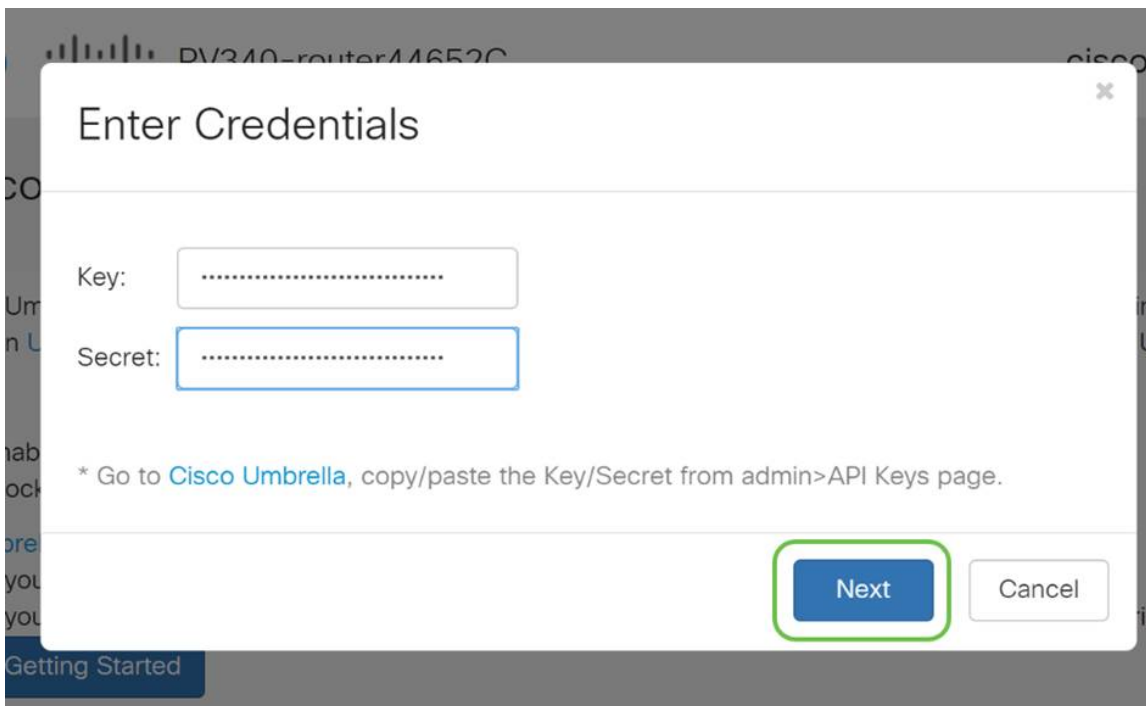
Enter the **API Key** and **Secret Key** to the text boxes.

Calling it out twice so you know it's important! If you lose or accidentally delete the secret key, there is no function or support number to call to retrieve this key. Keep it secret and safe. If lost, you will need to delete the key and re-authorize the new API key with each device you wish to protect with Umbrella.



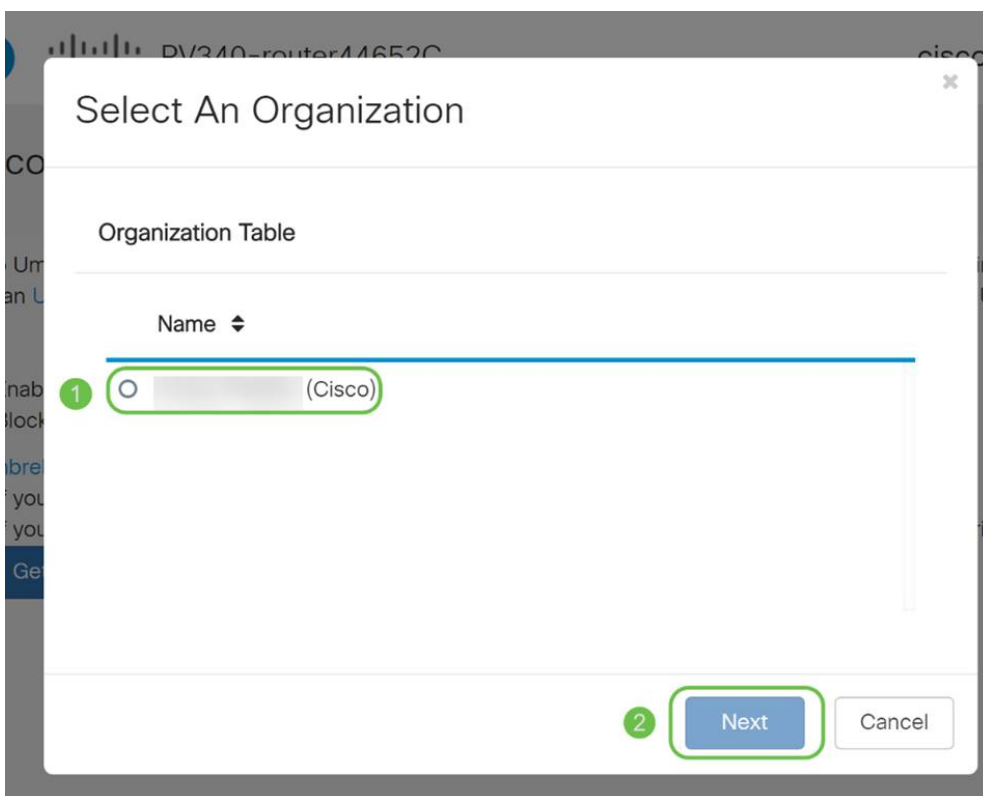
Step 7

After entering your API and Secret Key, click the **Next** button.



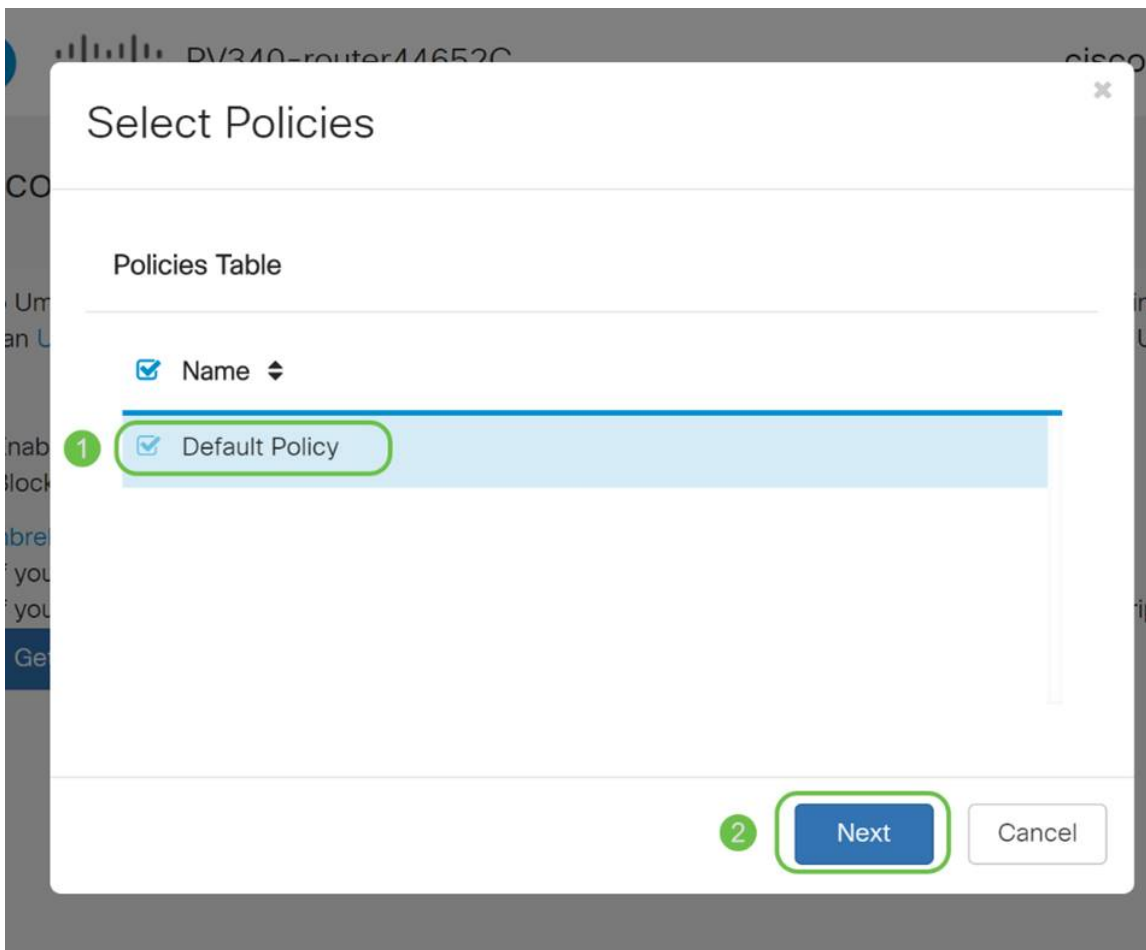
Step 8

In the next screen, select the **organization** you wish to associate with the router. Click **Next**.



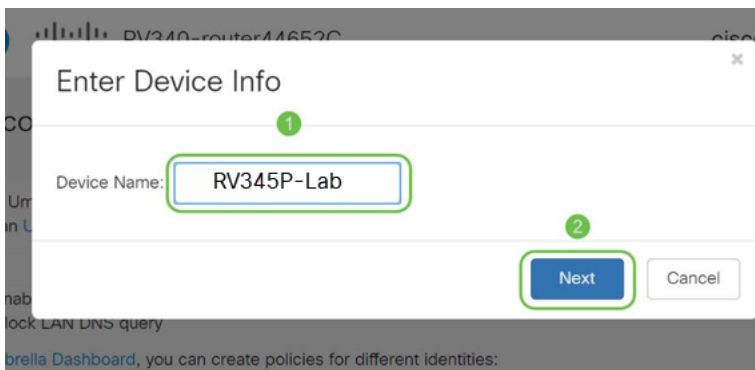
Step 9

Select the policy to apply to traffic routed by the RV345P. For most users, the default policy will provide enough coverage.



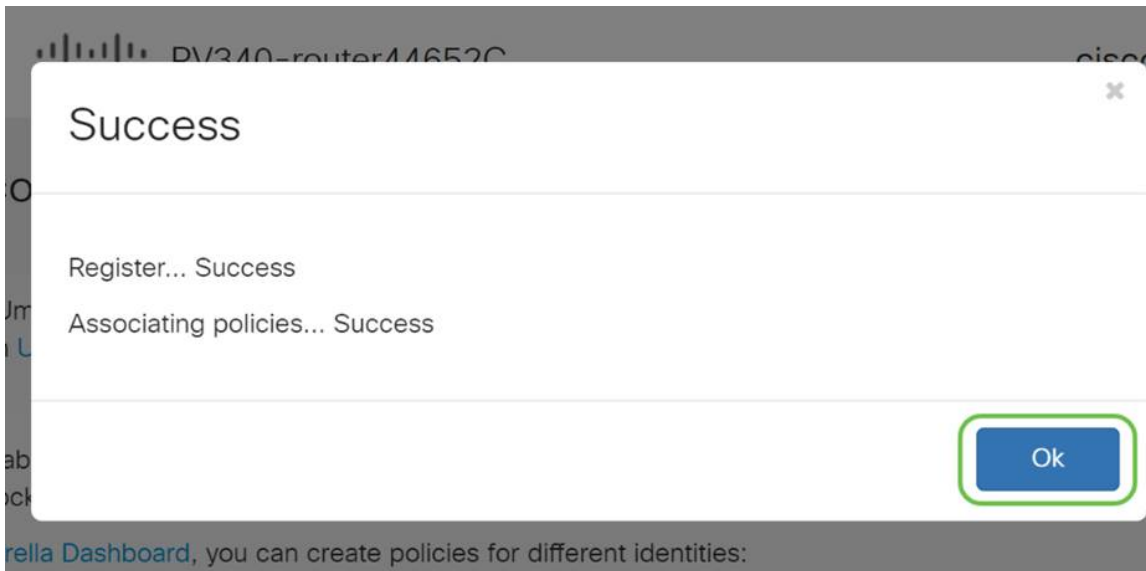
Step 10

Assign a name to the device so it may be designated in Umbrella reporting. In our setup, we have named it *RV345P-Lab*.



Step 11

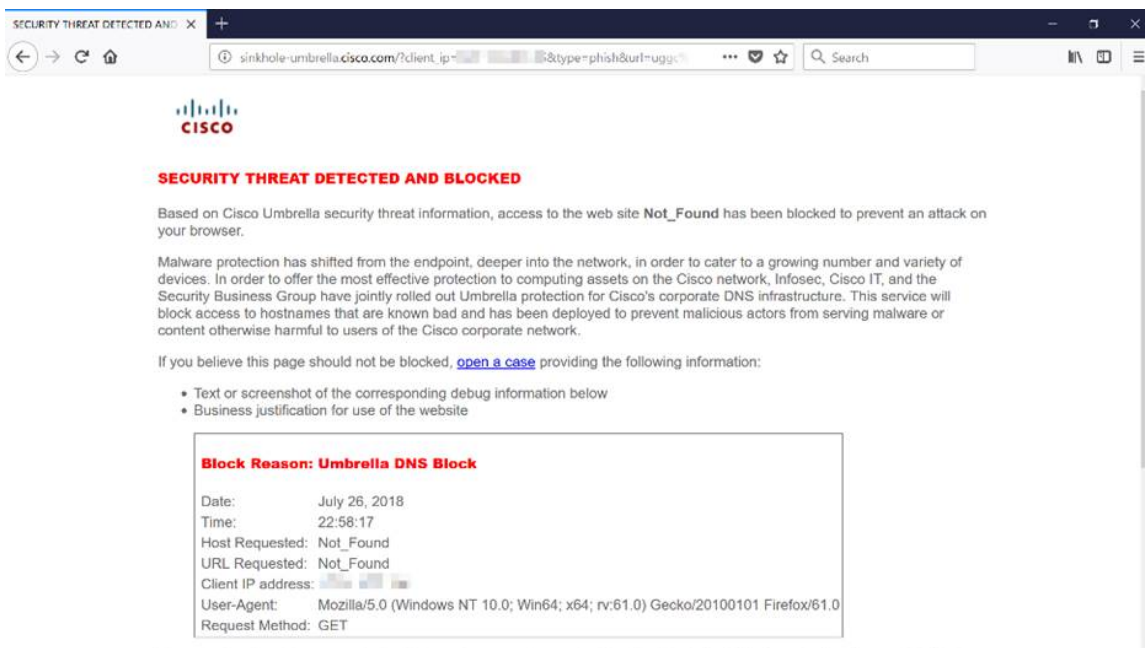
The next screen will validate your chosen settings and provide an update when associated successfully. Click **OK**.



Confirmation

Congratulations, you are now protected by Cisco Umbrella. Or are you? Let's be sure by double-checking with a live example, Cisco has created a website dedicated to determining this as quickly as the page loads. [Click here](#) or type <https://InternetBadGuys.com> into the browser bar.

If Umbrella is configured correctly, you will be greeted by a screen similar to this.



Other Security Options

Are you worried that someone would attempt unauthorized access to the network by unplugging an Ethernet cable from a network device and connecting to it? In this case, it is important to register a list of allowed hosts to directly connect to the router with their respective IP and MAC addresses. Instructions can be found in the article [Configure IP Source Guard on the RV34x Series Router](#).

VPN Options

A Virtual Private Network (VPN) connection allows users to access, send, and receive data to and from a private network by means of going through a public or shared network such as the Internet but still ensuring a secure connection to an underlying network infrastructure to protect the private network and its resources.

A VPN tunnel establishes a private network that can send data securely using encryption and authentication. Corporate offices mostly use VPN connection since it is both useful and necessary to allow their employees to have access to their private network even if they are outside the office.

The VPN allows a remote host to act as if they were located on the same local network. The router supports up to 50 tunnels. A VPN connection can be set up between the router and an endpoint after the router has been configured for Internet connection. The VPN client is entirely dependent on the settings of the VPN router to be able to establish a connection.

If you are not sure which VPN best fits your needs, check out [Cisco Business VPN Overview and Best Practices](#).

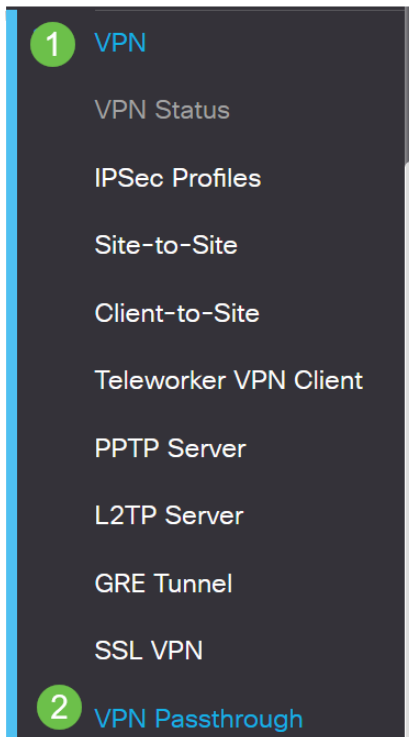
AnyConnect VPN is the only Cisco VPN supported product listed in this configuration guide. Third-party, non-Cisco products, including TheGreenBow and Shrew Soft are not supported by Cisco. They are included strictly for guidance purposes. If you need support on these beyond the article, you should contact that third-party for support.

If you are not planning on setting up a VPN, you can [click to jump to the next section](#).

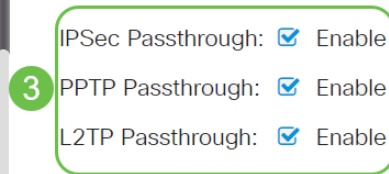
VPN Passthrough

Generally, every router supports Network Address Translation (NAT) in order to conserve IP addresses when you want to support several clients with the same Internet connection. However, Point-to-Point Tunneling Protocol (PPTP) and Internet Protocol Security (IPsec) VPN do not support NAT. This is where the VPN Passthrough comes in. A VPN Passthrough is a feature that allows VPN traffic generated from VPN clients connected to this router to pass through this router and connect to a VPN endpoint. The VPN Passthrough allows PPTP and IPsec VPN only to pass through to the Internet, which is initiated from a VPN client, and then reach the remote VPN gateway. This feature is commonly found on home routers that support NAT.

By default, IPsec, PPTP, and L2TP Passthrough are enabled. If you want to view or adjust these settings, select **VPN > VPN Passthrough**. View or adjust as needed.



VPN Passthrough



AnyConnect VPN

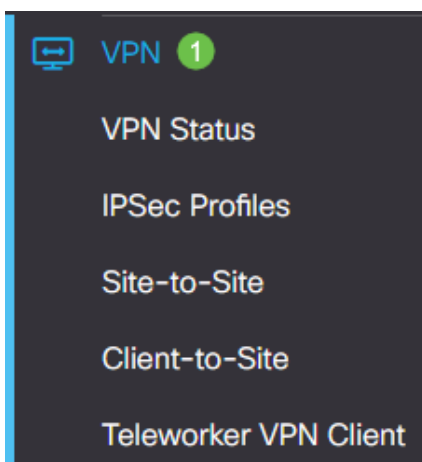
There are several advantages to using Cisco AnyConnect:

1. Secure and persistent connectivity
2. Persistent security and policy enforcement
3. Deployable from the Adaptive Security Appliance (ASA) or from Enterprise Software Deployment Systems
4. Customizable and translatable
5. Easily configured
6. Supports both Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL)
7. Supports Internet Key Exchange version 2.0 (IKEv2.0) protocol

Configure AnyConnect SSL VPN on the RV345P

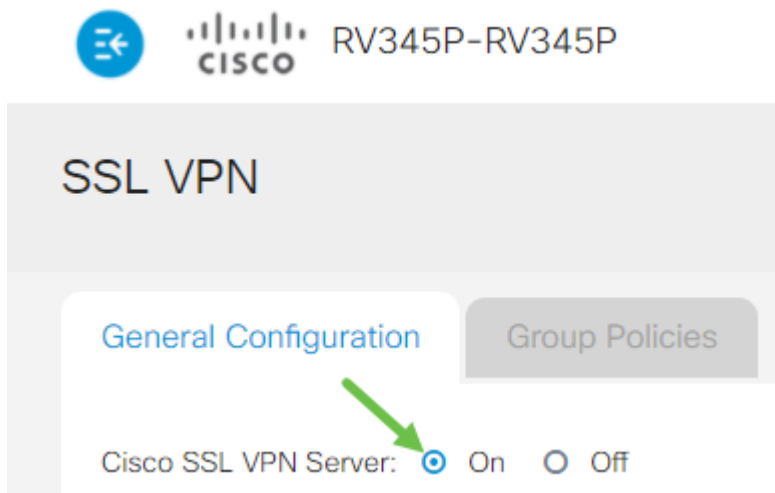
Step 1

Access the router web-based utility and choose **VPN > SSL VPN**.



Step 2

Click the **On** radio button to enable Cisco SSL VPN Server.



Mandatory Gateway Settings

Step 1

The following configuration settings are mandatory:

1. Choose the Gateway Interface from the drop-down list. This will be the port that will be used for passing traffic through the SSL VPN Tunnels. The options include: WAN1, WAN2, USB1, USB2
2. Enter the port number that is used for the SSL VPN gateway in the Gateway Port field ranging from 1 to 65535.
3. Choose the Certificate File from the drop-down list. This certificate authenticates users who attempt to access the network resource through the SSL VPN tunnels. The drop-down list contains a default certificate and the certificates that are imported.
4. Enter the IP address of the client address pool in the *Client Address Pool* field. This pool will be the range of IP addresses that will be allocated to remote VPN clients.

Make sure that the IP address range does not overlap with any of the IP addresses on the local network.

6. Choose the Client Netmask from the drop-down list.
7. Enter the client domain name in the *Client Domain* field. This will be the domain name that should be pushed to SSL VPN clients.
8. Enter the text that would appear as a login banner in the *Login Banner* field. This will be the banner that will be displayed each time a client logs in.

Mandatory Gateway Settings

Gateway Interface:

Step 2

Click **Apply**.



Optional Gateway Settings

Step 1

The following configuration settings are optional:

1. Enter a value in seconds for the Idle Timeout ranging from 60 to 86400. This will be the time duration that the SSL VPN session can remain idle.
2. Enter a value in seconds in the *Session Timeout* field. This is the time it takes for the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) session to time out after the specified idle time. The range is from 60 to 1209600.
3. Enter a value in seconds in the *ClientDPD Timeout* field ranging from 0 to 3600. This value specifies the periodic sending of HELLO/ACK messages to check the status of the VPN tunnel. This feature must be enabled on both ends of the VPN tunnel.
4. Enter a value in seconds in the *GatewayDPD Timeout* field ranging from 0 to 3600. This value specifies the periodic sending of HELLO/ACK messages to check the status of the VPN tunnel. This feature must be enabled on both ends of the VPN tunnel.
5. Enter a value in seconds in the *Keep Alive* field ranging from 0 to 600. This feature ensures that your router is always connected to the Internet. It will attempt to re-establish the VPN connection if it is dropped.
6. Enter a value in seconds for the duration of the tunnel to be connected in the *Lease Duration* field. The range is from 600 to 1209600.
7. Enter the packet size in bytes that can be sent over the network. The range is from 576 to 1406.
8. Enter the relay interval time in the *Rekey Interval* field. The Rekey feature allows the SSL keys to renegotiate after the session has been established. The range is from 0 to 43200.

Optional Gateway Settings

| | | |
|----------------------|------------------------------------|----------------------------|
| Idle Timeout: | <input type="text" value="3000"/> | sec. (Range: 60-86400) |
| Session Timeout: | <input type="text" value="60"/> | sec. (Range: 0,60-1209600) |
| Client DPD Timeout: | <input type="text" value="350"/> | sec. (Range: 0-3600) |
| Gateway DPD Timeout: | <input type="text" value="360"/> | sec. (Range: 0-3600) |
| Keep Alive: | <input type="text" value="40"/> | sec. (Range: 0-600) |
| Lease Duration: | <input type="text" value="43500"/> | sec. (Range: 600-1209600) |

Step 2

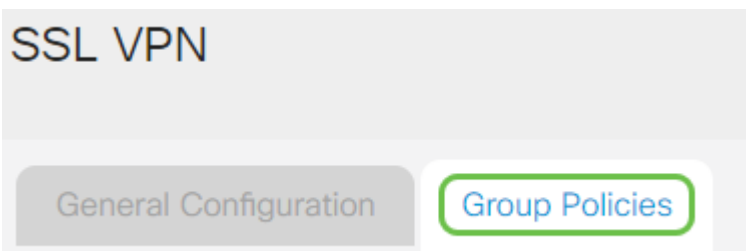
Click **Apply**.



Configure Group Policies

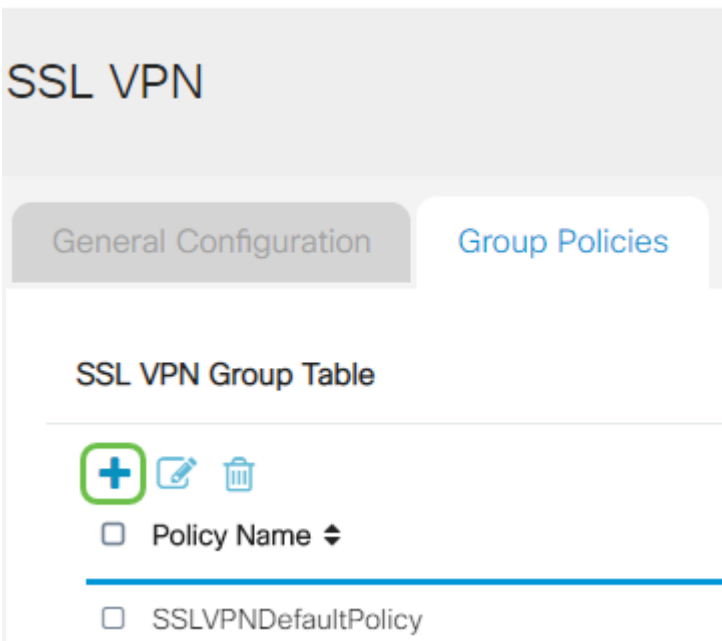
Step 1

Click the **Group Policies** tab.



Step 2

Click the **add icon** under the SSL VPN Group Table to add a group policy.



The SSL VPN Group table will show the list of group policies on the device. You can also edit the first group policy on the list, which is named SSLVPNDefaultPolicy. This is the default policy supplied by the device.

Step 3

1. Enter your preferred policy name in the *Policy Name* field.
2. Enter the IP address of the Primary DNS in the field provided. By default, this IP address is already supplied.

3. (Optional) Enter the IP address of the Secondary DNS in the field provided. This will serve as a backup in case the primary DNS failed.
4. (Optional) Enter the IP address of the primary WINS in the field provided.
5. (Optional) Enter the IP address of the secondary WINS in the field provided.
6. (Optional) Enter a description of the policy in the *Description* field.

SSLVPN Group Policy - Add/Edit

Basic Settings

| | |
|-----------------|---|
| Policy Name: | <input type="text" value="Group 1 Policy"/> |
| Primary DNS: | <input type="text" value="192.168.1.1"/> |
| Secondary DNS: | <input type="text" value="192.168.1.2"/> |
| Primary WINS: | <input type="text" value="192.168.1.1"/> |
| Secondary WINS: | <input type="text" value="192.168.1.2"/> |
| Description: | <input type="text" value="Group policy with split tunnel"/> |

Step 4 (Optional)

Click on a radio button to choose the IE Proxy Policy to enable Microsoft Internet Explorer (MSIE) proxy settings to establish VPN tunnel. The options are:

- None - Allows the browser to use no proxy settings.
- Auto - Allows the browser to automatically detect the proxy settings.
- Bypass-local - Allows the browser to bypass the proxy settings that are configured on the remote user.
- Disabled - Disables the MSIE proxy settings.

IE Proxy Settings

IE Proxy Policy: None Auto Bypass-local Disabled

Step 5 (Optional)

In the Split Tunneling Settings area, check the **Enable Split Tunneling** checkbox to allow Internet destined traffic to be sent unencrypted directly to the Internet. Full Tunneling sends all traffic to the end device where it is then routed to destination resources, eliminating the corporate network from the path for web access.

Split Tunneling Settings

Enable Split Tunneling

Step 6 (Optional)

Click on a radio button to choose whether to include or exclude traffic when applying the split tunneling.

Include Traffic Exclude Traffic

Step 7

In the Split Network Table, click the **add icon** to add a split Network exception.

Split Network Table



Step 8

Enter the IP address of the network in the field provided.

Split Tunneling Settings

Enable Split Tunneling

Split Selection Include Traffic Exclude Traffic

Split Network Table



Step 9

In the Split DNS Table, click the **add icon** to add a split DNS exception.

Split DNS Table



Step 10

Enter the Domain name in the field provided and then click **Apply**.

Split DNS Table



The router comes with 2 AnyConnect server licenses by default. This means that once you have AnyConnect client licenses, you can establish 2 VPN tunnels simultaneously with any other RV340 series router.

In short, the RV345P router does not need a license, but all clients will need one. AnyConnect client licenses allow desktop and mobile clients to access the VPN network remotely.

This next section details how to get licenses for your clients.

AnyConnect Mobility Client

A VPN client is software that is installed and ran on a computer that wishes to connect to the remote network. This client software must be set up with the same configuration as that of the VPN server such as the IP address and authentication information. This authentication information includes the username and the pre-shared key that will be used to encrypt the data. Depending on the physical location of the networks to be connected, a VPN client can also be a hardware device. This usually happens if the VPN connection is used to connect two networks that are in separate locations.

The Cisco AnyConnect Secure Mobility Client is a software application for connecting to a VPN that works on various operating systems and hardware configurations. This software application makes it possible for remote resources of another network to become accessible as if the user is directly connected to his network, but in a secure way.

Once the router is registered and configured with AnyConnect, the client can install licenses on the router from your available pool of licenses that you purchase, which is detailed in the next section.

Purchase License

You must purchase a license from your Cisco distributor or your Cisco partner. When ordering a license, you must provide your Cisco Smart Account ID or Domain ID in the form of [name@domain.com](#).

If you don't have a Cisco distributor or partner, you can locate one [here](#).

At the time of writing, the following Product SKUs can be used to purchase additional licenses in bundles of 25. Note that there are other options for the AnyConnect client licenses as outlined in the Cisco AnyConnect Ordering Guide, however, the Product ID listed would be the minimum requirement for full functionality.

Please note, the AnyConnect client license Product SKU listed first, provides licenses for a term of 1 year, and requires a minimum purchase of 25 licenses. Other product SKUs which are applicable to the RV340 series routers are also available with varying subscription levels, as follows:

- **LS-AC-PLS-1Y-S1** — 1-year Cisco AnyConnect Plus client license
- **LS-AC-PLS-3Y-S1** — 3-year Cisco AnyConnect Plus client license
- **LS-AC-PLS-5Y-S1** — 5-year Cisco AnyConnect Plus client license
- **LS-AC-PLS-P-25-S** — 25 pack Cisco AnyConnect Plus perpetual client license
- **LS-AC-PLS-P-50-S** — 50 pack Cisco AnyConnect Plus perpetual client license

Client Information

When your client sets up one of the following, you should send them these links:

- Windows: [AnyConnect on a Windows Computer](#)
- Mac: [Install AnyConnect on Mac](#).
- Ubuntu Desktop: [Installing and Using AnyConnect on Ubuntu Desktop](#)
- If you have problems, you can go to [Gather Information for Basic Troubleshooting on Cisco AnyConnect Secure Mobility Client Errors](#).

Verify AnyConnect VPN Connectivity

Step 1

Click on the **AnyConnect Secure Mobility Client icon**.

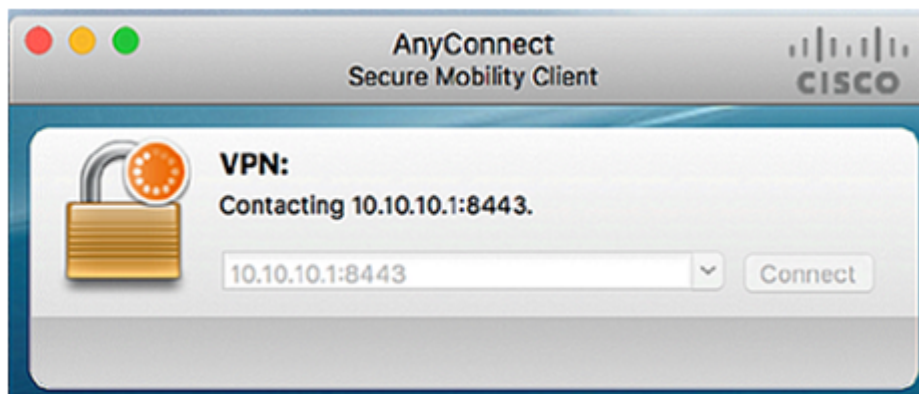


Step 2

In the AnyConnect Secure Mobility Client window, enter the gateway IP address and the gateway port number separated by a colon (:), and then click **Connect**.

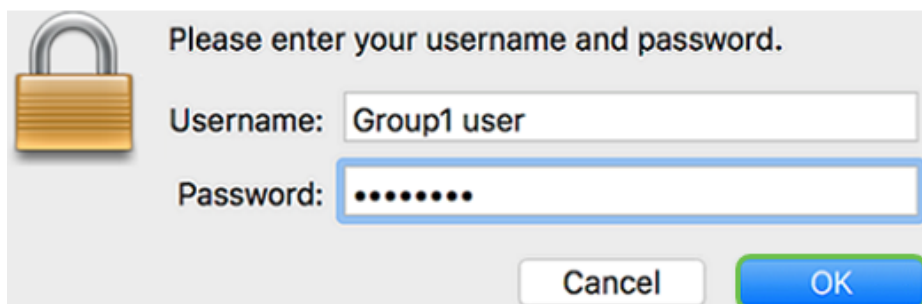


The software will now show that it is contacting the remote network.



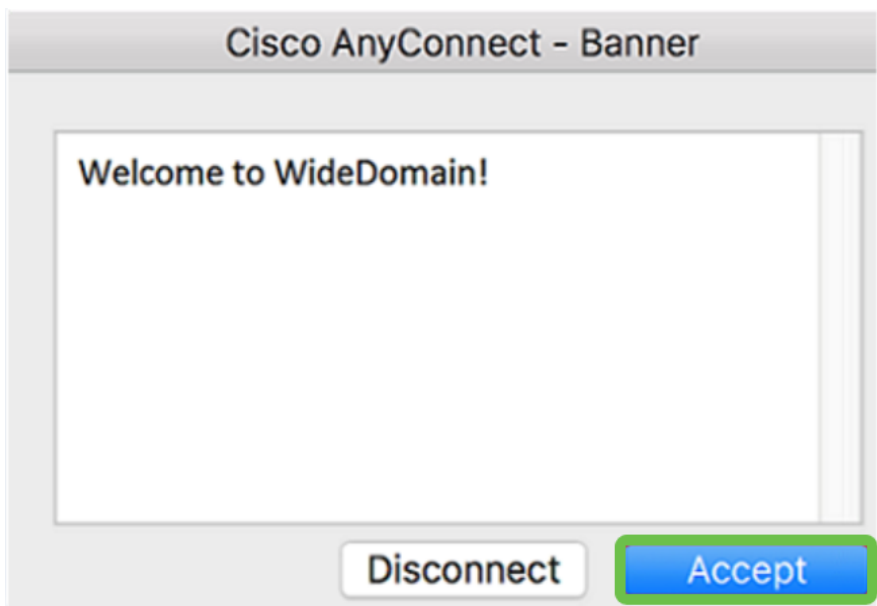
Step 3

Enter your server username and password in the respective fields and then click **OK**.

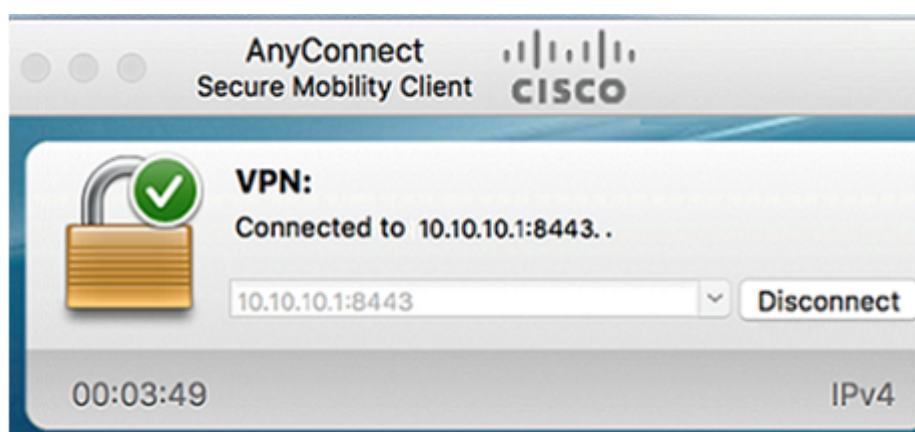


Step 4

As soon as the connection is established, the Login Banner will appear. Click **Accept**.



The AnyConnect window should now indicate the successful VPN connection to the network.



If you are now using AnyConnect VPN, you can skip past other VPN options and move to the [next section](#).

Shrew Soft VPN

An IPsec VPN allows you to securely obtain remote resources by establishing an encrypted tunnel across the Internet. The RV34X series routers work as IPsec VPN servers and support the Shrew Soft VPN Client. This section will show you how to configure your router and the Shrew Soft Client to secure a connection to a VPN.

Cisco does not support Shrew Soft. This example is provided for demonstration purposes only. If you have problems with Shrew Soft, please contact them for support.

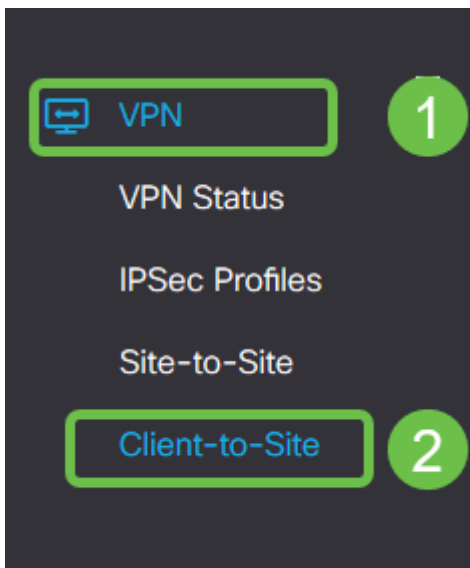
You can download the latest version of the Shrew Soft VPN client software here: <https://www.shrew.net/download/vpn>

Configure Shrew Soft on the RV345P Series Router

We will start by configuring the **Client-to-Site VPN** on the RV345P.

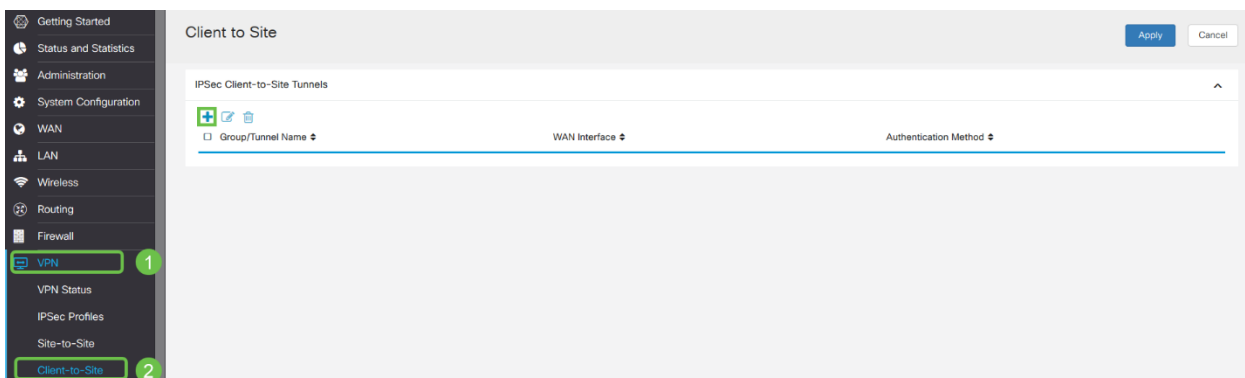
Step 1

Navigate to **VPN > Client-to-Site**.



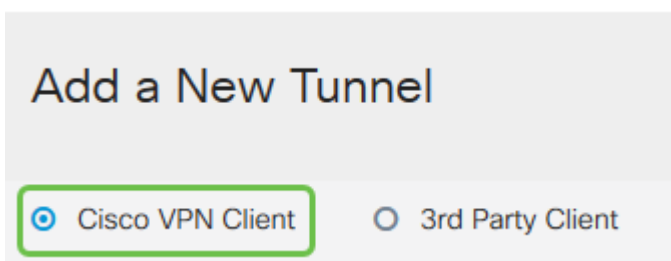
Step 2

Add a **Client-to-Site** VPN profile.



Step 3

Select the **Cisco VPN Client** option.



Step 4

Check the **Enable** box to make the VPN Client Profile active. We will also configure the *Group Name*, select the **WAN interface**, and enter a **Pre-shared Key**.

Please note the *Group Name* and *Pre-shared Key* as they will be used later when configuring the client.

Enable:

Group Name:

Interface:

IKE Authentication Method

Pre-shared Key:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Step 5

Leave the **User Group Table** blank for now. This is for the *User Group* on the router, but we have not configured it yet. Make sure the **Mode** is set to **Client**. Enter the **Pool Range for Client LAN**. We will use 172.16.10.1 through 172.16.10.10.

The Pool Range should use a unique subnet that isn't used elsewhere on the network.

User Group:

User Group Table

Group Name

Mode: Client NEM

Pool Range for Client LAN

Start IP:

End IP:

Step 6

Here is where we configure the **Mode Configuration** settings. Here are the settings we will use:

- **Primary DNS Server:** If you have an internal DNS Server or want to use an external DNS Server, you can enter it here. Otherwise, the default is set to the RV345P LAN IP address. We will use the default in our example.
- **Split Tunnel:** Check to enable Split Tunneling. This is used to specify which traffic will go over the VPN tunnel. We will use Split Tunnel in our example.
- **Split Tunnel Table:** Enter the networks the VPN client should have access to over the VPN. This example uses the RV345P LAN network.

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Default Domain:

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Split Tunnel:

Split Tunnel Table

+ [edit] [delete]

IP Address [dropdown] Netmask [dropdown]

| | | |
|-------------------------------------|--|--|
| <input checked="" type="checkbox"/> | <input type="text" value="192.168.1.0"/> | <input type="text" value="255.255.255.0"/> |
|-------------------------------------|--|--|

Step 7

After clicking **Save**, we can see the Profile in the **IPsec Client-to-Site Groups** list.

Client to Site

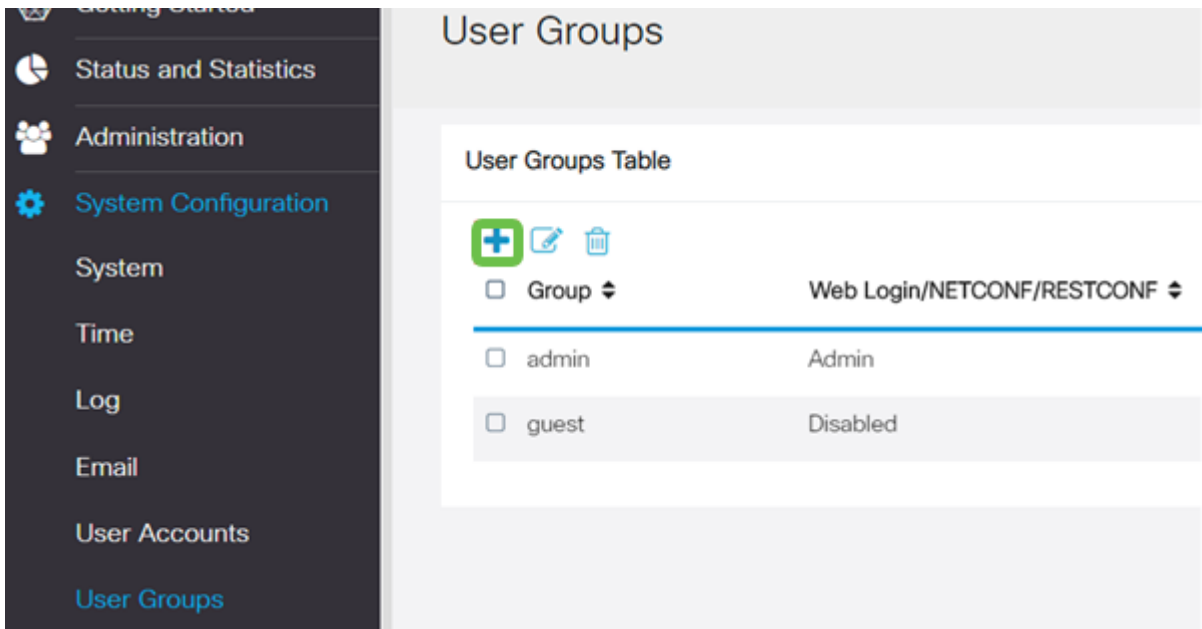
IPSec Client-to-Site Tunnels

+ [edit] [delete]

| <input type="checkbox"/> Group/Tunnel Name [dropdown] | WAN Interface [dropdown] | Authentication Method [dropdown] |
|---|--------------------------|----------------------------------|
| <input type="checkbox"/> Clients | WAN1 | Pre-shared Key |

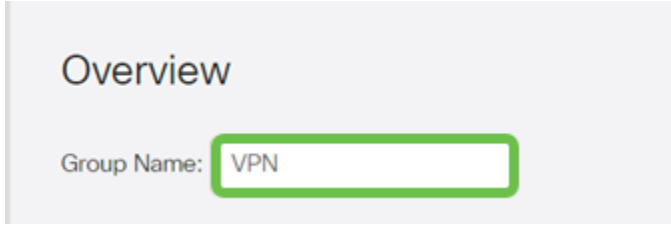
Step 8

Configure a **User Group** to use for Authenticating VPN client users. Under **System Configuration > User Groups**, click on the **plus icon** to add a User Group.



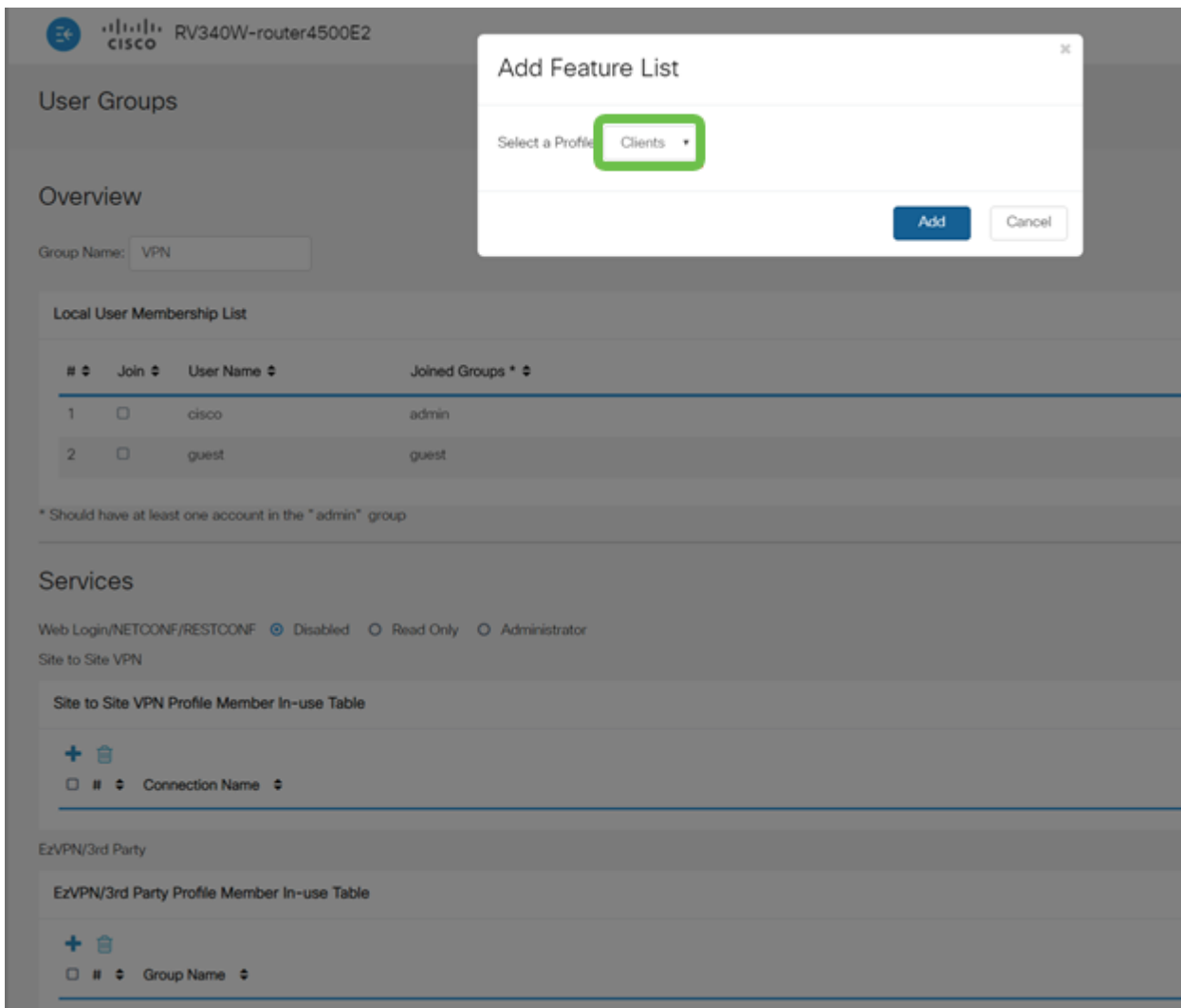
Step 9

Enter a **Group Name**.



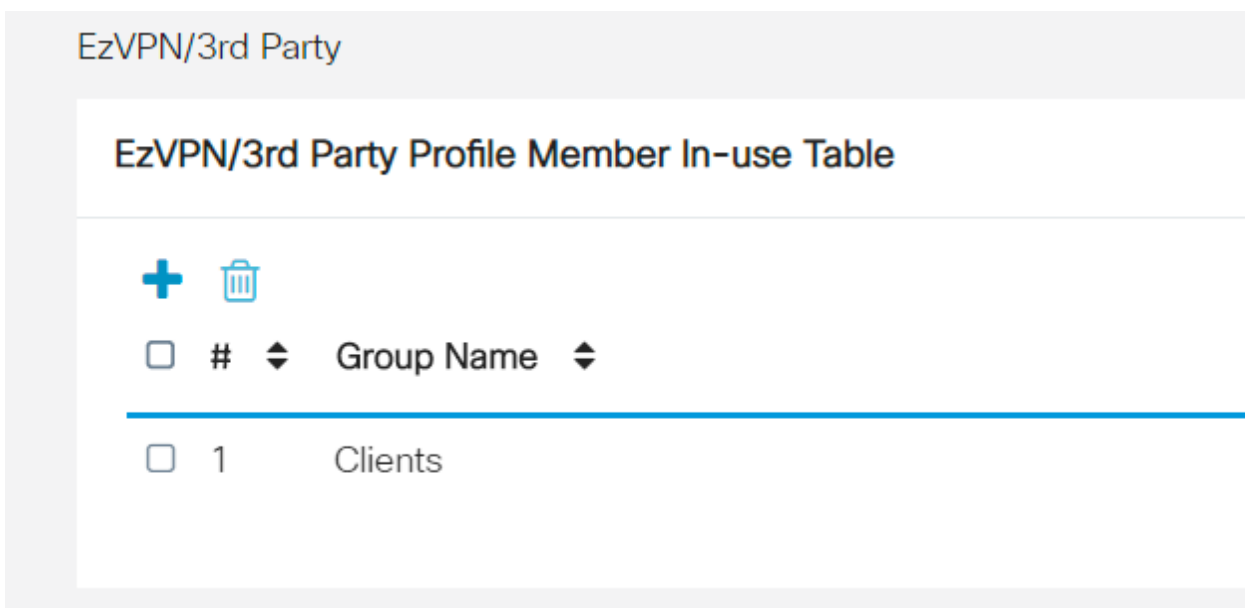
Step 10

Under **Services > EzVPN/3rd Party**, click **Add** to link this User Group to the **Client-to-Site** Profile that was configured earlier.



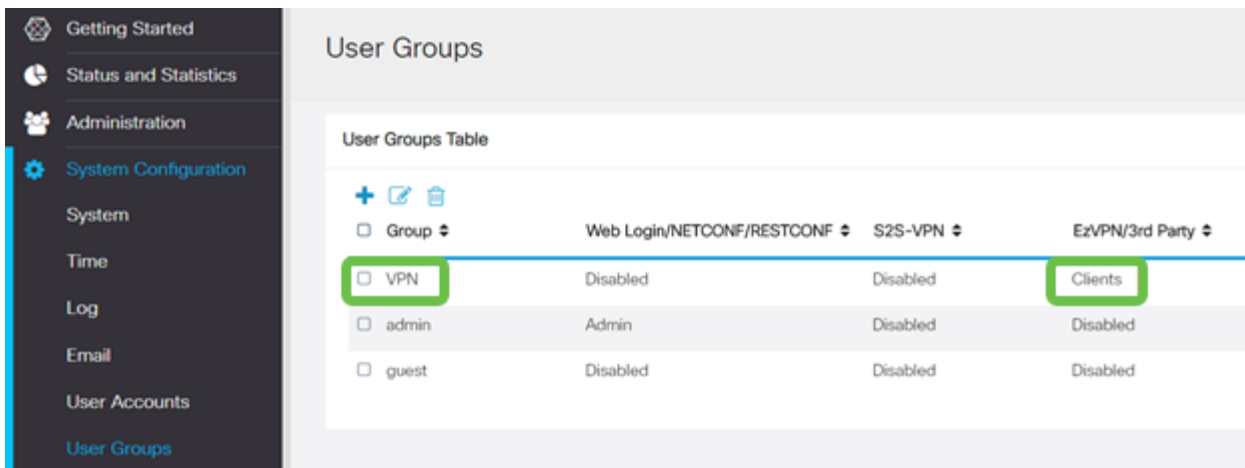
Step 11

You should now see the **Client-to-Site** Group Name in the list for **EzVPN/3rd Party**.



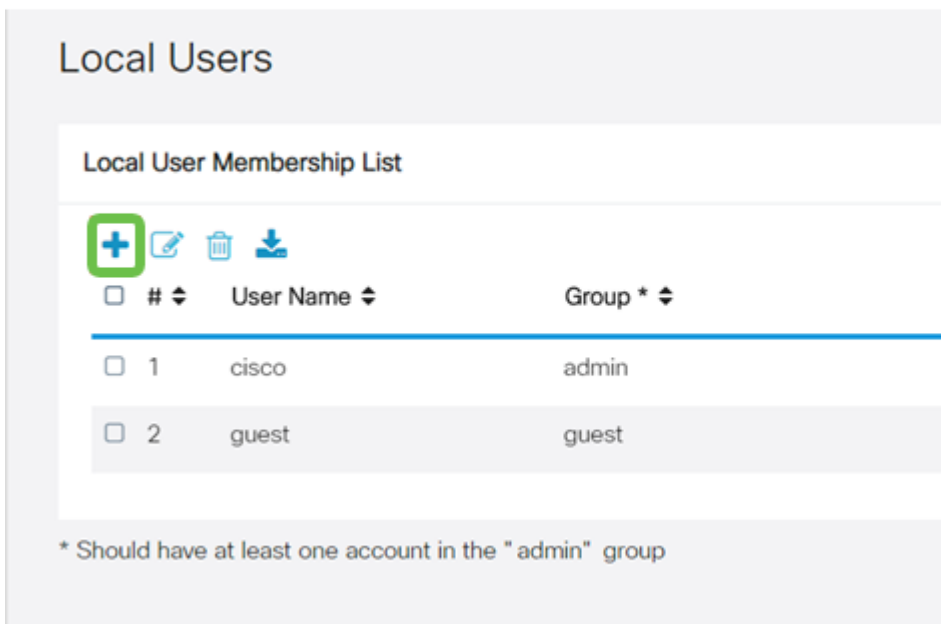
Step 12

After you **Apply** the User Group configuration, you will see it in the **User Groups** list and it will show the new User Group will be used with the Client-to-Site Profile you created earlier.



Step 13

Configure a new User in **System Configuration > User Accounts**. Click on the **plus icon** to create a new user.



Step 14

Enter the new **User Name** along with the **New Password**. Verify that the **Group** is set to the new **User Group** you just configured. Click **Apply** when finished.

User Accounts

Add User Account

| | | |
|----------------------|--|--------------------|
| User Name | <input type="text" value="vpnuser"/> | |
| New Password | <input type="password" value="....."/> | (Range: 0 - 127) |
| New Password Confirm | <input type="password" value="....."/> | |
| Group | <input type="text" value="VPN"/> | |

Step 15

The new **User** will show up in the list of **Local Users**.

Local Users

Local User Membership List



| <input type="checkbox"/> | # | User Name | Group * |
|--------------------------|---|-----------|---------|
|--------------------------|---|-----------|---------|

| | | | |
|--------------------------|---|-------|-------|
| <input type="checkbox"/> | 1 | cisco | admin |
|--------------------------|---|-------|-------|

| | | | |
|--------------------------|---|-------|-------|
| <input type="checkbox"/> | 2 | guest | guest |
|--------------------------|---|-------|-------|

| | | | |
|--------------------------|---|---------|-----|
| <input type="checkbox"/> | 3 | vpnuser | VPN |
|--------------------------|---|---------|-----|

* Should have at least one account in the "admin" group

This completes the configuration on the RV345P Series Router. Next, you will configure the Shrew Soft VPN client.

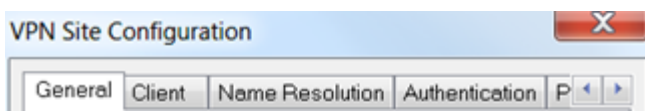
Configure the Shrew Soft VPN client

Perform the following steps.

Step 1

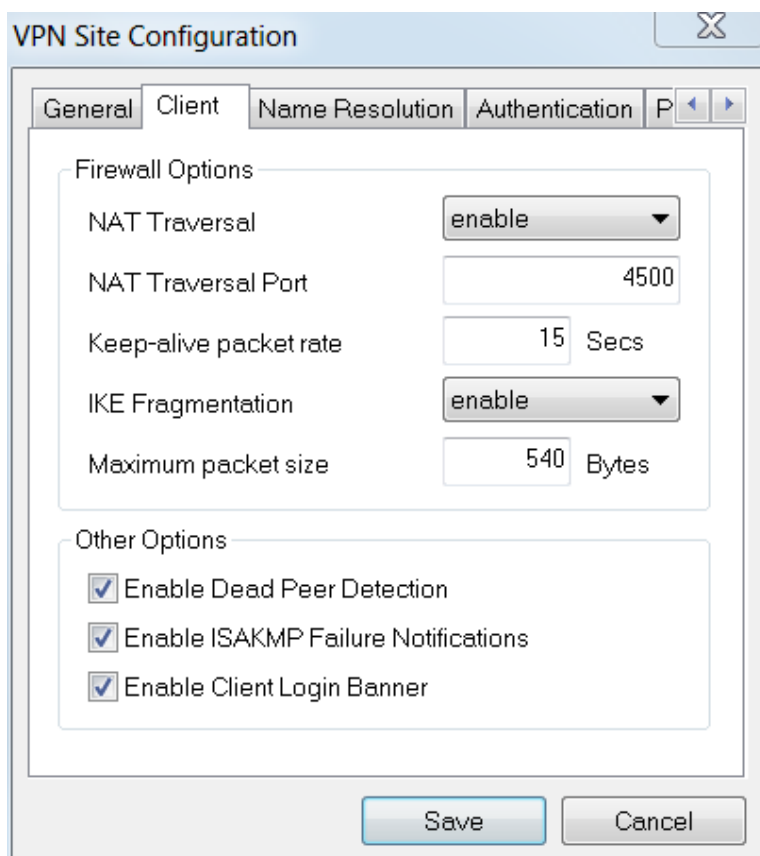
Open the Shrew Soft *VPN Access Manager* and click **Add** to add a Profile. In the *VPN Site Configuration* window that appears, configure the **General** tab:

- **Hostname or IP Address:** Use the WAN IP address (or hostname of the RV345P)
- **Auto Configuration:** Select **ike config pull**
- **Adapter Mode:** Select **Use a Virtual adapter and assigned address**



Step 2

Configure the **Client** tab. In this example, we kept the default settings.



The screenshot shows the 'VPN Site Configuration' dialog box with the 'Client' tab selected. The 'Firewall Options' section includes:

- NAT Traversal: enable
- NAT Traversal Port: 4500
- Keep-alive packet rate: 15 Secs
- IKE Fragmentation: enable
- Maximum packet size: 540 Bytes

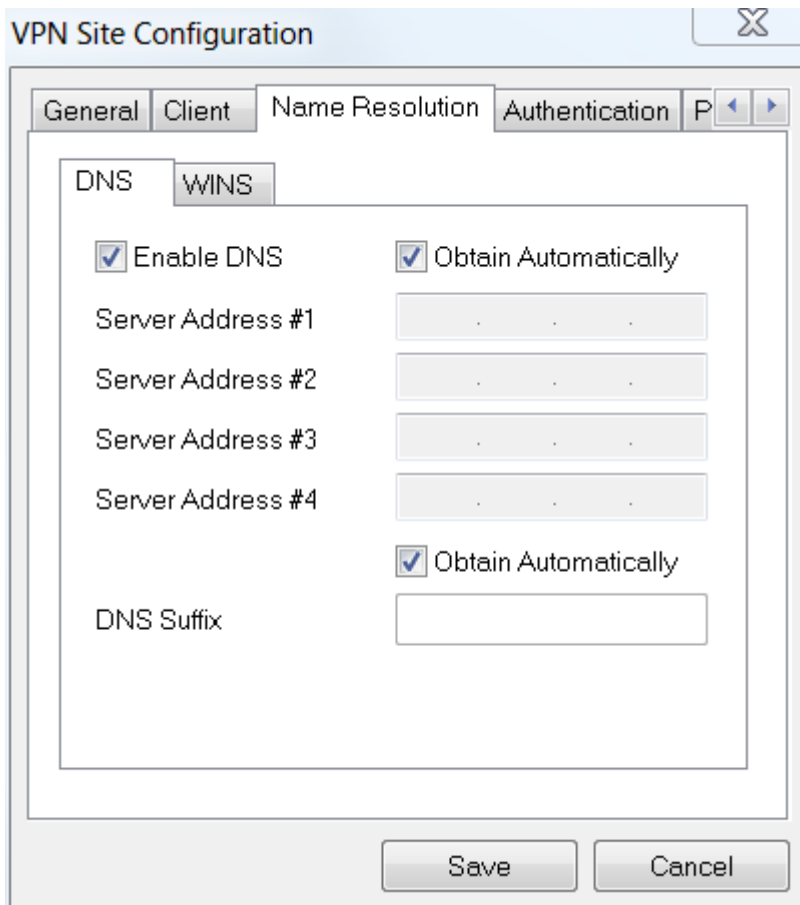
The 'Other Options' section includes three checked checkboxes:

- Enable Dead Peer Detection
- Enable ISAKMP Failure Notifications
- Enable Client Login Banner

Buttons for 'Save' and 'Cancel' are visible at the bottom.

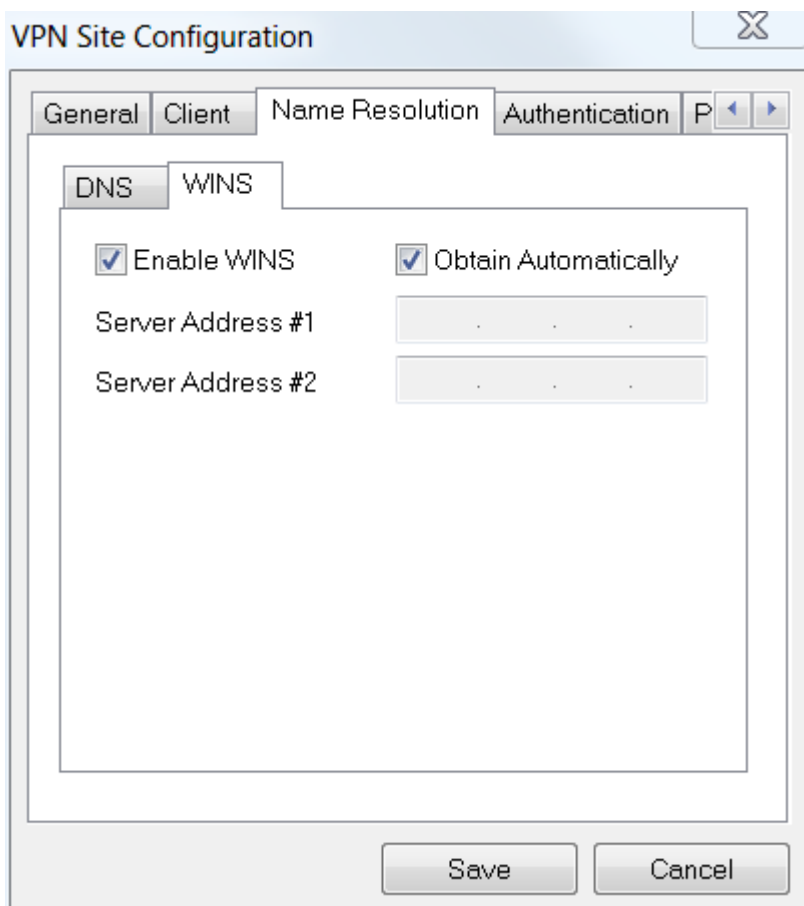
Step 3

Under **Name Resolution > DNS**, check the **Enable DNS** box and leave the **Obtain Automatically** boxes checked.



Step 4

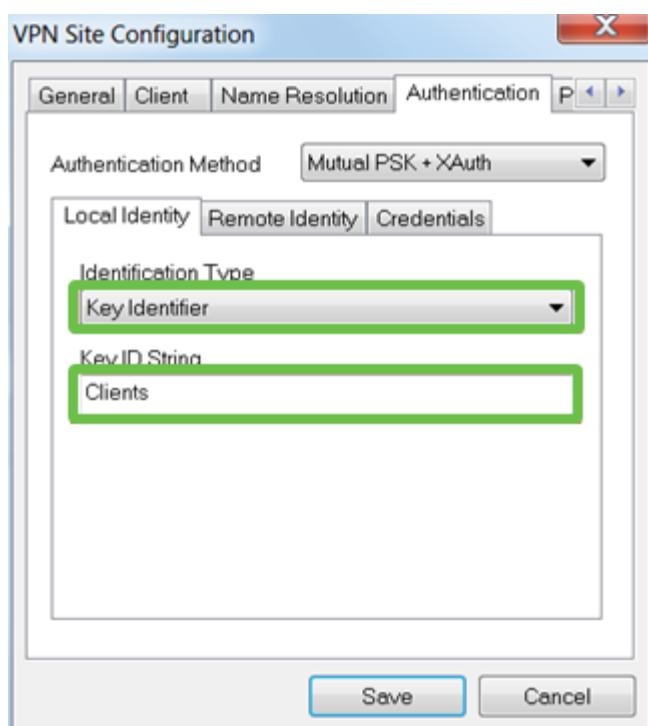
Under **Name Resolution** > **WINS** tab, check the **Enable WINS** box and leave the **Obtain Automatically** box checked.



Step 5

Click **Authentication > Local Identity**.

- **Identification Type:** Select **Key Identifier**
- **Key ID String:** Enter the **Group Name** that was configured on the RV345P

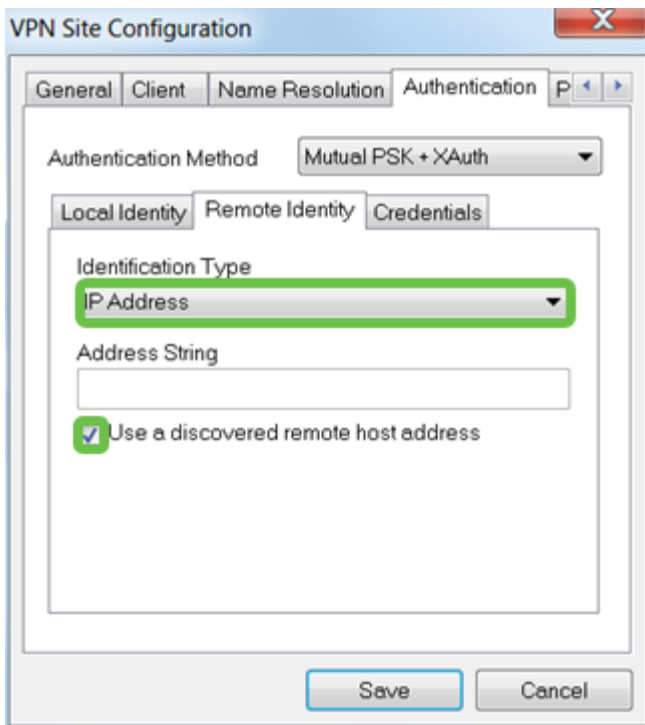


Step 6

Under **Authentication > Remote Identity**. In this example, we kept the default

settings.

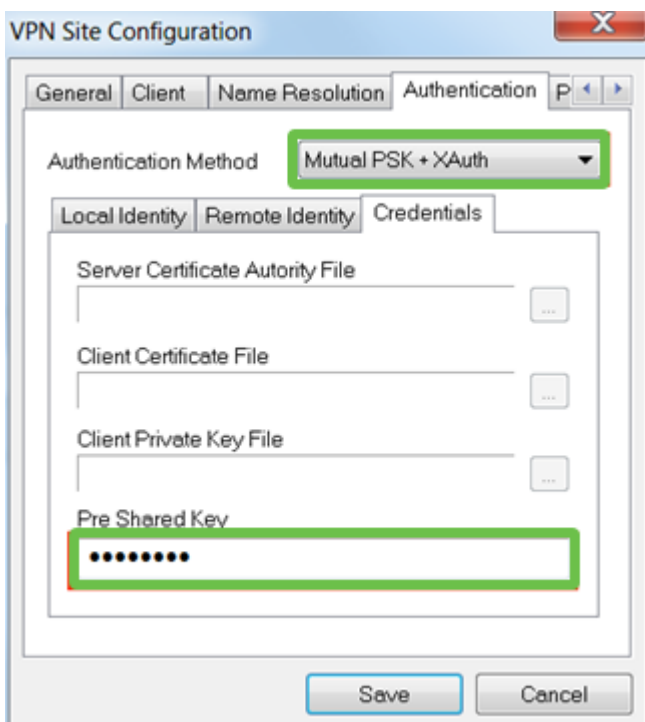
- **Identification Type:** IP Address
- **Address String:** <blank>
- **Use a discovered remote host address** box: Checked



Step 7

Under **Authentication > Credentials**, configure the following:

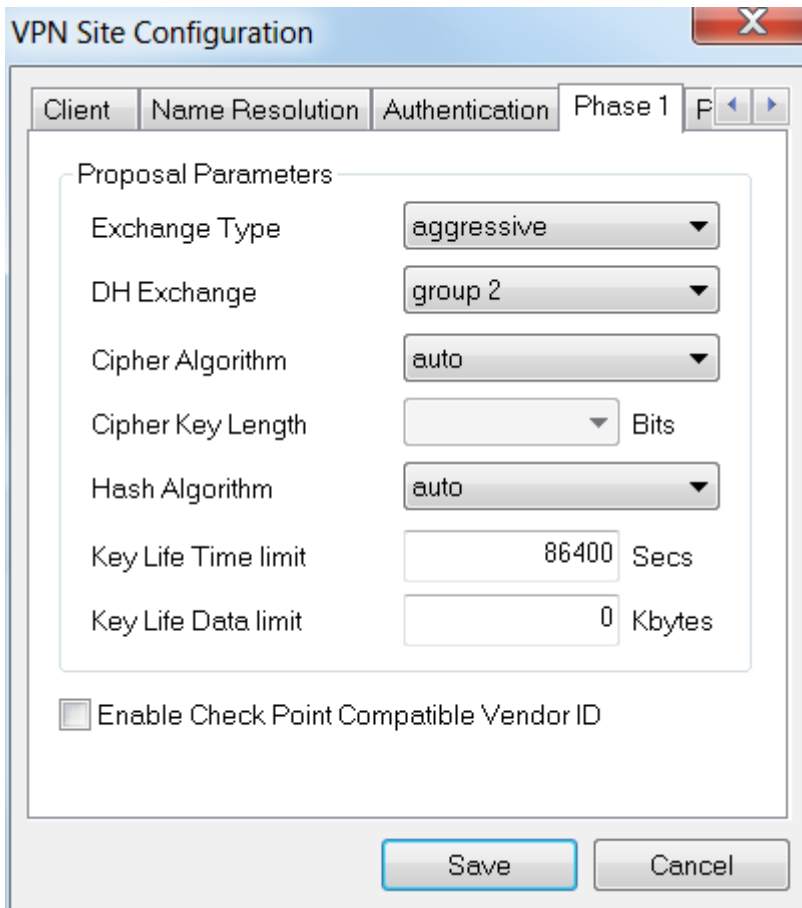
- **Authentication Method:** Select **Mutual PSK + XAuth**
- **Pre-Shared Key:** Enter the **Pre-shared Key** configured in the RV345P Client Profile



Step 8

For the **Phase 1** tab. In this example, the default settings were kept:

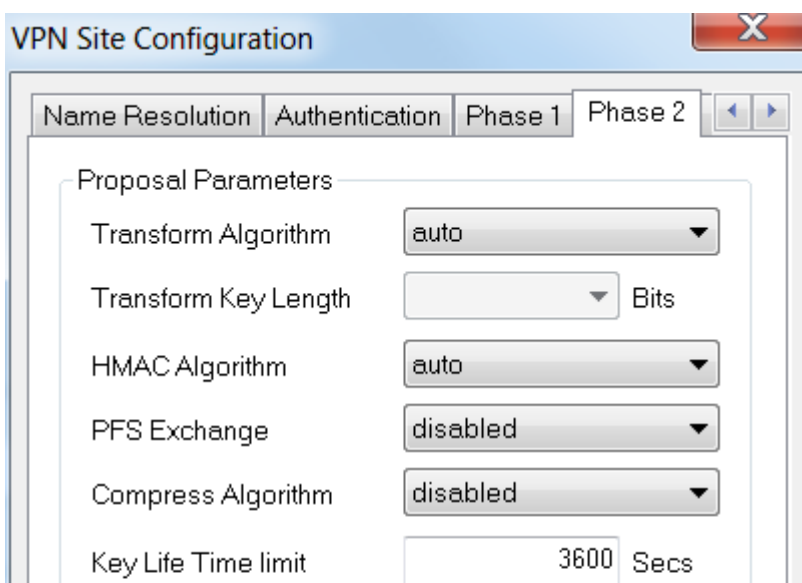
- **Exchange Type:** Aggressive
- **DH Exchange:** group 2
- **Cipher Algorithm:** Auto
- **Hash Algorithm:** Auto



Step 9

In this example, the defaults for the **Phase 2** tab were kept the same.

- **Transform Algorithm:** Auto
- **HMAC Algorithm:** Auto
- **PFS Exchange:** Disabled
- **Compress Algorithm:** Disabled

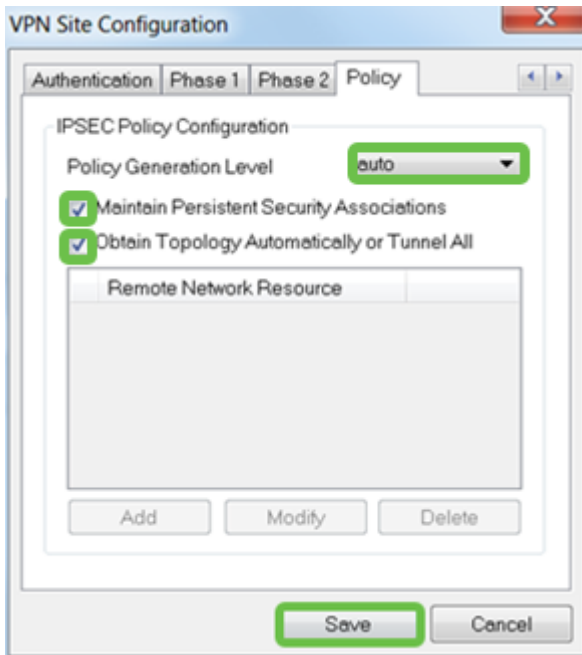


Step 10

For the **Policy** tab example, we used the following settings:

- **Policy Generation Level:** Auto
- **Maintain Persistent Security Associations:** Checked
- **Obtain Topology Automatically or Tunnel All:** Checked

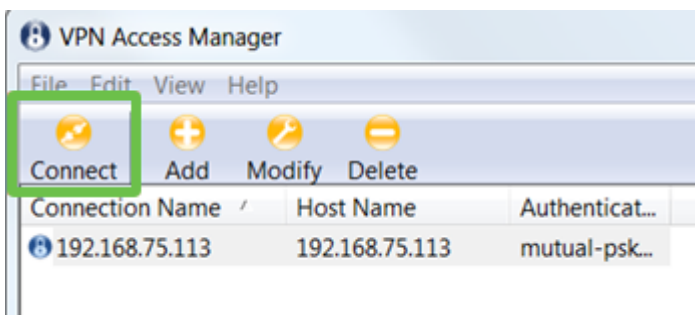
Since we configured **Split-Tunneling** on the RV345P, we don't need to configure it here.



When finished, click **Save**.

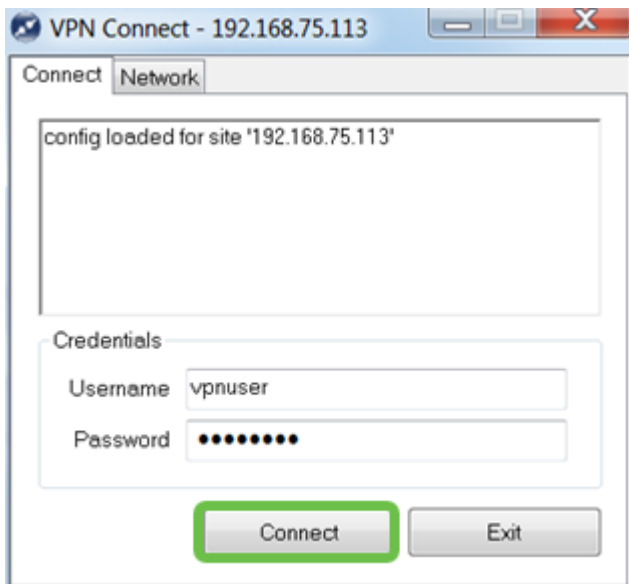
Step 11

You are now ready to test the connection. In *VPN Access Manager*, highlight the connection profile and click on the **Connect** button.



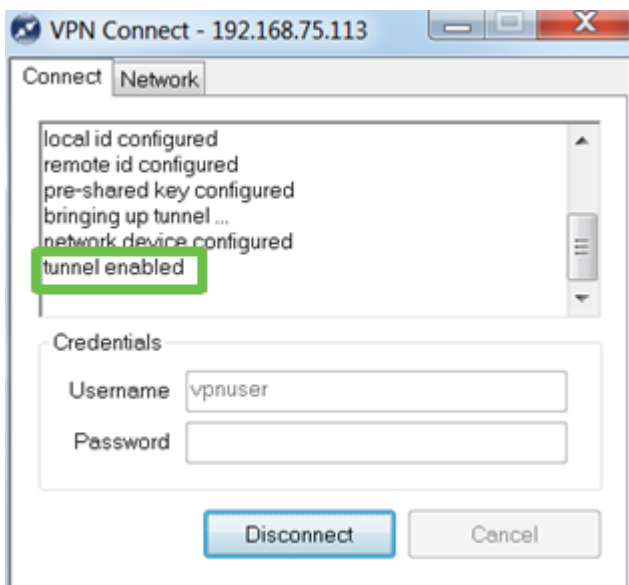
Step 12

In the **VPN Connect** window that comes up, enter the **Username** and **Password** using the credentials for the **User Account** you created on the RV345P (step 13 & 14). When finished, click **Connect**.



Step 13

Verify the tunnel is connected. You should see **tunnel enabled**.



Shrew Soft was used as an example in this configuration. Since Shrew Soft is not a Cisco product, please contact this third-party if you need technical assistance.

Other VPN Options

There are some other options for using a VPN. Click on the following links for more information:

- [Use TheGreenBow VPN Client to Connect with RV34x Series Router](#)
- [Configure a Teleworker VPN Client on the RV34x Series Router](#)
- [Configure a Point-to-Point Tunneling Protocol \(PPTP\) Server on the Rv34x Series Router](#)
- [Configure an Internet Protocol Security \(IPsec\) Profile on an RV34x Series Router](#)
- [Configure L2TP WAN Settings on the RV34x Router](#)
- [Configuring Site-to-Site VPN on the RV34x](#)

Supplemental Configurations on the RV345P Router

Configure VLANs (Optional)

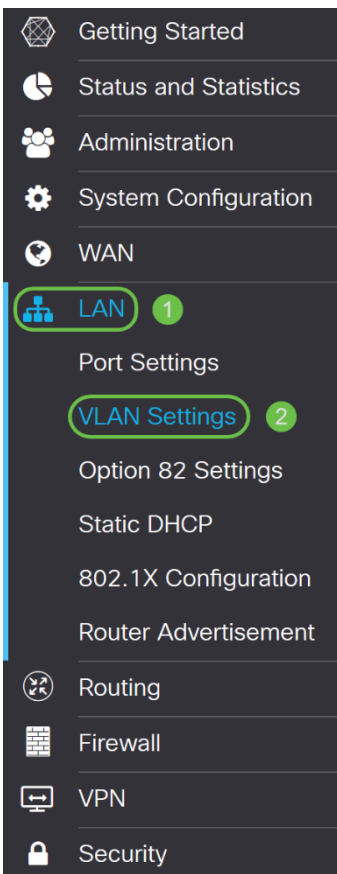
A Virtual Local Area Network (VLAN) allows you to logically segment a Local Area Network (LAN) into different broadcast domains. In scenarios where sensitive data may be broadcast on a network, VLANs can be created to enhance security by designating a broadcast to a specific VLAN. VLANs can also be used to enhance performance by reducing the need to send broadcasts and multicasts to unnecessary destinations. You can create a VLAN, but this has no effect until the VLAN is attached to at least one port, either manually or dynamically. Ports must always belong to one or more VLANs.

You may want to refer to [VLAN Best Practices and Security Tips](#) for additional guidance.

If you do not want to create VLANs, you can skip to the [next section](#).

Step 1

Navigate to **LAN > VLAN Settings**.



Step 2

Click the **add icon** to create a new VLAN.

VLAN Table



Step 3

Enter the *VLAN ID* that you want to create and a *Name* for it. The *VLAN ID* range is from 1-4093.

VLAN Table



| <input type="checkbox"/> | VLAN ID ↕ | Name | Inter-VLAN Routing | Device Management | IPv4 Address/Mask |
|-------------------------------------|-----------|---------|-------------------------------------|---------------------------------------|--|
| <input type="checkbox"/> | 1 | VLAN1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> ⓘ | 192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149 |
| <input checked="" type="checkbox"/> | 200 | VLAN200 | <input type="checkbox"/> | <input type="checkbox"/> ⓘ | IPv4 Address: <input type="text" value="192.168.2.1"/> / <input type="text" value="24"/> Subnet Mask: <input type="text" value="255.255.255.0"/> DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server <input type="radio"/> Relay |

Step 4

Uncheck the *Enabled* box for both *Inter-VLAN Routing* and *Device Management* if desired. Inter-VLAN routing is used to route packets from one VLAN to another VLAN.

In general, this is not recommended for guest networks as you will want to isolate guest users it leaves VLANs less secure. There are times when it may be necessary for VLANs to route between each other. If this is the case, check out [Inter-VLAN Routing on an RV34x Router with Targeted ACL Restrictions](#) to configure specific traffic that you allow between VLANs.

Device Management is the software that allows you to use your browser to log into the Web UI of the RV345P, from the VLAN, and manage the RV345P. This should also be disabled on Guest networks.

In this example, we did not enable either the *Inter-VLAN Routing* or *Device Management* to keep the VLAN more secure.

VLAN Table



| <input type="checkbox"/> | VLAN ID ↕ | Name | Inter-VLAN Routing | Device Management | IPv4 Address/Mask |
|-------------------------------------|----------------------------------|---------|-------------------------------------|---------------------------------------|--|
| <input type="checkbox"/> | 1 | VLAN1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> ⓘ | 192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149 |
| <input checked="" type="checkbox"/> | <input type="text" value="200"/> | VLAN200 | <input type="checkbox"/> | <input type="checkbox"/> ⓘ | IPv4 Address: <input type="text" value="192.168.2.1"/> / <input type="text" value="24"/> Subnet Mask: <input type="text" value="255.255.255.0"/> DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server <input type="radio"/> Relay |

Step 5

The private IPv4 address will auto-populate in the *IP Address* field. You can adjust this if you choose. In this example, the subnet has 192.168.2.100-192.168.2.149 IP addresses available for DHCP. 192.168.2.1-192.168.2.99, and 192.168.2.150-192.168.2.254 are available for static IP addresses.

VLAN Table



| <input type="checkbox"/> | VLAN ID ↕ | Name | Inter-VLAN Routing | Device Management | IPv4 Address/Mask |
|-------------------------------------|----------------------------------|---------|-------------------------------------|---------------------------------------|--|
| <input type="checkbox"/> | 1 | VLAN1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> ⓘ | 192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149 |
| <input checked="" type="checkbox"/> | <input type="text" value="200"/> | VLAN200 | <input type="checkbox"/> | <input type="checkbox"/> ⓘ | IPv4 Address: <input type="text" value="192.168.2.1"/> / <input type="text" value="24"/> Subnet Mask: <input type="text" value="255.255.255.0"/> DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server <input type="radio"/> Relay |

Step 6

The subnet mask under *Subnet Mask* will auto-populate. If you make changes, this will automatically adjust the field.

For this demonstration, we will be leaving the *Subnet Mask* as **255.255.255.0** or **/24**.

VLAN Table



| <input type="checkbox"/> | VLAN ID ↕ | Name | Inter-VLAN Routing | Device Management | IPv4 Address/Mask |
|-------------------------------------|----------------------------------|---------|-------------------------------------|-------------------------------------|---|
| <input type="checkbox"/> | 1 | VLAN1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149 |
| <input checked="" type="checkbox"/> | <input type="text" value="200"/> | VLAN200 | <input type="checkbox"/> | <input type="checkbox"/> | IPv4 Address: <input type="text" value="192.168.2.1"/> / <input type="text" value="24"/> <input type="text" value="255.255.255.0"/> DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server <input type="radio"/> Relay |

Step 7

Select a *Dynamic Host Configuration Protocol (DHCP) Type*. The following options are:

Disabled – Disables the DHCP IPv4 server on VLAN. This is recommended in a test environment. In this scenario, all IP addresses would need to be manually configured and all communication would be internal.

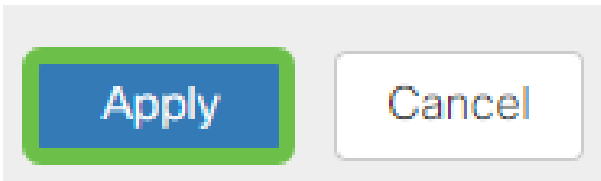
Server - This is the most often used option.

- Lease Time – Enter a time value of 5 to 43,200 minutes. The default is 1440 minutes (equal to 24 hours).
- Range Start and Range End – Enter the range start and end of IP addresses that can be assigned dynamically.
- DNS Server – Select to use the DNS server as a proxy, or from ISP from the drop-down list.
- WINS Server – Enter the WINS server name.
- DHCP Options:
 - Option 66 – Enter the IP address of the TFTP server.
 - Option 150 – Enter the IP address of a list of TFTP servers.
 - Option 67 – Enter the configuration filename.
- Relay – Enter the remote DHCP server IPv4 address to configure the DHCP relay agent. This is a more advanced configuration.

| | | | | | |
|-------------------------------------|----------------------------------|---------|--------------------------|--------------------------|--|
| <input checked="" type="checkbox"/> | <input type="text" value="200"/> | VLAN200 | <input type="checkbox"/> | <input type="checkbox"/> | IPv4 Address: <input type="text" value="192.168.2.1"/> / <input type="text" value="24"/> |
| | | | | | Subnet Mask: <input type="text" value="255.255.255.0"/> |
| | | | | | DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay |
| | | | | | Lease Time: <input type="text" value="1440"/> min. |
| | | | | | Range Start: <input type="text" value="192.168.2.100"/> |
| | | | | | Range End: <input type="text" value="192.168.2.149"/> |

Step 8

Click **Apply** to create the new VLAN.



Assign VLANs to Ports (Optional)

16 VLANs can be configured on the RV345P, with one VLAN for the Wide Area Network (WAN). VLANs that are not on a port should be *Excluded*. This keeps the traffic on that port exclusively for the VLAN/VLANs the user specifically assigned. It is considered a best practice.

Ports can be set to be an Access Port or a Trunk Port:

- Access Port - Assigned one VLAN. Untagged frames are passed.
- Trunk Port - Can carry more than one VLAN. 802.1q trunking allows for a native VLAN to be Untagged. VLANs that you don't want on the trunk should be Excluded.

One VLAN assigned its own port:

- Considered an Access port.
- The VLAN that is assigned to this port should be labeled Untagged.
- All other VLANs should be labeled Excluded for that port.

Two or more VLANs that share one port:

- Considered a Trunk Port.
- One of the VLANs can be labeled Untagged.
- The rest of the VLANs that are part of the Trunk Port should be labeled Tagged.
- The VLANs that are not part of the Trunk Port should be labeled Excluded for that port.

In this example, there are no trunks.

Step 1

Select the *VLAN IDs* to edit.

In this example, we have selected *VLAN 1* and *VLAN 200*.

Assign VLANs to ports

| VLAN ID | LAN1 | LAN2 |
|---------|----------|----------|
| 1 | Untagged | Excluded |
| 200 | Excluded | Untagged |

Step 2

Click **Edit** to assign a VLAN to a LAN port and specify each setting as *Tagged*, *Untagged*, or *Excluded*.

In this example, on LAN1 we assigned VLAN 1 as **Untagged** and VLAN 200 as **Excluded**. For LAN2 we assigned VLAN 1 as **Excluded** and VLAN 200 as **Untagged**.

Assign VLANs to ports

| VLAN ID | LAN1 | LAN2 |
|---------|----------|----------|
| 1 | Untagged | Excluded |
| 200 | Excluded | Untagged |

Step 3

Click **Apply** to save the configuration.



You should now have successfully created a new VLAN and configured VLANs to ports on the RV345P. Repeat the process to create the other VLANs. For example, VLAN300 would be created for Marketing with a subnet of 192.168.3.x and VLAN400 would be created for Accounting with a subnet of 192.168.4.x.

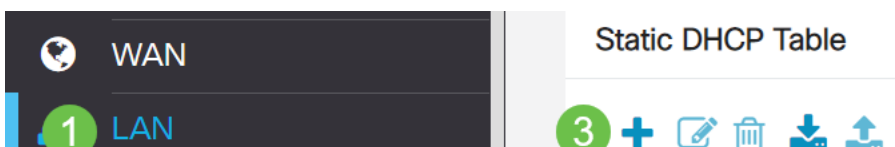
Add a Static IP (Optional)

If you would like a certain device to be reachable to other VLANs, you can give that device a static local IP address and create an access rule to make it accessible. This only works if Inter-VLAN routing is enabled. There are other situations where a static IP may be useful. For more information on setting static IP addresses, check out [Best Practices for Setting Static IP Addresses on Cisco Business Hardware](#).

If you don't need to add a static IP address, you can move to the [next section](#) of this article.

Step 1

Navigate to **LAN > Static DHCP**. Click on the **plus icon**.



Step 2

Add the **Static DHCP** information for the device. In this example, the device is a printer.

| Name | MAC address | Static IPv4 Address | Enabled |
|---------|-------------------|---------------------|---------|
| Printer | 00:11:22:33:44:55 | 192.168.2.10 | Enabled |

Managing Certificates (Optional)

A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows relying parties to depend upon signatures or assertions made by the private key that corresponds to the public key that is certified. A router can generate a self-signed certificate, a certificate created by a network administrator. It can also send out requests to Certificate Authorities (CA) to apply for a digital identity certificate. It is important to have legitimate certificates from third party applications.

A Certificate Authority (CA) is used for authentication. Certificates can be purchased from any number of third-party sites. It is an official way to prove that your site is secure. Essentially, the CA is a trusted source that verifies that you are a legitimate business and can be trusted. Depending on your needs, a certificate at a minimal cost. You get checked out by the CA, and once they verify your information, they will issue the certificate to you. This certificate can be downloaded as a file on your computer. You can then go into your router (or VPN server) and upload it there.

Generate CSR/Certificate

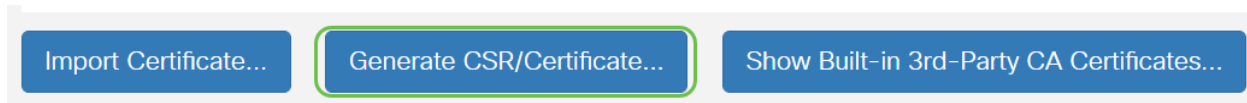
Step 1

Log in to the web-based utility of the router and choose **Administration > Certificate**.

- Getting Started
- Status and Statistics
- Administration** 1
- File Management
- Reboot

Step 2

Click **Generate CSR/Certificate**. You will be brought to the Generate CSR/Certificate page.



Step 3

Fill in the boxes with the following:

- Choose the appropriate certificate type
 - Self-Signing Certificate — This is a Secure Socket Layer (SSL) certificate which is signed by its own creator. This certificate is less trusted, as it cannot be cancelled if the private key is compromised somehow by an attacker.
 - Certified Signing Request — This is a Public Key Infrastructure (PKI) which is sent to the certificate authority to apply for a digital identity certificate. It is more secure than self-signed as the private key is kept secret.
- Enter a name for your certificate in the Certificate Name field to identify the request. This field cannot be blank nor contain spaces and special characters.
- (Optional) Under the Subject Alternative Name area, click a radio button. The options are:
 - IP Address — Enter an Internet Protocol (IP) address
 - FQDN — Enter a Fully Qualified Domain Name (FQDN)
 - Email — Enter an email address
- In the Subject Alternative Name field, enter the FQDN.
- Choose a country name in which your organization is legally registered from the Country Name drop-down list.
- Enter a name or abbreviation of the state, province, region, or territory where your organization is located in the State or Province Name(ST) field.
- Enter a name of the locality or city in which your organization is registered or located in the Locality Name field.
- Enter a name under which your business is legally registered. If you are enrolling as a small business or sole proprietor, enter the name of the certificate requester in the Organization Name field. Special characters cannot be used.
- Enter a name in the Organization Unit Name field to differentiate between divisions within an organization.
- Enter a name in the Common Name field. This name must be the fully-qualified domain name of the website for which you use the certificate for.
- Enter the Email Address of person who wants to generate the certificate.
- From the Key Encryption Length drop-down list, choose a key length. The options are 512, 1024, and 2048. The greater the key length, the more secure the certificate.
- In the Valid Duration field, enter the number of days the certificate will be valid. The default is 360.
- Click **Generate**.



Certificate

2

Generate

Cancel

Generate CSR/Certificate

Type: Self-Signing Certificate

Certificate Name: TestCACertificate

Subject Alternative Name: spprtfrms

IP Address FQDN Email

Country Name(C): US - United States

State or Province Name(ST): Wisconsin

Locality Name(L): Oconomowoc

Organization Name(O): Cisco

Organization Unit(OU): Cisco Business

Common Name(CN): cisco.com

Email Address(E): @cisco.com

Key Encryption Length: 2048

Valid Duration: 360 days (Range: 1-10950, Default: 360)

1

The generated certificate should now appear in the Certificate Table.

Certificate Table



| <input type="checkbox"/> Index | Certificate | Used By | Type | Signed By | Duration | Details | Action |
|--------------------------------|---------------|------------|-----------|---------------|---|---------|--------|
| <input type="checkbox"/> 1 | Default | WebServ... | Local ... | Self Signed | From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT | | |
| <input type="checkbox"/> 2 | TestCACert... | - | CA C... | Self Signed | From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT | | |
| <input type="checkbox"/> 3 | Router | - | Local ... | CiscoTest-... | From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT | | |
| <input type="checkbox"/> 4 | TestCACert... | - | Local ... | Self Signed | From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT | | |

Import Certificate...

Generate CSR/Certificate...

Show Built-in 3rd-Party CA Certificates...

Select as Primary Certificate...

You should now have successfully created a certificate on the RV345P router.

Export a Certificate

Step 1

In the Certificate Table, check the checkbox of the certificate you want to export and click the **export icon**.

Certificate Table ^

Index ⌵ Certificate ⌵ Used By ⌵ Type ⌵ Signed By ⌵ Duration ⌵ Details Action

| | | | | | | | | |
|-------------------------------------|---|---------------|------------|-----------|---------------|---|--|--|
| <input type="checkbox"/> | 1 | Default | WebServ... | Local ... | Self Signed | From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT | | |
| <input type="checkbox"/> | 2 | TestCACert... | - | CA C... | Self Signed | From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT | | |
| <input type="checkbox"/> | 3 | Router | - | Local ... | CiscoTest-... | From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT | | |
| <input checked="" type="checkbox"/> | 4 | TestCACert... | - | Local ... | Self Signed | From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT | | |

1 2

Step 2

- Click a format to export the certificate. The options are:
 - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 is an exported certificate that comes in a .p12 extension. A password will be required in order to encrypt the file to protect it as it is exported, imported, and deleted.
 - PEM — Privacy Enhanced Mail (PEM) is often used for web servers for their ability to be easily translated into readable data by using a simple text editor such as notepad.
- If you chose PEM, just click **Export**.
- Enter a password to secure the file to be exported in the Enter Password field.
- Re-enter the password in the Confirm Password field.
- In the Select Destination area, PC has been chosen and is the only option currently available.
- Click **Export**.

Export Certificate x

1 Export as PKCS#12 format

Enter Password

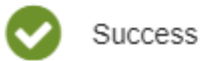
Confirm Password

Export as PEM format

Step 3

A message indicating the success of the download will appear below the Download button. A file will begin to download in your browser. Click **Ok**.

Information



Success



You should now have successfully exported a certificate on the RV345P Series Router.

Import a Certificate

Step 1

Click on **Import Certificate...**

A screenshot of a web interface showing a table of certificates. The table has columns for Index, Certificate, Used By, Type, Signed By, Duration, Details, and Action. Below the table are several buttons: "Import Certificate..." (highlighted with a green box), "Generate CSR/Certificate...", "Show Built-in 3rd-Party CA Certificates...", and "Select as Primary Certificate...".

| Index | Certificate | Used By | Type | Signed By | Duration | Details | Action |
|-------|---------------|------------|-----------|---------------|---|---------|--------|
| 1 | Default | WebServ... | Local ... | Self Signed | From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT | | |
| 2 | TestCACert... | - | CA C... | Self Signed | From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT | | |
| 3 | Router | - | Local ... | CiscoTest-... | From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT | | |
| 4 | TestCACert... | - | Local ... | Self Signed | From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT | | |

Step 2

- Choose the type of certificate to import from the drop-down list. The options are:
 - Local Certificate — A certificate generated on the router.
 - CA Certificate — A certificate that is certified by a trusted third-party authority that has confirmed that the information contained in the certificate is accurate.
 - PKCS #12 Encoded file — Public Key Cryptography Standards (PKCS) #12 is a format of storing a server certificate.
- Enter a name for the certificate in the Certificate Name field.

- If PKCS #12 was chosen, enter a password for the file in the Import Password field. Otherwise, skip to Step 3.
- Click a source to import the certificate. The options are:
 - Import from PC
 - Import from USB
- If the router does not detect a USB drive, the Import from USB option will be grayed out.
- If you chose Import From USB and your USB is not being recognized by the router, click Refresh.
- Click on the Choose File button and choose the appropriate file.
- Click **Upload**.

Certificate

3
Upload
Cancel

Import Certificate

Type: PKCS#12 encoded file v

Certificate Name: cisco 1

Import Password:

Upload certificate file

Import From PC

2 Browse... TestCACertificate

Import From USB ↻

Once successful, you will automatically be taken to the main Certificate page. The Certificate Table will populate with the recently imported certificate.

Certificate Table

🗑️

| Index | Certificate | Used By | Type | Signed By | Duration | Details | Action |
|-------|---------------|------------|-----------|---------------|---|--|---|
| 1 | Default | WebServ... | Local ... | Self Signed | From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT | 📄 | ⬆️ |
| 2 | TestCACert... | - | CA C... | Self Signed | From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT | 📄 | ⬆️ |
| 3 | Router | - | Local ... | CiscoTest-... | From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT | 📄 | ⬆️ |
| 4 | TestCACert... | - | Local ... | Self Signed | From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT | 📄 | ⬆️ |

Import Certificate...
Generate CSR/Certificate...
Show Built-in 3rd-Party CA Certificates...

Select as Primary Certificate...

You should now have successfully imported a certificate on your RV345P router.

Configure a Mobile Network Using a Dongle and an RV345P Series Router (Optional)

Perhaps you want to configure a backup mobile network using a dongle and your RV345P router. If this is the case, you should read [Configure a Mobile Network Using a Dongle and an RV34x Series Router](#).

Congratulations, you have completed the configuration of your RV345P router! You will now configure your Cisco Business Wireless devices.

Configure the CBW140AC

CBW140AC Out of the Box

Start by plugging an Ethernet cable from the PoE port on your CBW140AC to a PoE port on the RV345P. The first 4 ports on the RV345P can supply PoE, so any of them can be used.

Check the status of the indicator lights. The access point will take about 10 minutes to boot. The LED will blink green in multiple patterns, alternating rapidly through green, red, and amber before turning green again. There may be small variations in the LED color intensity and hue from unit to unit. When the LED light is blinking green, proceed to the next step.

The PoE Ethernet uplink port on the Primary AP can ONLY be used to provide an uplink to the LAN, and NOT to connect to any other Primary capable or mesh extender devices.

If your access point isn't new, out of the box, make sure it is reset to factory default settings for the *CiscoBusiness-Setup* SSID to show up in your Wi-Fi options. For assistance with this, check out [How to Reboot and Reset to Factory Default Settings on RV345x Routers](#).

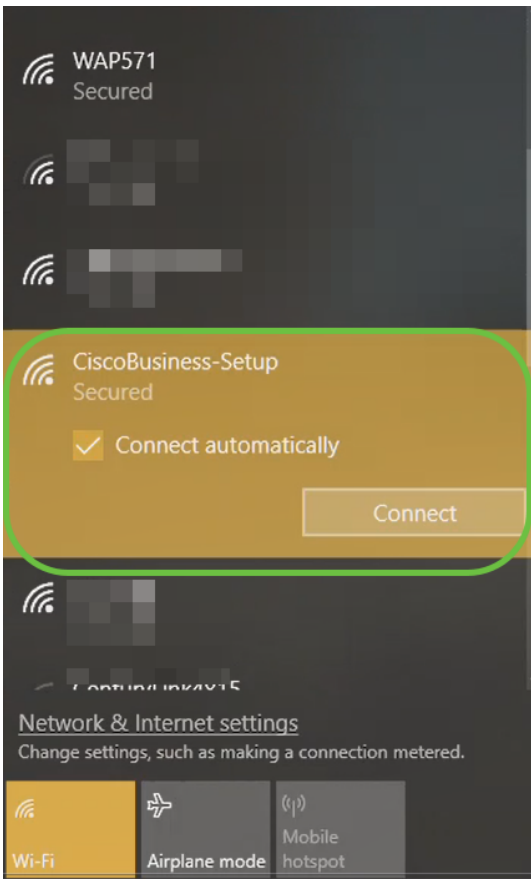
Set Up the 140AC Primary Wireless Access Point on the Web UI

You can set up the Access Point using the mobile application or the Web UI. This article uses the Web UI for setup, which gives more options for configuration but is a little more complicated. If you would like to use the mobile application for the next sections, click to access the [mobile application instructions](#).

If you have trouble connecting, refer to the [Wireless Troubleshooting Tips](#) section of this article.

Step 1

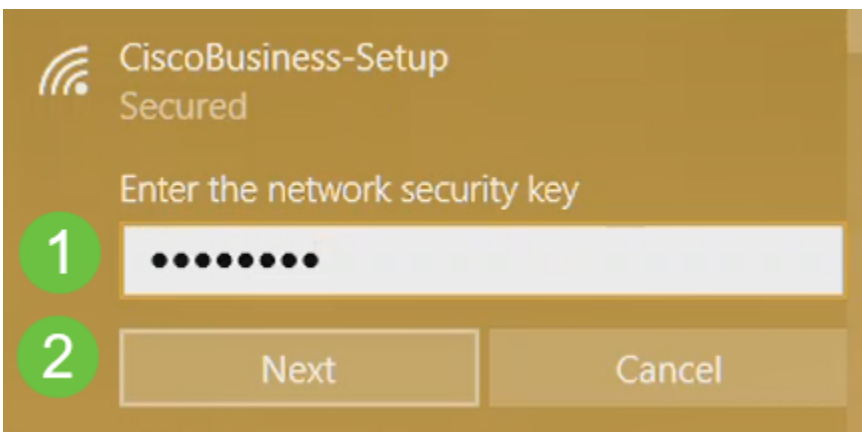
On your PC, click the **Wi-Fi icon** and choose *CiscoBusiness-Setup* wireless network. Click Connect.



If your access point isn't new, out of the box, make sure it is reset to factory default settings for the *CiscoBusiness-Setup* SSID to show up in your Wi-Fi options.

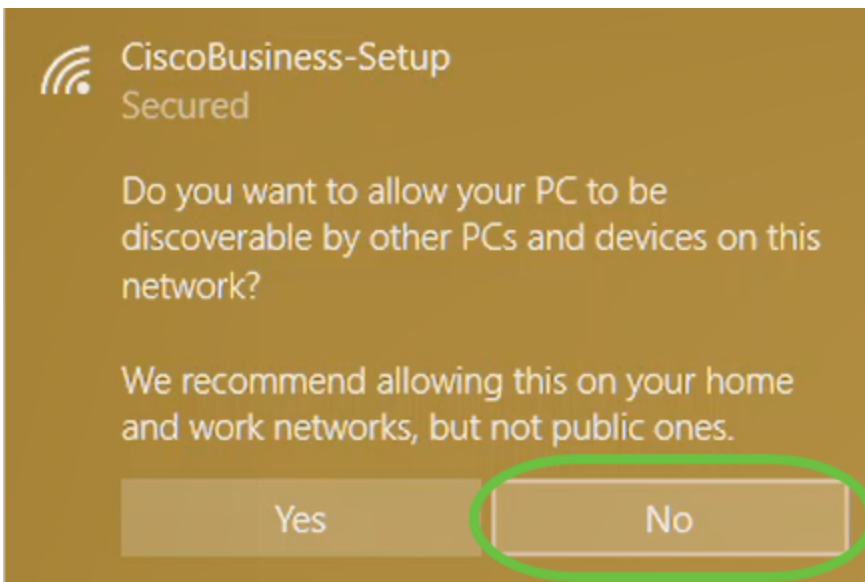
Step 2

Enter the passphrase **cisco123** and click **Next**.



Step 3

You will get the following screen. Since you can configure only one device at a time, click **No**.



Only one device can be connected to the *CiscoBusiness-Setup* SSID. If a second device attempts to connect, it will not be able to. If you are unable to connect to the SSID and have validated the password, some other device may have made the connection. Restart the AP and try again.

Step 4

Once connected, the web browser should auto-redirect to the CBW AP setup wizard. If not, open a web browser, such as Internet Explorer, Firefox, Chrome, or Safari. In the address bar, type **http://ciscobusiness.cisco** and press **Enter**. Click **Start** on the webpage.



If you do not see the webpage, wait for a few more minutes or reload the page. After this initial setup, you will use <https://ciscobusiness.cisco> to log in. If your web browser auto-populates with <http://>, you need to manually type in the <https://> to gain access.

Step 5

Create an *admin account* by entering the following:

- Admin username (Maximum of 24 characters)
- Admin password
- Confirm admin password

You can choose to show the password by checking the checkbox next to *Show Password*. Click **Start**.

Welcome! Please start by creating an admin account.

admin

password

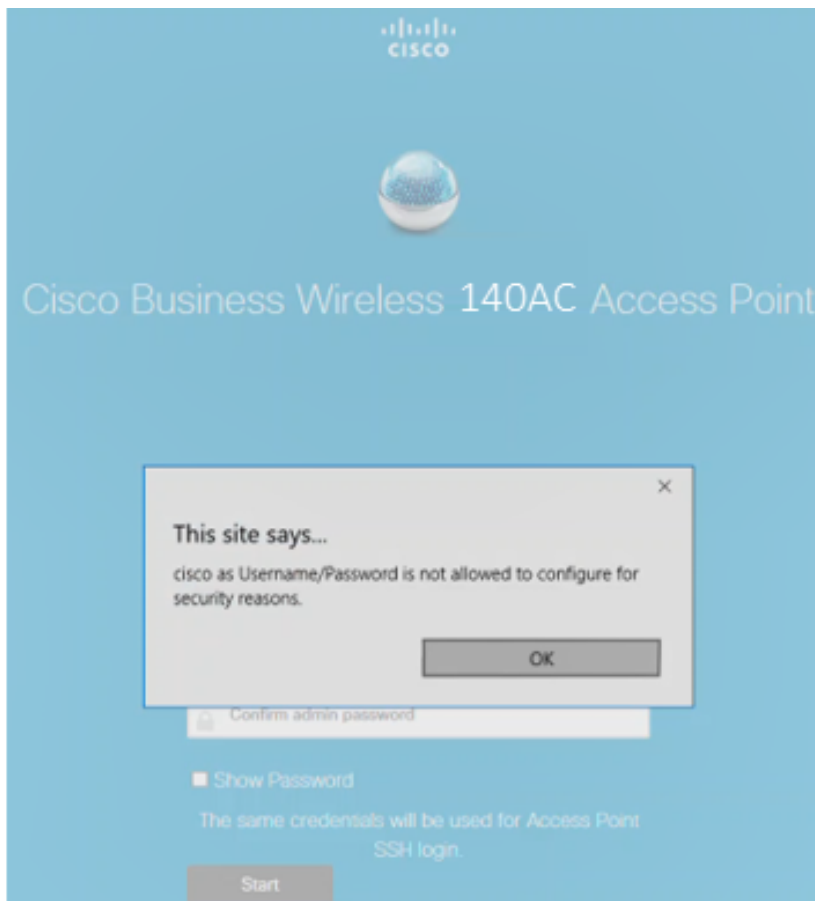
password

Show Password

Credentials will be used to manage the Access Point

Start

Do not use *cisco*, or variations of it in the username or password fields. If you do, you will get an error message as shown below.



Step 6

Set Up Your Primary AP by entering the following:

- Primary AP Name
- Country
- Date & Time
- Timezone
- Mesh

1 Set Up Your Primary AP

Primary AP Name



1

Country



2

Date & Time



3

Timezone



4

Mesh



5

Mesh should be enabled only if you plan to create a mesh network. By default, it is disabled.

Step 7

(Optional) You can enable *Static IP for your CBW140AC* for management purposes. If not, the interface gets an IP address from your DHCP server. To configure static IP, enter the following:

- Management IP Address
- Subnet Mask
- Default Gateway

Click **Next**.

By default, this option is disabled.

Step 8

Create Your Wireless Networks by entering the following:

- Network Name
- Choose Security
- Passphrase
- Confirm Passphrase
- (Optional) Check the checkbox to Show Passphrase.

Click **Next**.

2 Create Your Wireless Network

Network Name: CBWWlan

Security: WPA2

Passphrase:

Confirm Passphrase:

Show Passphrase

Back Next

Wi-Fi protected Access (WPA) version 2 (WPA2), is the current standard for Wi-Fi security.

Step 9

Confirm the settings and click **Apply**.

Please confirm the configurations and Apply

1 Primary AP Settings

Username **Admin**
 Primary AP Name **Test**
 Country **United States (US)**
 Date & Time **04/09/2021 9:14:16**
 Timezone **Central Time (US and Canada)**
 Mesh **No**
 Management IP Address **DHCP assigned IP Address**

2 Wireless Network Settings

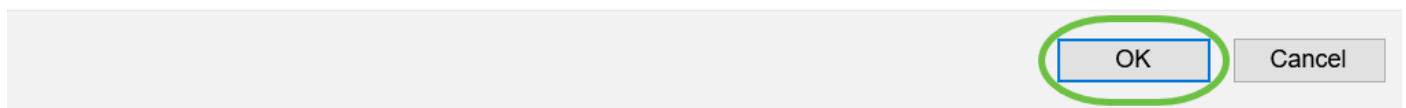
Network Name **Test123**
 Security **WPA2 Personal**
 Passphrase: *********



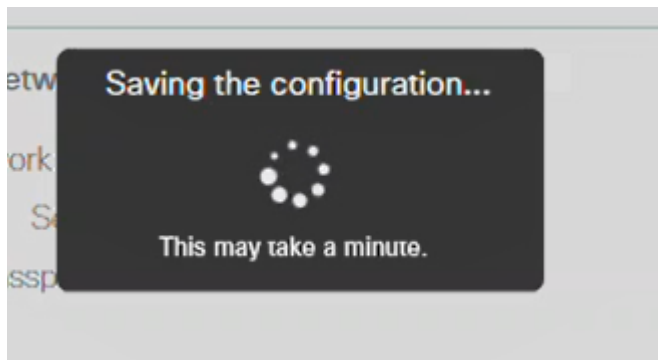
Step 10

Click **OK** to apply the settings.

Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set up wizard.



You will see the following screen while the configurations are being saved and the system reboots. This might take 10 minutes.

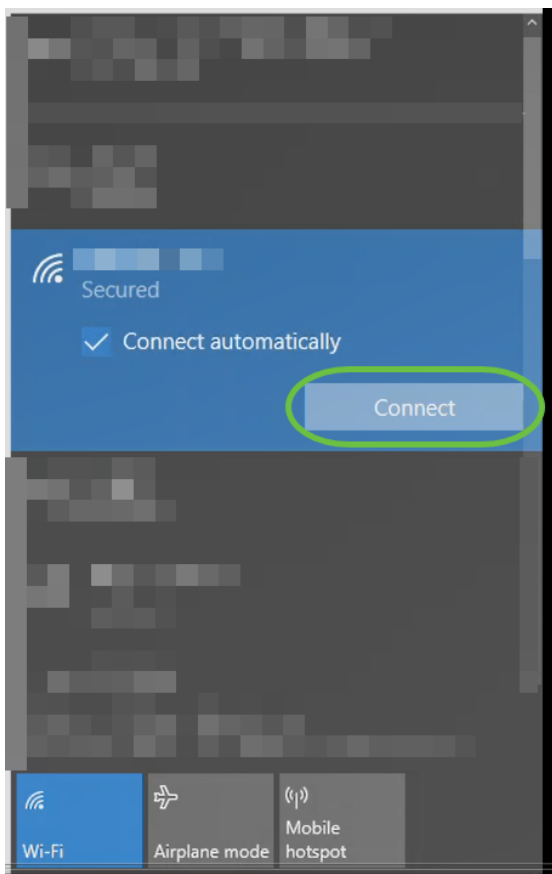


During the reboot, the LED in the access point will go through multiple color patterns. When the LED is blinking green, proceed to the next step. If the LED does not get past the red flashing pattern, it indicates that there is no DHCP server in your network. Ensure that the AP is connected to a switch or a router with a DHCP server.

Step 11

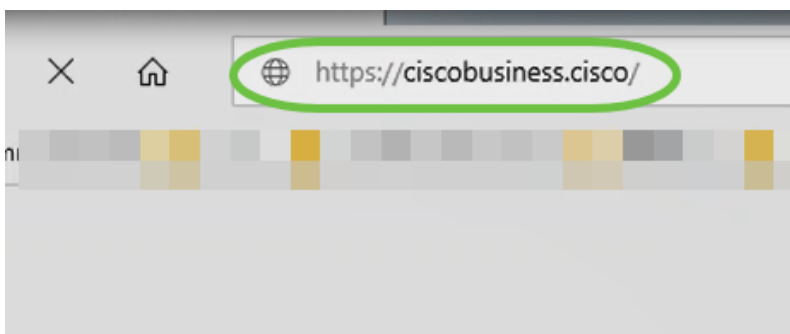
Go to the wireless options on your PC and choose the network that you configured. Click **Connect**.

The *CiscoBusiness-Setup* SSID will disappear after reboot.



Step 12

Open a web browser and type in *https://[IP address of the CBW AP]*. Alternatively, you can type *https://ciscobusiness.cisco* in the address bar and press enter.



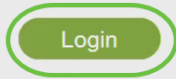
Make sure that you type *https* and not *http* at this step.

Step 13

Click **Login**.

Cisco Business Wireless Access Point

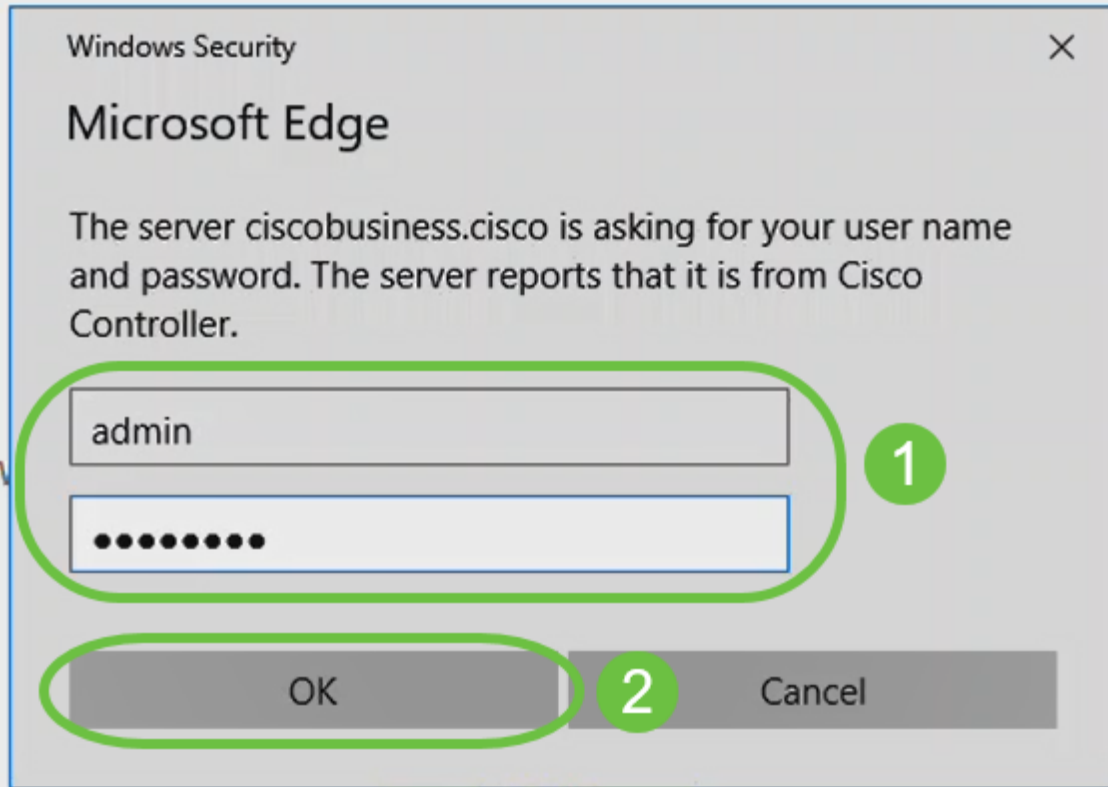
Welcome! Please click the login button to enter your user name and password



© 2015 - 2020 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

Step 14

Log in using the credentials that were configured. Click **OK**.



© 2015 - 2020 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

Step 15

You will be able to access the Web UI page of the AP.



Wireless Troubleshooting Tips

If you have any issues, check out the following tips:

- Make sure the correct Service Set Identifier (SSID) is selected. This is the name that you created for the wireless network.
- Disconnect any VPN for either the mobile app or on a laptop. You might even be connected to a VPN that your mobile service provider uses that you might not even know. For example, an Android (Pixel 3) phone with Google Fi as a service provider there is a built-in VPN that auto-connects without notification. This would need to be disabled to find the Primary AP.
- Log into the Primary AP with `https://<IP address of the Primary AP>`.
- Once you do the initial setup, be sure `https://` is being used whether you are logging into `ciscobusiness.cisco` or by entering the IP address into your web browser. Depending on your settings, your computer may have auto-populated with `http://` since that is what you used the very first time you logged in.
- To help with problems related to accessing the Web UI or browser issues during the use of the AP, in the web browser (Firefox in this case) click on the Open menu, go to Help > Troubleshooting Information and click on Refresh Firefox.

Configure the CBW142ACM Mesh Extenders Using the Web UI

You are in the home stretch of setting up this network, you just need to add your mesh extenders!

Step 1

Plug the two Mesh Extenders into the wall in the locations you have selected. Write down the MAC Address of each mesh extender.

Step 2

Wait about 10 minutes for the Mesh Extenders to boot up.

Step 3

Enter the Primary Access Points (APs) IP address on the web browser. Click **Login** to access the Primary AP.

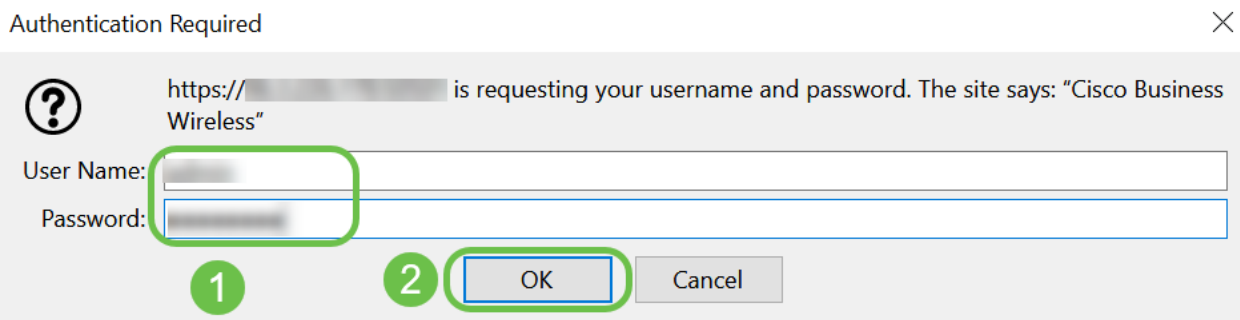
Cisco Business Wireless Access Point

Welcome! Please click the login button to enter your user name and password



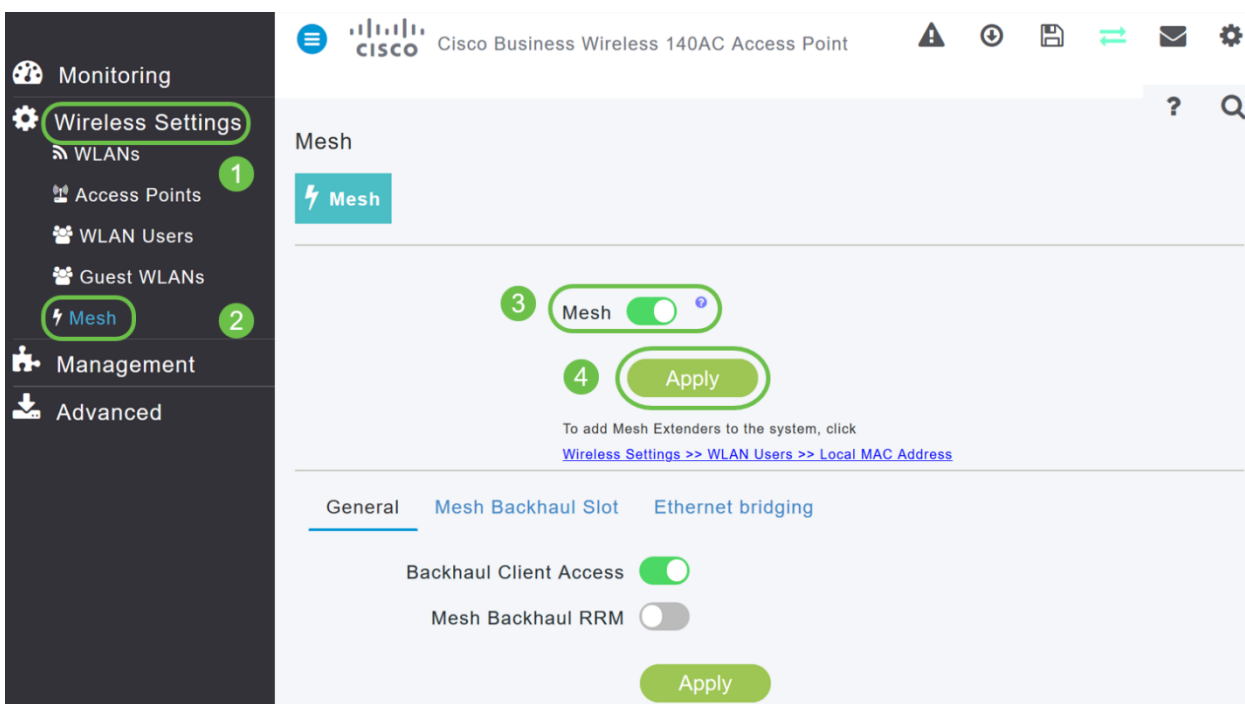
Step 4

Enter your *User Name* and *Password* credentials to access the Primary AP. Click **OK**.



Step 5

Navigate to **Wireless Settings > Mesh** . Make sure the *Mesh* is Enabled. Click **Apply**.



Step 6

If Mesh was not already enabled, the WAP may need to perform a reboot. A pop-up will appear to do a reboot. Confirm. This will take about 10 minutes. During a reboot, the LED will blink green in multiple patterns, alternating rapidly through green, red, and amber before turning green again. There may be small variations in the LED color intensity and hue from unit to unit.

Step 7

Navigate to **Wireless Settings > WLAN Users > Local MAC Addresses**. Click **Add MAC Address**.

The screenshot shows the Cisco Business Wireless 140AC Access Point configuration interface. The left sidebar is dark grey with a white menu. The main content area is light grey. The breadcrumb path is **Wireless Settings > WLAN Users > Local MAC Addresses**. The **Local MAC Addresses** section shows a search bar, an **Add MAC Address** button, a **Refresh** button, and a status bar indicating **Number of Blacklist:0** and **Number of Whitelist:2**. Below this is a table with columns: **Action**, **MAC Address**, **Type**, **Profile Name**, and **Description**. The table contains two entries:

| Action | MAC Address | Type | Profile Name | Description |
|--------|-------------------|-----------|---------------|----------------------|
| | 68:ca:e4:6e:15:58 | AllowList | Any WLAN/RLAN | CBW142 Mesh Extender |
| | a4:53:0e:1f:e4:88 | AllowList | Any WLAN/RLAN | CBW140AC-e488 |

Step 8

Enter the MAC address and Description of the Mesh Extender. Select the *Type* as Allow list. Select the *Profile Name* from the drop-down menu. Click **Apply**.

The screenshot shows the **Add MAC Address** dialog box. It has a blue header with a close button. The form contains the following fields:

- MAC Address**: 68:ca:e4:6e:15:38 (1)
- Description**: CBW142 Mesh Extender (2)
- Type**: Block list Allow list (3)
- Profile Name**: Any WLAN/RLAN (4)

At the bottom, there are two buttons: **Apply** (5) and **Cancel**.

Step 9

Be sure to save all your configurations by pressing the **save icon** on the top-right pane of the screen.



Repeat for each mesh extender.

Check and Update Software Using the Web UI

Don't skip this important step! There are a few ways to update software, but the steps listed below are recommended as the easiest to execute when you use the Web UI.

To view and update the current software version of your Primary AP, perform the following steps.

Step 1

Click the **gear icon** at the top-right corner of the web interface, and then click **Primary AP Information**.

| Primary AP Information | |
|-----------------------------|------------------------------|
| Primary AP Name | Cisco Buisness Wireless |
| Model | CBW-145AC |
| Serial Number | ABC1415DEF1 |
| Software Version | 10.4.1.0 |
| Up Time | 2 days, 17 hours, 45 minutes |
| Primary AP Time | Sat Feb 27 10:05:15 2021 |
| Timezone | San jose |
| Country | Multiple Countries : US |
| Management IP Address | 10.10.10.7 |
| Memory Usage | 63% |
| Max Access Points Supported | 50 |

Step 2

Compare the version that is running to the latest software version. Close the window once you know if you need to update the software.

AP Information

| | |
|-----------------------------|------------------------------|
| Primary AP Name | |
| Model | CBW140AC-B |
| Serial Number | |
| Software Version | 10.0.251.24 |
| Up Time | 5 days, 1 hour, 57 minutes |
| Primary AP Time | Sun Mar 29 16:50:26 2020 |
| Timezone | Central Time (US and Canada) |
| Country | US - United States |
| Management IP Address | 192.168.1.125 |
| Memory Usage | 55% |
| Max Access Points Supported | 50 |

If you are running the latest version of software, you can jump to the [Create WLANs](#) section.

Step 3

Choose **Management > Software Update** from the menu.

The *Software Update* window is displayed with the current software version number listed at the top.

The screenshot shows the 'Software Update' configuration page. On the left is a dark sidebar menu with the following items: 'Management' (1), 'Access', 'Admin Accounts', 'Time', 'Software Update' (2), and 'Advanced'. The main content area is titled 'Software Update' and features a teal 'Version' button with a downward arrow and a green circle containing the number '3'. To the right of this button is a text input field containing '10.0.251.24'. Below this, there is a 'Transfer Mode' dropdown menu set to 'TFTP' and an 'IP Address(IPv4)/Name *' text input field containing '172.16.1.35'.

You can update the CBW AP software and the Current configurations on the Primary AP will not be deleted.

From the *Transfer Mode* drop-down list, choose **Cisco.com**.

| | |
|---------------------------------|-----------|
| Transfer Mode | Cisco.com |
| Automatically Check For Updates | HTTP |
| Last Software Check | TFTP |
| Latest Software Release | SFTP |
| | Cisco.com |

Step 4

To set the Primary AP to automatically check for software updates, choose **Enabled** in the *Automatically Check for Updates* drop-down list. This is enabled by default.

| | |
|---------------------------------|-----------|
| Transfer Mode | Cisco.com |
| Automatically Check For Updates | Enabled |

When a software check is done and if a newer latest or recommended software update is available on Cisco.com, then:

- The **Software Update Alert icon** at the top right corner of the Web UI will be green in color (or gray). Clicking the icon will bring you to the Software Update page.
- The Update button at the bottom of the *Software Update* page is enabled.

Cisco Business Wireless 140AC Access Point

Software Update

Version

10.0.251.24

| | |
|---------------------------------|--------------------------|
| Transfer Mode | Cisco.com |
| Automatically Check For Updates | Enabled |
| Last Software Check | Fri Mar 27 10:44:29 2020 |
| Latest Software Release | 10.0.1.0 |
| Recommended Software Release | 10.0.1.0 |

Check Now

Save
Update
Abort

Software update is available for your Cisco Business Wireless AP/APs on cisco.com

Step 5

Click **Save**. This saves the entries or changes you have made in both *Transfer Mode* and *Automatically Check For Updates*.

The screenshot shows a settings panel with the following elements:

- Transfer Mode:** A dropdown menu set to "Cisco.com".
- Automatically Check For Updates:** A dropdown menu set to "Enabled".
- Last Software Check:** A text field displaying "Tue Apr 21 13:07:11 2020" and a blue "Check Now" button to its right.
- Latest Software Release:** A text field displaying "10.0.1.0" with a blue question mark icon to its right.
- Recommended Software Release:** A text field displaying "10.0.1.0" with a blue question mark icon to its right.
- Buttons:** Three green buttons at the bottom: "Save" (circled in green), "Update", and "Abort".

The *Last Software Check* field displays the timestamp of the last automatic or manual software check. You can view the notes of displayed releases by clicking the **question mark icon** next to it.

This screenshot is identical to the previous one but includes annotations:

- A green circle with the number "1" is placed over the "Automatically Check For Updates" dropdown menu.
- A green circle with the number "2" is placed over the question mark icons next to the "Latest Software Release" and "Recommended Software Release" fields.
- The "Last Software Check" text field is also circled in green.

Step 6

You can manually run a software check anytime by clicking *Check Now*.

| | | |
|---------------------------------|--------------------------|---------------------------|
| Transfer Mode | Cisco.com | ▼ |
| Automatically Check For Updates | Enabled | ▼ |
| Last Software Check | Tue Apr 21 13:07:11 2020 | Check Now |
| Latest Software Release | 10.0.1.0 | ? |
| Recommended Software Release | 10.0.1.0 | ? |

[Save](#) [Update](#) [Abort](#)

Step 7

To proceed with the software update, click **Update**.

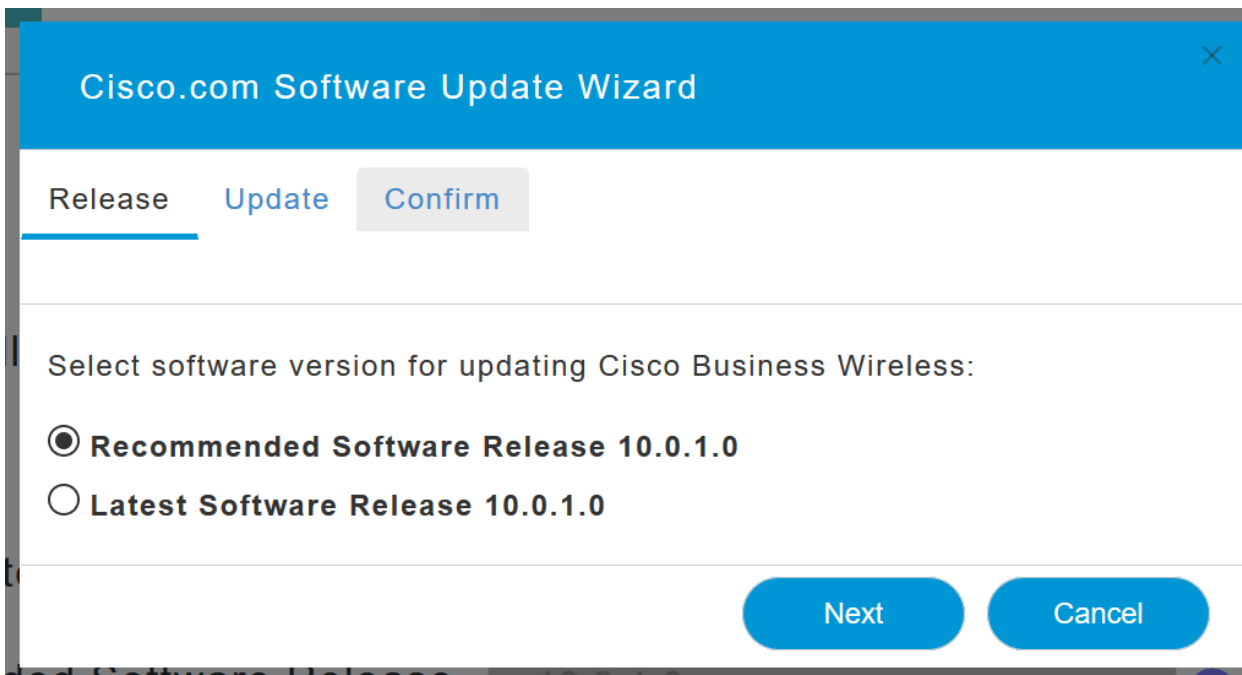
| | | |
|---------------------------------|--------------------------|---------------------------|
| Transfer Mode | Cisco.com | ▼ |
| Automatically Check For Updates | Enabled | ▼ |
| Last Software Check | Tue Apr 21 13:07:11 2020 | Check Now |
| Latest Software Release | 10.0.1.0 | ? |
| Recommended Software Release | 10.0.1.0 | ? |

[Save](#) [Update](#) [Abort](#)

The *Software Update Wizard* appears. The wizard takes you through the following three tabs in sequence:

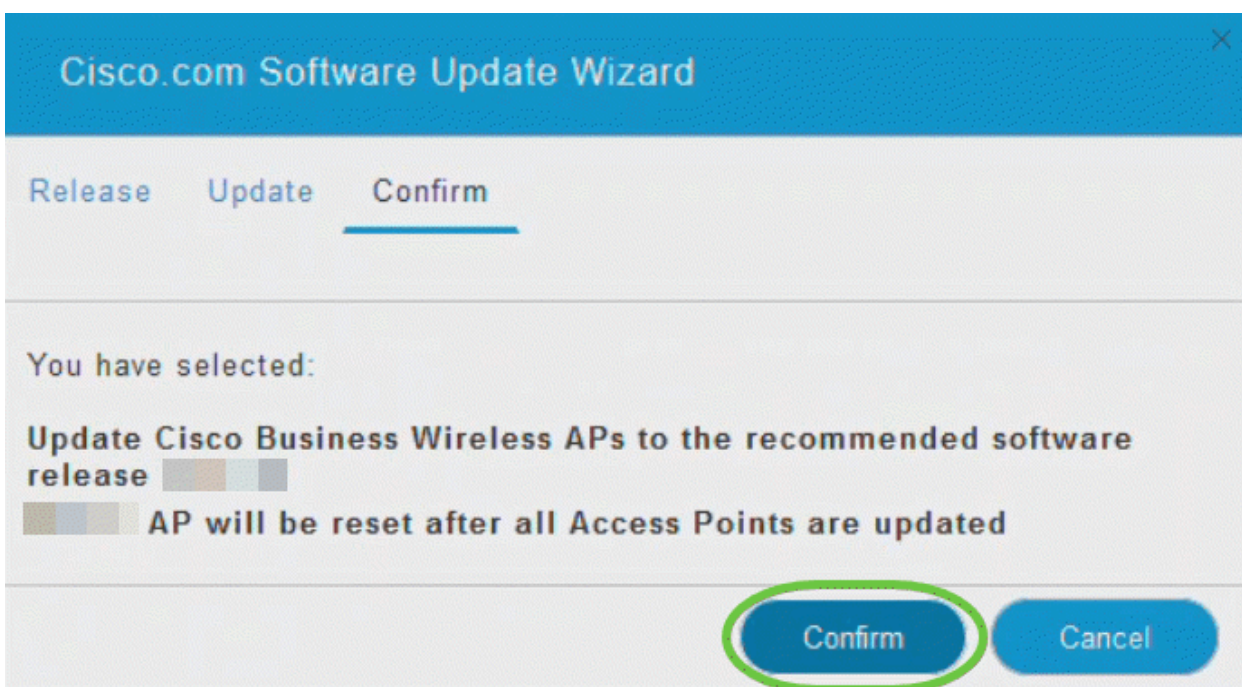
- Release tab - Specify whether you want to update to the recommended software release or the latest software release.
- Update tab - Specify when the APs should be reset. You can opt to have it done right away or schedule it for a later time. To set the Primary AP to automatically reboot after the image pre-download is complete, check the Auto Restart checkbox.
- Confirm tab - Confirm your selections.

Follow the instructions in the wizard. You can go back to any tab at any time before you click *Confirm*.



Step 8

Click **Confirm**.

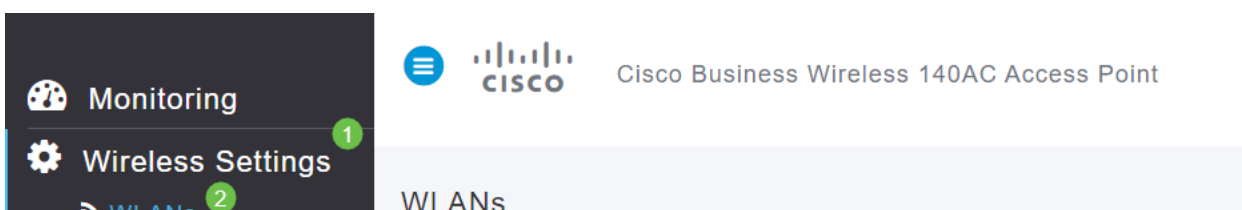


Create WLANs on the Web UI

This section allows you to create Wireless Local Area Networks (WLANs).

Step 1

A WLAN can be created by navigating to **Wireless Settings > WLANs**. Then select **Add new WLAN/RLAN**.



Step 2

Under the *General* tab, enter the following information:

- WLAN ID – Select a number for the WLAN
- Type – Select **WLAN**
- Profile Name – When you enter a name, the SSID will auto-populate with the same name. The name must be unique and should not exceed 31 characters.

The following fields were left as default in this example, but explanations are listed in case you would like to configure them differently.

- SSID – The profile name also acts as the SSID. You can change this if you would like. The name must be unique and should not exceed 31 characters.
- Enable – This should be left enabled for the WLAN to work.
- Radio Policy – Typically you would want to leave this as **All** so that 2.4GHz and 5GHz clients can access the network.
- Broadcast SSID – Usually you would want the SSID to be discovered so you would want to leave this as Enabled.
- Local Profiling – You would only want to enable this option to view the Operating System that is running on the Client or to see the User name.

Click **Apply**.

The screenshot shows the 'Add new WLAN/RLAN' configuration window with the 'General' tab selected. The configuration fields are as follows:

- WLAN ID:** 2 (marked with a green circle 1)
- Type:** WLAN (marked with a green circle 2)
- Profile Name *:** Engineering (marked with a green circle 3)
- SSID *:** Engineering (marked with a green circle 3). A note below states: "WLANs with same SSID can be configured, unless layer-2 security settings are different."
- Enable:**
- Radio Policy:** ALL (marked with a blue question mark icon)
- Broadcast SSID:**
- Local Profiling:** (marked with a blue question mark icon)

At the bottom, there are two buttons: **Apply** (marked with a green circle 4) and **Cancel**.

Step 3

You will be taken to the *WLAN Security* tab.

In this example, the following options were left as the default:

- Guest Network, Captive Network Assistant, and MAC Filtering were left disabled. Details for setting up a guest network are detailed in the next section.
- WPA2 Personal – Wi-Fi Protected Access 2 with Pre-shared Key (PSK) Passphrase Format – ASCII. This option stands for Wi-Fi Protected Access 2 with Pre-Shared Key (PSK).

WPA2 Personal is a method used for securing your network with the use of a PSK authentication. The PSK is configured separately both on the Primary AP, under the WLAN security policy, and on the client. WPA2 Personal does not rely on an authentication server on your network.

- Passphrase Format - **ASCII is left as default.**

The following fields were entered in this scenario:

- Show Passphrase – click the checkbox to be able to see the Passphrase you enter.
- Passphrase – Enter a name for the Passphrase (password).
- Confirm Passphrase – Enter the password again to confirm.

Click **Apply**. This will automatically activate the new WLAN.

General WLAN Security VLAN & Firewall Traffic Shaping Scheduling

Guest Network
 Captive Network Assistant
 MAC Filtering ?
 Security Type WPA2 Personal ▼
 Passphrase Format ASCII ▼
 Passphrase * VerySecure 3
 Confirm Passphrase * VerySecure 2
 1 Show Passphrase
 Password Expiry ?

4

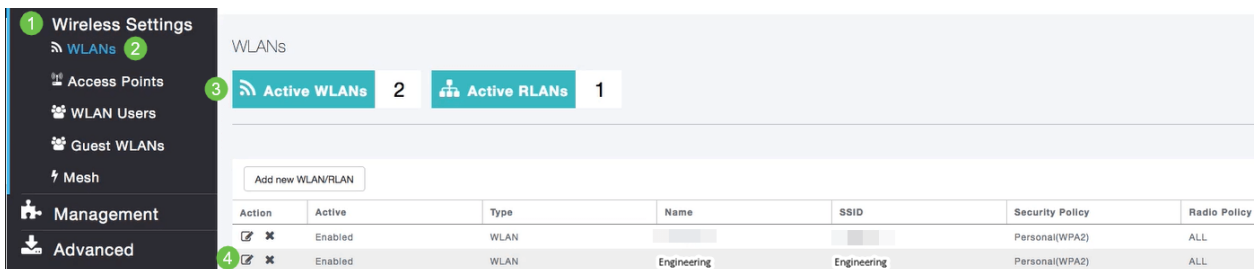
Step 4

Be sure to save your configurations by clicking the **save icon** on the top right panel of the Web UI screen.



Step 5

To view the WLAN you created, select **Wireless Settings > WLANs**. You will see the number of Active WLANs raised to 2, and the new WLAN is displayed.



Repeat these steps for other WLANs you want to create.

Optional Wireless Configurations

You now have all basic configurations set and are ready to roll. You have some options, so feel free to jump to any of the following sections:

- [Create a Guest WLAN using the Web UI \(Optional\)](#)
- [Application Profiling \(Optional\)](#)
- [Client Profiling \(Optional\)](#)
- [I'm ready to wrap this up and start using my network!](#)

Create a Guest WLAN using the Web UI (Optional)

A guest WLAN gives guest access to your Cisco Business Wireless network.

Step 1

Log into the Web UI of the Primary AP. Open a web browser and enter [www.https://ciscobusiness.cisco](https://ciscobusiness.cisco). You may receive a warning before proceeding. Enter your credentials. You can also access it by entering the IP address of the Primary AP.

Step 2

A Wireless Local Area Network (WLAN) can be created by navigating to **Wireless Settings > WLANs**. Then select **Add new WLAN/RLAN**.



Step 3

Under the *General* tab, enter the following information:

WLAN ID – Select a number for the WLAN

Type – Select **WLAN**

Profile Name – When you enter a name, the SSID will auto-populate with the same name. The name must be unique and should not exceed 31 characters.

The following fields were left as default in this example, but explanations are listed in case you would like to configure them differently.

SSID – The profile name also acts as the SSID. You can change this if you would like. The name must be unique and should not exceed 31 characters.

Enable – This should be left enabled for the WLAN to work.

Radio Policy – Typically you would want to leave this as **All** so that 2.4GHz and 5GHz clients can access the network.

Broadcast SSID – Usually you would want the SSID to be discovered so you would want to leave this as Enabled.

Local Profiling – You would only want to enable this option to view the Operating System that is running on the Client or to see the User name.

Click **Apply**.

Add new WLAN/RLAN



General

WLAN Security

VLAN & Firewall

Traffic Shaping

Scheduling

WLAN ID

1

Type

2

Profile Name *

3

SSID *

WLANs with same SSID can be configured, unless layer-2 security settings are different.

Enable

Radio Policy

?

Broadcast SSID

Local Profiling

?

4

Apply

Cancel

Step 4

You will be taken to the *WLAN Security* tab. In this example, the following options were selected.

- Guest Network – Enable
- Captive Network Assistant – If you use Mac or IOS, you will probably want to enable this. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to a Uniform Resource Locator (URL) for iPhone models and if a response is received, then the Internet access is assumed available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window. The CNA may break when redirecting to an Identity Services Engine (ISE) captive portal. The Primary AP prevents this pseudo-browser from popping up.
- Captive Portal – This field is visible only when the Guest Network option is enabled. This is used to specify the type of web portal that can be used for authentication purposes. Select Internal Splash Page to use the default Cisco web-portal-based authentication. Choose External Splash Page if you will have captive portal authentication, using a web

server outside your network. Also, specify the URL of the server in the Site URL field.

Add new WLAN/RLAN

General WLAN Security VLAN & Firewall Traffic Shaping Scheduling

Guest Network 1

Captive Network Assistant 2

MAC Filtering

Captive Portal Internal Splash Page ▼ 3

Access Type Social Login ▼

ACL Name(IPv4) None ▼ ?

ACL Name(IPv6) None ▼ ?

In this example, the Guest WLAN with an enabled Social login access type will be created. Once the user connects to this guest WLAN, they will be redirected to the Cisco default login page where they can find the login buttons for Google and Facebook. The user can log in using their Google or Facebook account to obtain Internet access.

Step 5

On this same tab, select an *Access Type* from the drop-down menu. In this example, *Social Login* was selected. This is the option that allows guests to use their Google or Facebook credentials to authenticate and get access to the network.

Other options for *Access Type* include:

Local User Account – The default option. Choose this option to authenticate guests using the username and password which you can specify for guest users of this WLAN, under **Wireless Settings > WLAN Users**. This is an example of the default Internal Splash Page.



Welcome to the Cisco Business Wireless

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name

Password

You can customize this by navigating to **Wireless Settings > Guest WLANs**. From here you can enter a *Page Headline* and *Page Message*. Click **Apply**. Click **Preview**.

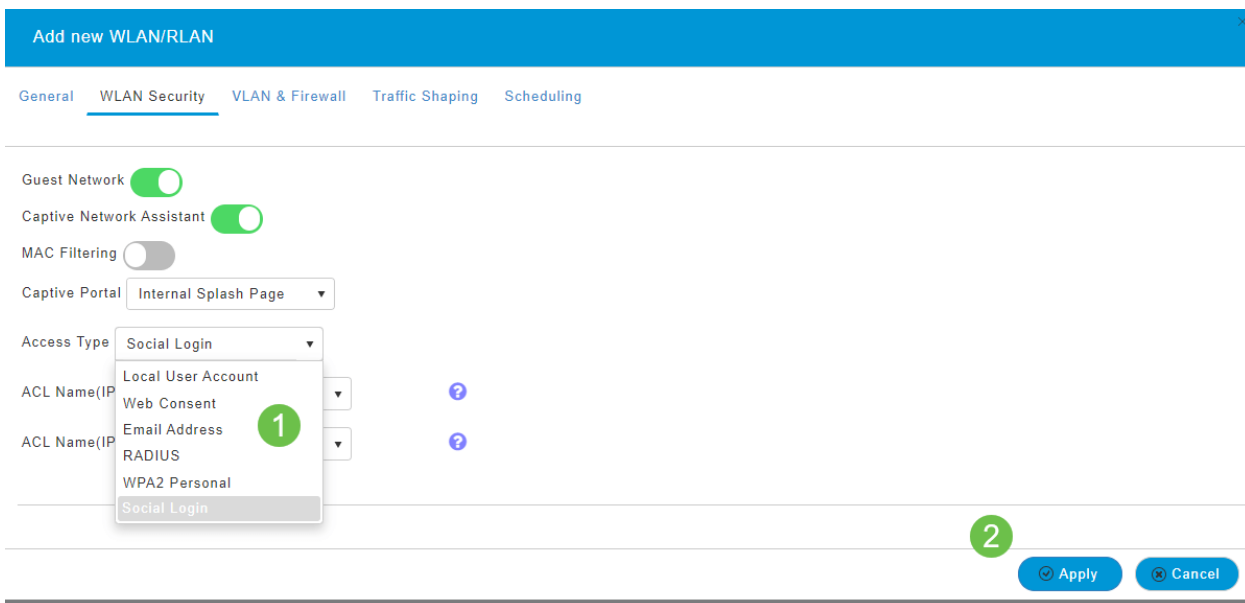
Web Consent – Allows guests access to the WLAN upon acceptance of displayed terms and conditions. Guest users can access the WLAN without entering a username and password.

Email Address – Guest users will need to enter their email address to access the network.

RADIUS – Use this with an external authentication server.

WPA2 Personal – Wi-Fi Protected Access 2 with Pre-shared Key (PSK)

Click **Apply**.



Step 6

Be sure to save your configurations by clicking the **save icon** on the top right panel of the Web UI screen.



You have now created a guest network that is available on your CBW network. Your guests will appreciate the convenience.

Application Profiling using the Web UI (Optional)

Profiling is a subset of features that enable enacting organizational policy. It allows you to match and prioritize traffic types. Like rules make decisions about how to rank or drop the traffic. The Cisco Business Mesh Wireless system features client and application profiling. The act of accessing a network as a user begins with many exchanges of information, among that information is the type of traffic. Policy interrupts traffic flow to direct the path, much like a flow-chart. Other types of policy features include - guest access, access control lists, and QoS.

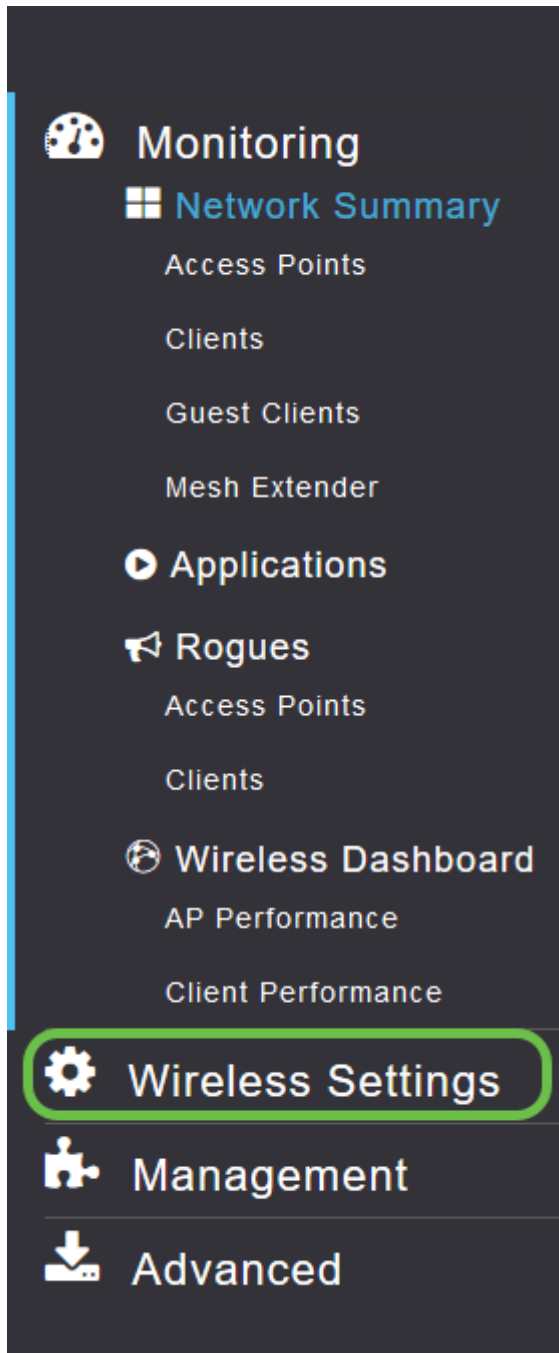
Step 1

Navigate to the menu on the left-hand side of the screen if you don't see the left-hand menu bar.



Step 2

The Monitoring menu loads by default when signing into the device. You will need to click **Wireless Settings**.



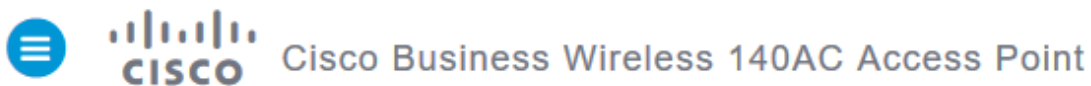
The image below is similar to what you will see when you click the Wireless Settings link.

The screenshot shows the Cisco Business Wireless 140AC Access Point management interface. The left sidebar contains navigation options: Monitoring, Wireless Settings (with sub-options: WLANs, Access Points, WLAN Users, Guest WLANs, Mesh), Management, and Advanced. The main content area is titled 'WLANs' and features a teal button with a Wi-Fi icon and the text 'Active WLANs 1'. Below this is a table with the following data:


| Action | Active | Type | Name | SSID | Security Policy | Radio Policy |
|---------------------------------------|---------|------|------|------|-----------------|--------------|
| <input checked="" type="checkbox"/> ✕ | Enabled | WLAN | EZ1K | EZ1K | Personal(WPA2) | ALL |

Step 3

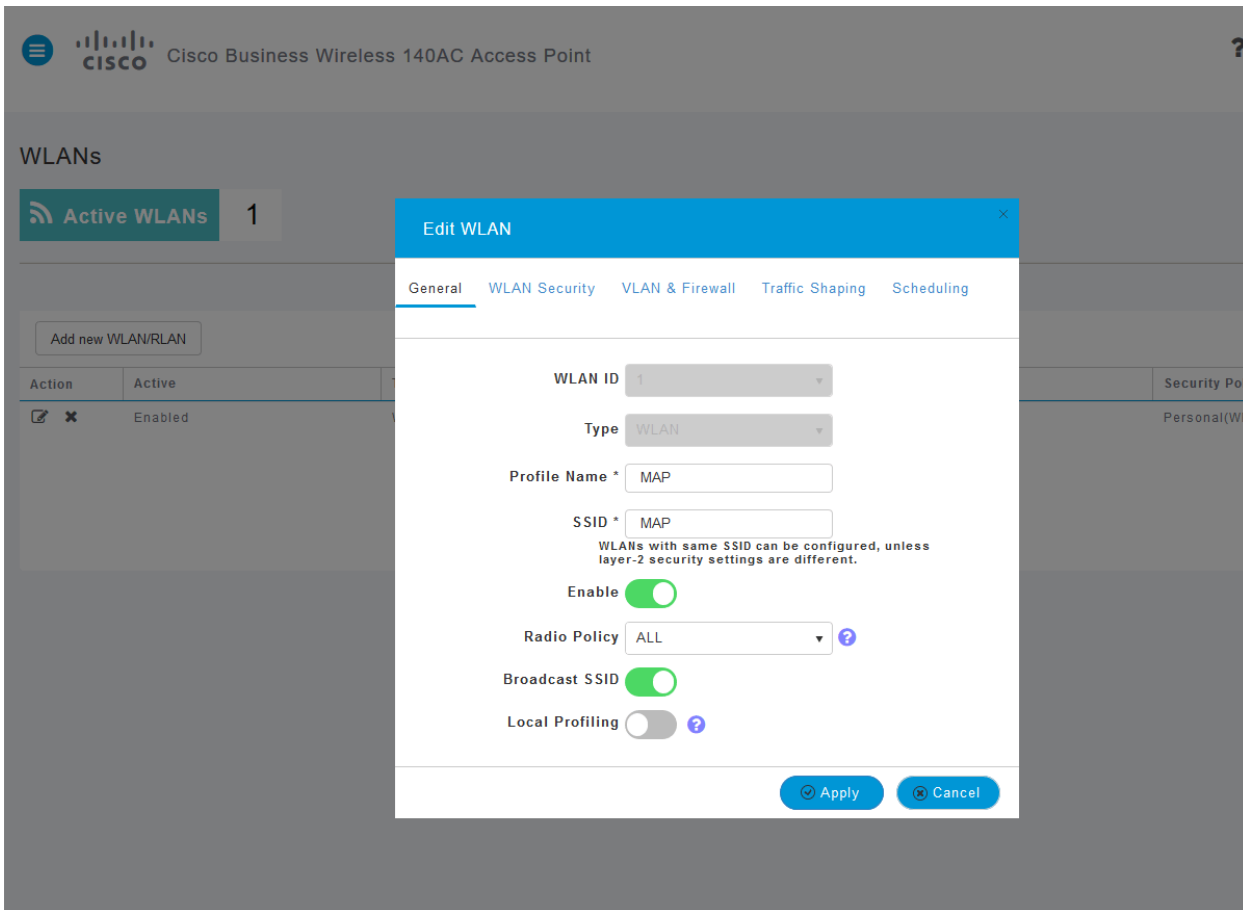
Click the **edit icon** to the left of the Wireless Local Area Network you want to enable the application on.



The screenshot shows the Cisco Business Wireless 140AC Access Point management interface. The left sidebar contains navigation options: Monitoring, Wireless Settings (with sub-options: WLANs, Access Points, WLAN Users, Guest WLANs, Mesh), Management, and Advanced. The main content area is titled 'WLANs' and features a teal button with a Wi-Fi icon and the text 'Active WLANs 1'. Below this is a table with the following data:

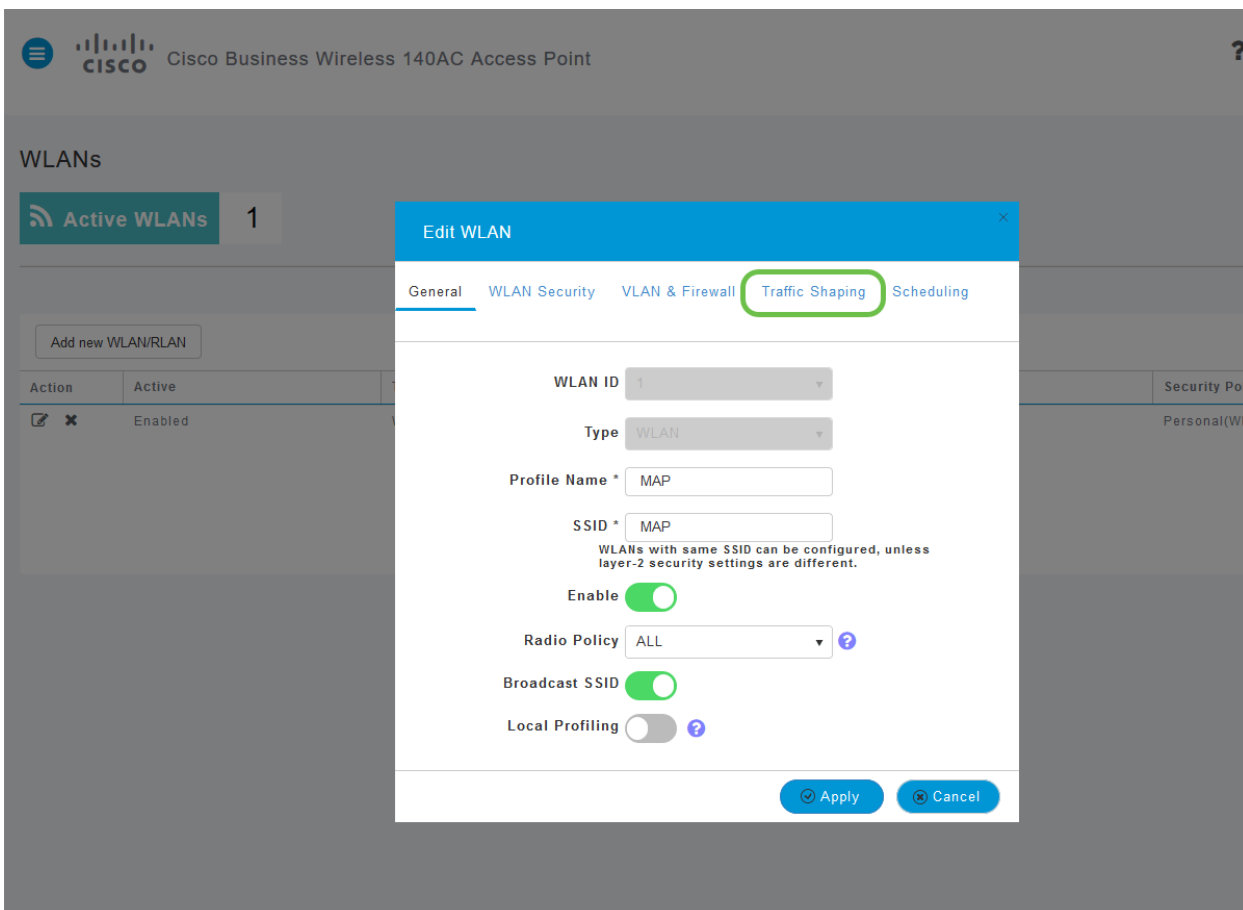
| Action | Active | Type | Name | SSID | Security Policy | Radio Policy |
|---|---------|------|------|------|-----------------|--------------|
| <input checked="" type="checkbox"/> ✕  | Enabled | WLAN | EZ1K | EZ1K | Personal(WPA2) | ALL |

Since you recently added the WLAN, your *Edit WLAN* page may appear similar to the below:

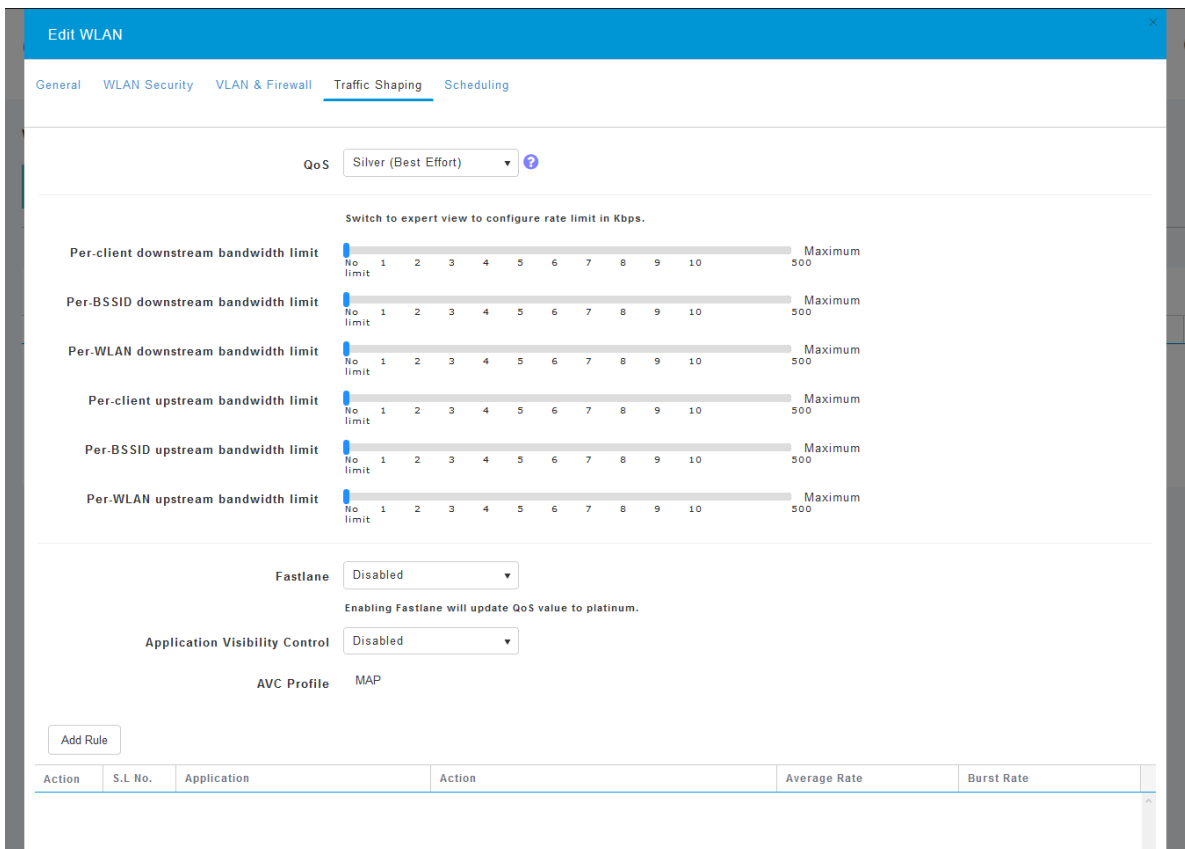


Step 4

Navigate to the **Traffic Shaping** tab by clicking on it.

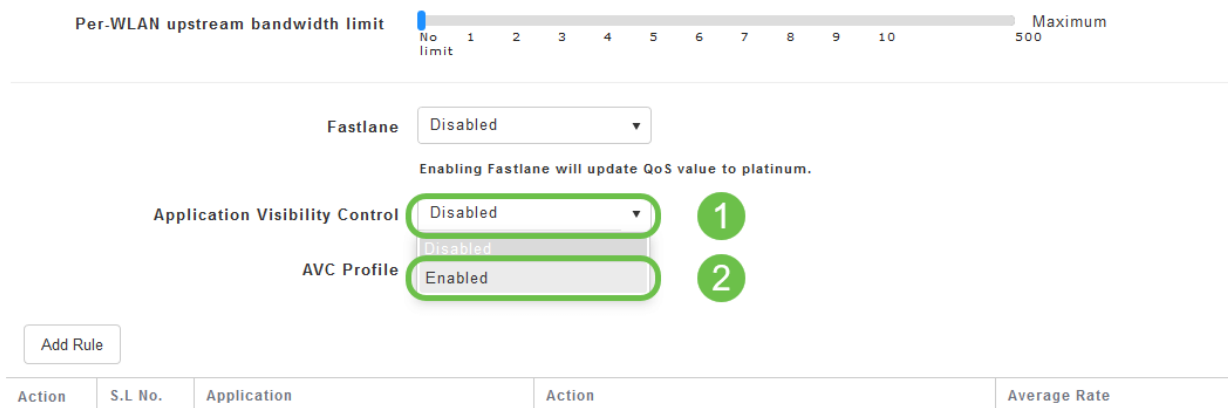


Your screen may appear as follows:



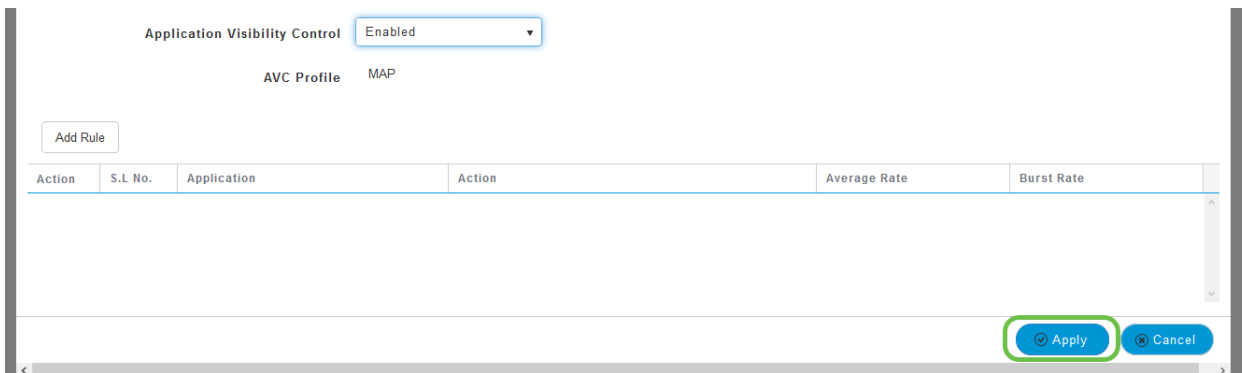
Step 5

Toward the bottom of the page, you will find the *Application Visibility Control* feature. This is disabled by default. Click the dropdown and select **Enabled**.



Step 6

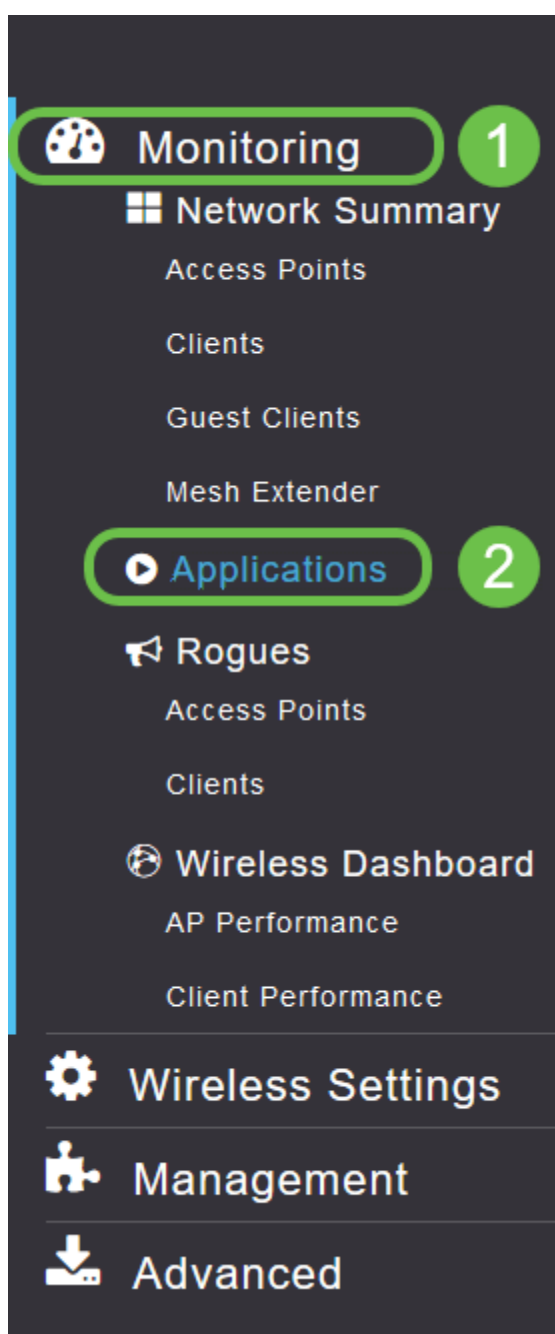
Click the **Apply** button.



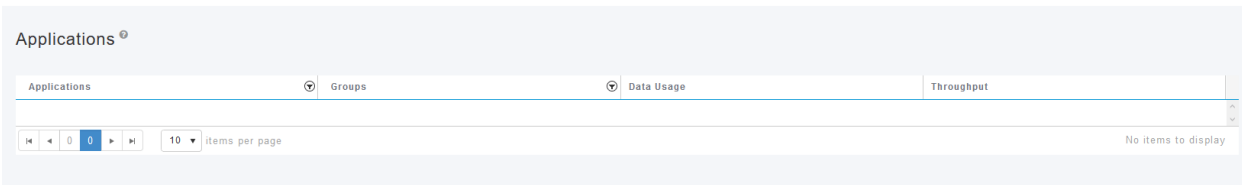
This setting must be enabled, otherwise the feature will not function.

Step 7

Click the cancel button to close the WLAN sub-menu. Then click the **Monitoring** menu on the left-hand menu bar. Once you are able, click the **Applications** menu item.



If you've had no traffic to any source, your page will be blank as shown below.



This page will display the following information:

- Application – includes many different types
- Groups – Indicates the type of application group for easier sorting
- Data Usage – The amount of data used by this service overall
- Throughput – The amount of bandwidth used by the application

You can click on the tabs to sort from largest to smallest, which can help identify the largest consumers of network resources.

This feature is very powerful for managing your WLAN resources on a granular level. Below are some of the more common groups and application types. Your list is likely to include many more, including the following groups and examples:

- Browsing
 - EX: Client-specific, SSL
- Email
 - EX: Outlook, Secure-pop3
- Voice-and-video
 - EX: WebEx, Cisco Spark,
- Business-and-Productivity-tools
 - EX: Microsoft Office 365,
- Backup-and-storage
 - EX: Windows-Azure,
- Consumer-Internet
 - iCloud, Google Drive
- Social Networking
 - EX: Twitter, Facebook
- Software Updates
 - EX: Google-Play, IOS
- Instant Messaging
 - EX: Hangouts, Messages

Shown here is an example of what the page will look like when populated.

Cisco Business Wireless 145AC Access Point

Applications

| Applications | Groups | Data Usage | Throughput |
|---------------------|---------------------------------|------------|------------|
| ssl | browsing | 2.6 MB | 1.1 Mbps |
| outlook-web-service | email | 819.4 KB | 233.1 kbps |
| cisco-spark | voice-and-video | 735.6 KB | 0.0 bps |
| secure-pop3 | email | 453.1 KB | 0.0 bps |
| ms-office-365 | business-and-productivity-tools | 238.2 KB | 75.1 kbps |
| webex-meeting | voice-and-video | 132.3 KB | 0.0 bps |
| samsung | browsing | 79.4 KB | 0.0 bps |
| windows-azure | backup-and-storage | 74.0 KB | 5.7 kbps |
| twitter | social-networking | 48.6 KB | 0.0 bps |
| icloud | consumer-internet | 47.3 KB | 0.0 bps |

10 items per page 1 - 10 of 28 items

Each table heading is clickable for sorting which is especially useful for *Data Usage* and *Throughput* fields.

Step 8

Click the row for the type of traffic you would like to manage.

Cisco Business Wireless 145AC Access Point

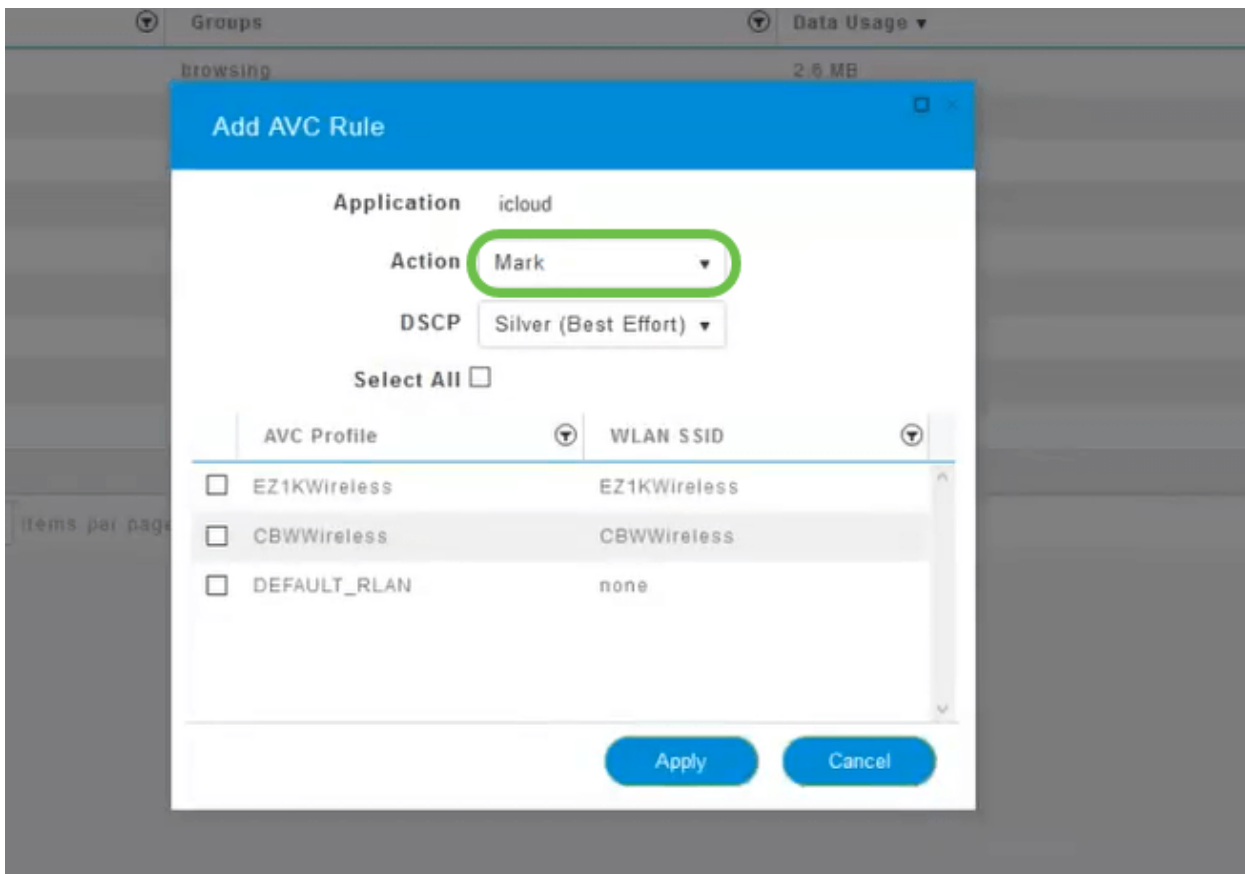
Applications

| Applications | Groups | Data Usage | Throughput |
|---------------------|---------------------------------|------------|------------|
| ssl | browsing | 2.6 MB | 1.1 Mbps |
| outlook-web-service | email | 819.4 KB | 233.1 kbps |
| cisco-spark | voice-and-video | 735.6 KB | 0.0 bps |
| secure-pop3 | email | 453.1 KB | 0.0 bps |
| ms-office-365 | business-and-productivity-tools | 238.2 KB | 75.1 kbps |
| webex-meeting | voice-and-video | 132.3 KB | 0.0 bps |
| samsung | browsing | 79.4 KB | 0.0 bps |
| windows-azure | backup-and-storage | 74.0 KB | 5.7 kbps |
| twitter | social-networking | 48.6 KB | 0.0 bps |
| icloud | consumer-internet | 47.3 KB | 0.0 bps |

10 items per page 1 - 10 of 28 items

Step 9

Click the **Action** drop-down box to select how you will treat that traffic type.



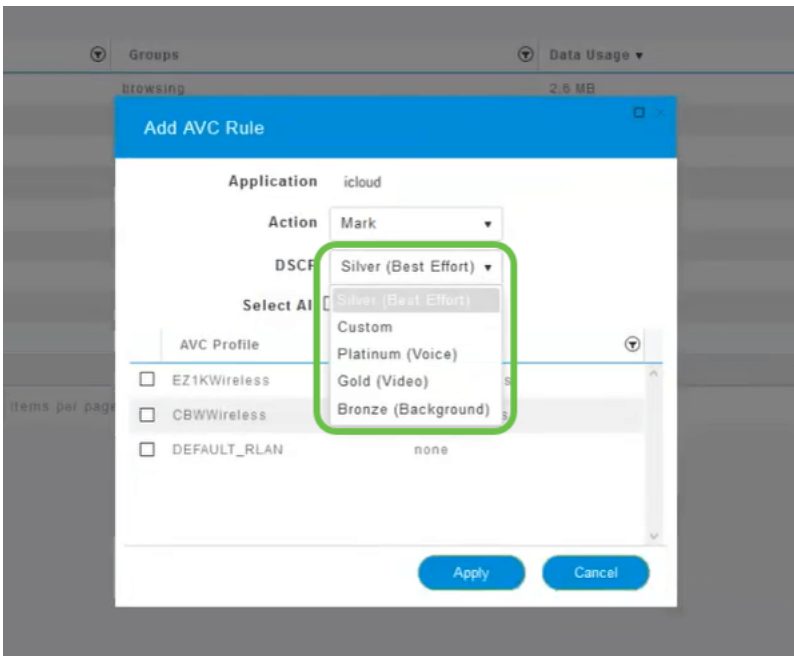
For this example, we're leaving this option at *Mark*.

Action to take on traffic

- Mark – Places the traffic type into one of Differentiated Services Code Point (DSCP) 3 tiers -governing how many resources are available to the application type
- Drop – Do not do anything but discard the traffic
- Rate Limit – Enables you to set the Average Rate, Burst Rate in Kbps

Step 10

Click the drop-down box in the **DSCP** field to select from the following options.



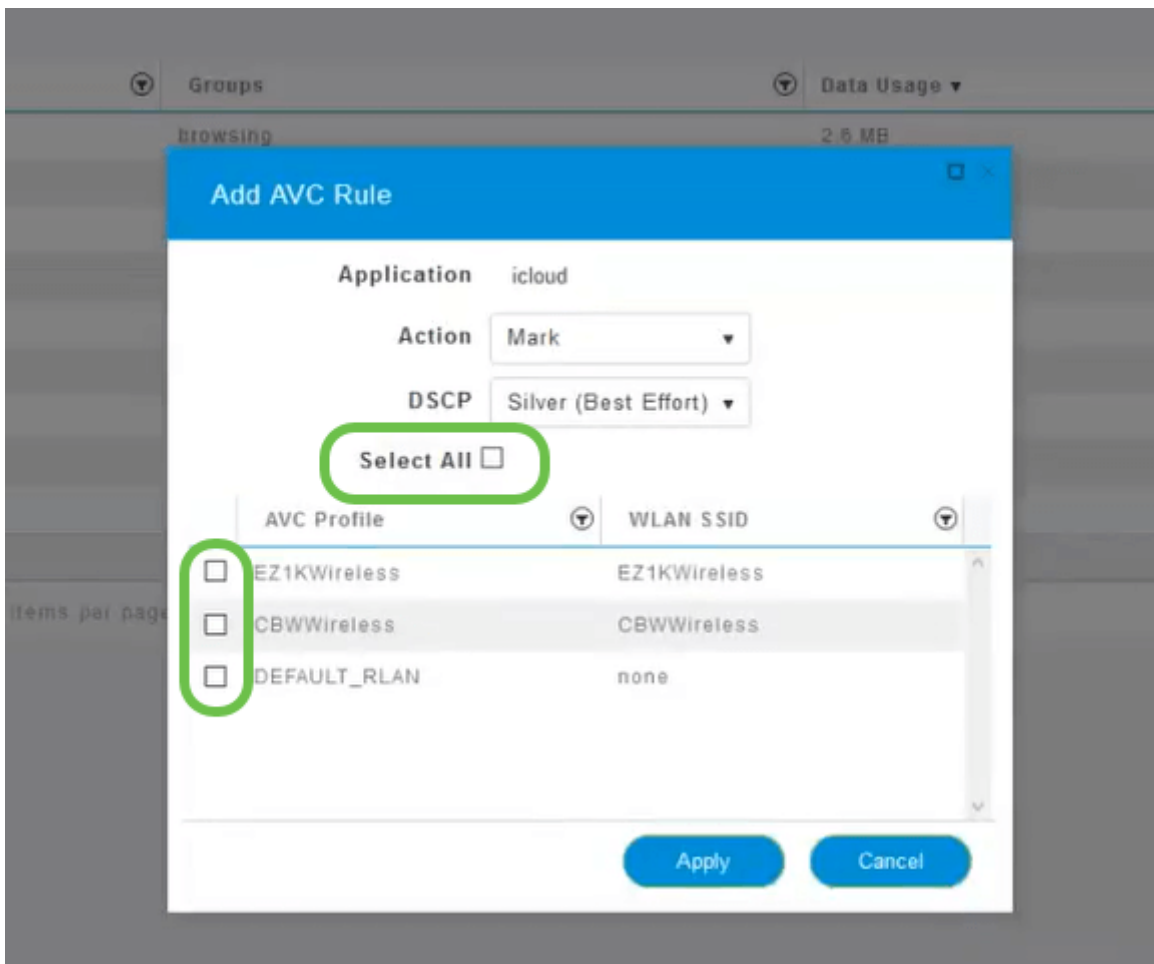
Below are the DSCP options for the traffic to be marked. These options progress from fewer resources to more resources available to the traffic type you are editing.

- Bronze (Background) – Less
- Silver (Best Effort)
- Gold (Video)
- Platinum (Voice) More
- Custom – User set

As a web convention, traffic has migrated toward SSL browsing, which prevents you from seeing what's inside the packets as they move from your network into the WAN. As such, a large majority of web traffic will be using SSL. Setting SSL traffic for a lower priority may affect your browsing experience.

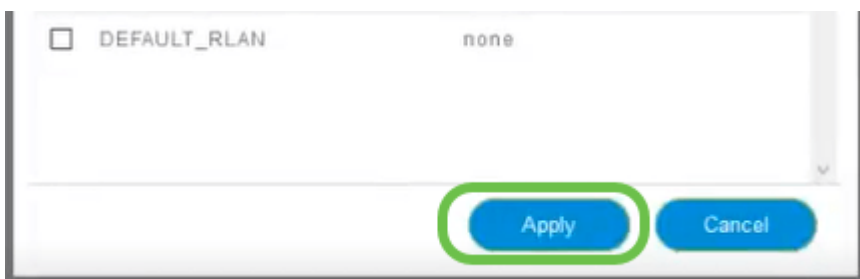
Step 11

Now select the individual SSID you would like this policy to run or click **Select All**.



Step 12

Now click **Apply** to begin this policy.



Two cases where this could apply:

- Guests/Users streaming a large amount of traffic preventing mission-critical traffic from getting through. You can either raise the priority for Voice, lower the priority of Netflix traffic to improve things.
- Large software updates downloading during office hours can be deprioritized or rate limited.

You did it! Application profiling is a very powerful tool that can be further enabled by also enabling Client Profiling, as is detailed in the next section.

Client Profiling using the Web UI (Optional)

Upon connecting to a network, devices exchange client profiling information. By

default, *Client Profiling* is disabled. This information may include:

- Host Name – or the name of the device
- Operating System – the core software of the device
- OS Version – The iteration of the applicable software

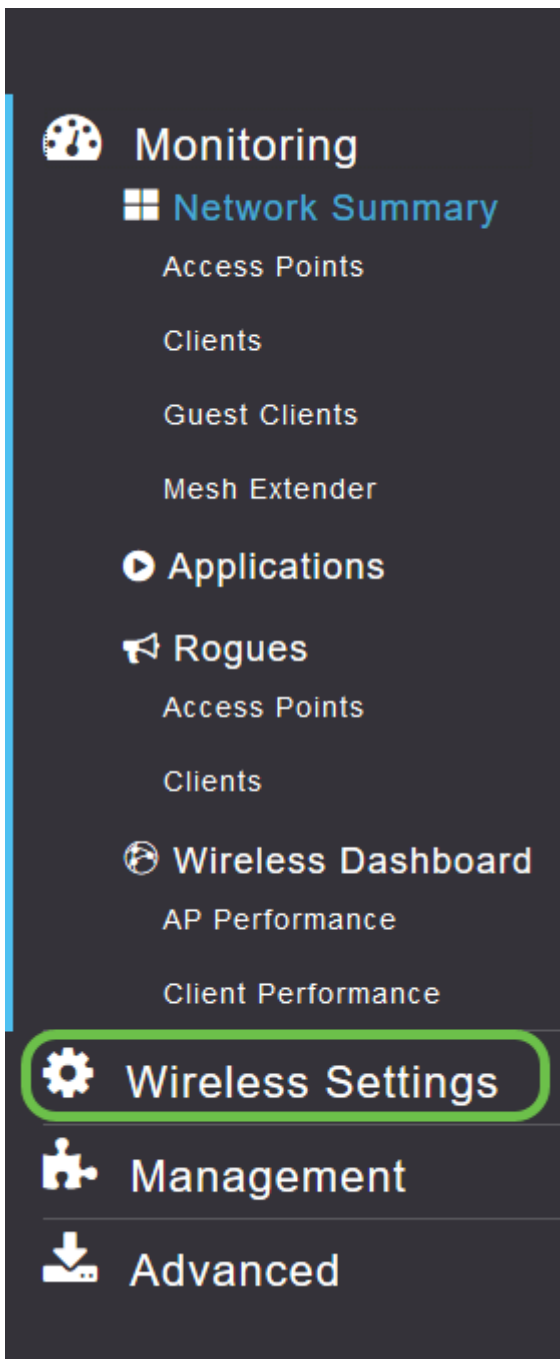
Statistics about these clients include the amount of data used and throughput.

Tracking client profiles enables greater control over the wireless local area network. Or you could use it as a function of another feature. Such as using application throttling device types that don't carry mission-critical data for your business.

Once enabled, client details for your network can be found on the Monitoring section of the Web UI.

Step 1

Click **Wireless Settings**.



The below is similar to what you will see when your click the Wireless Settings link:

Monitoring

Wireless Settings

- WLANs
- Access Points
- WLAN Users
- Guest WLANs
- Mesh

Management

Advanced

WLANs

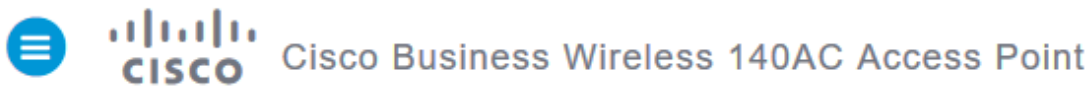
Active WLANs 1

Add new WLAN/RLAN

| Action | Active | Type | Name | SSID | Security Policy | Radio Policy |
|--------|---------|------|------|------|-----------------|--------------|
| | Enabled | WLAN | EZ1K | EZ1K | Personal(WPA2) | ALL |

Step 2

Decide which WLAN you want to use for the application and click the **edit icon** to the left of it.



WLANs

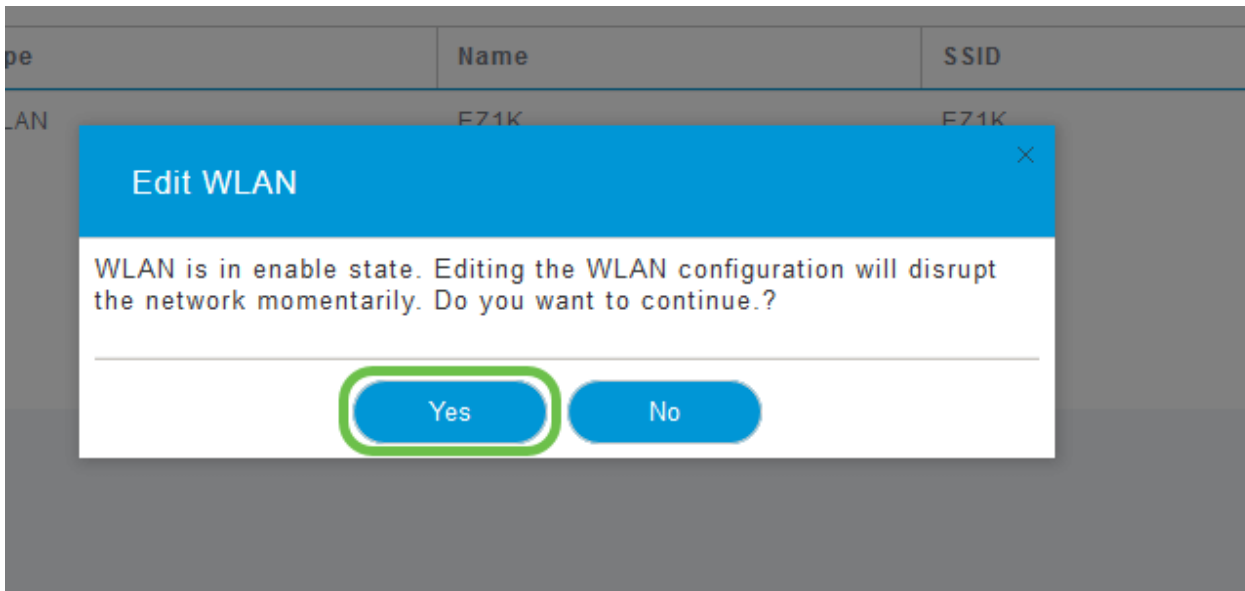
Active WLANs 1

Add new WLAN/RLAN

| Action | Active | Type | Name | SSID | Security Policy | Radio Policy |
|--------|---------|------|------|------|-----------------|--------------|
| | Enabled | WLAN | EZ1K | EZ1K | Personal(WPA2) | ALL |

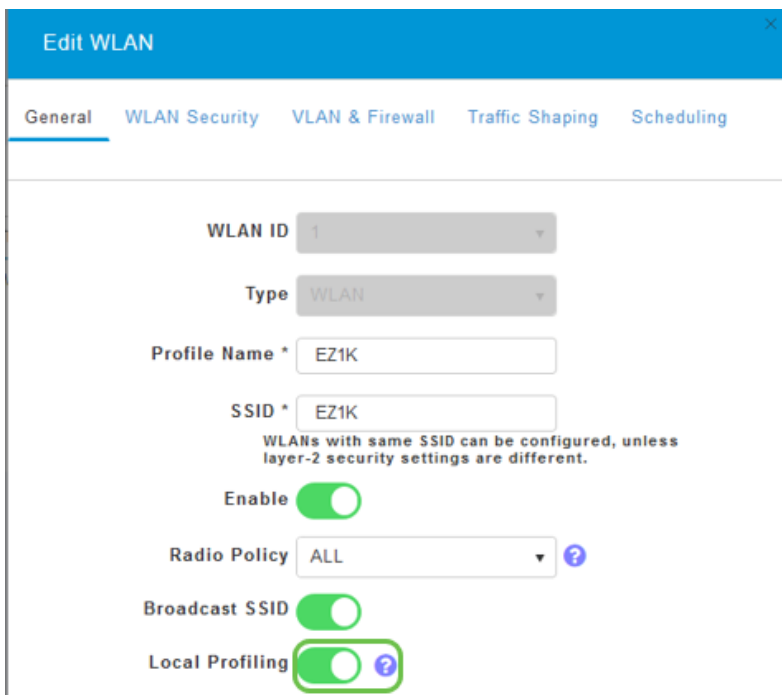
Step 3

A pop-up menu may appear similar to the below. This important message may temporarily affect service on your network. Click **Yes** to move forward.



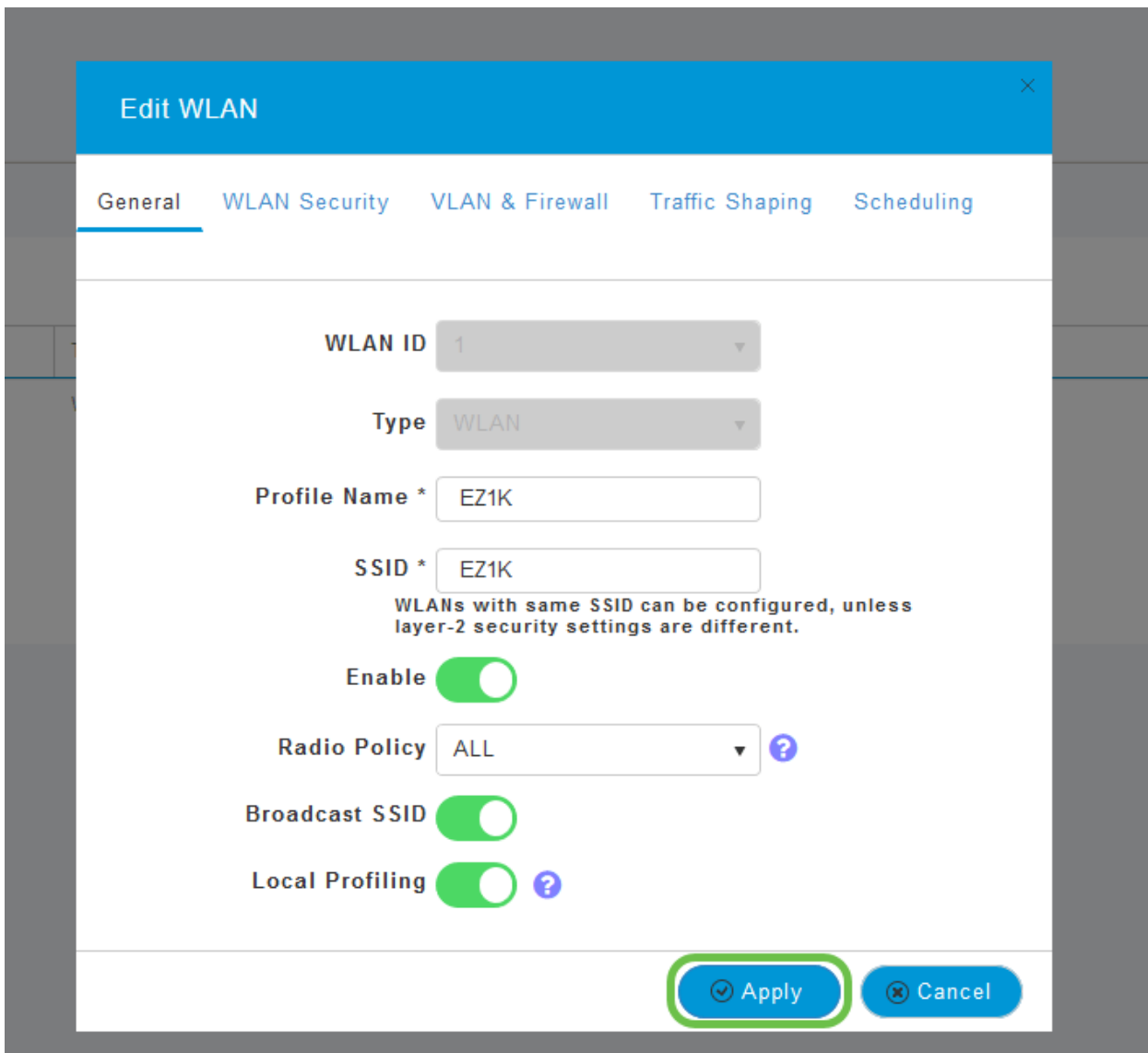
Step 4

Toggle client profiling by clicking the **Local Profiling** toggle button.



Step 5

Click **Apply**.



Step 6

Click the **Monitoring** section menu item on the left-hand side. You will see the client data begin to appear in the Dashboard of the *Monitoring* tab.

| CLIENTS | | | |
|------------------|--------------------------|--------|------------|
| Client Identity | Device Type | Usage | Throughput |
| 1 Anthony's-iPad | Apple-iPad | 1.0 GB | 260.3 bps |
| 2 Galaxy-S9 | Android-Samsung-Galax... | 8.4 MB | 1.2 kbps |

Conclusion

You now have now completed the setup of your secure network. What a great feeling, now take a minute to celebrate and then get to work!

We want the best for our customers, so if you have any comments or suggestions regarding this topic, please send us an email to the [Cisco Content Team](#).

If you would like to read other articles and documentation, check out the support pages for your hardware:

- [Cisco RV345P VPN Router with PoE](#)
- [Cisco Business 140AC Access Point](#)
- [Cisco Business 142ACM Mesh Extender](#)