

e·quinux



VPN Tracker 365

VPN Configuration Guide

Cisco Small Business RV3xx VPN Routers

© 2021 equinix AG and equinix USA, Inc. All rights reserved.

Under copyright law, this configuration guide may not be copied, in whole or in part, without the written consent of equinix AG or equinix USA, Inc. Your rights to the software are governed by the accompanying software license agreement.

The equinix logo is a trademark of equinix AG and equinix USA, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

equinix shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of this document or any change to the router in general, including without limitation, any lost profits, business, or data, even if equinix has been advised of the possibility of such damages.

Every effort has been made to ensure that the information in this configuration guide is accurate. equinix is not responsible for printing or clerical errors.

Revised October 2021

Apple, the Apple logo, Mac, and macOS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

www.equinix.com

Contents

Task 1 – Configure your Cisco Small Business VPN Router	5
Step 1 – Retrieve your network settings	5
Step 2 - Set up a new VPN tunnel	6
Task 2 – VPN Tracker Configuration	7
Step 1 - Add a connection	7
Step 2 – Configure the VPN Connection	7
Task 3 - Testing the VPN connection	8
Troubleshooting	9
Technical Support	9

Introduction

My VPN Gateway Configuration Checklist

Throughout this guide, there are certain pieces of information that are needed later on for configuring VPN Tracker 365. This information is marked with red numbers to make it easier to reference it later. You can print this checklist to help keep track of the various settings of your Cisco Small Business VPN router.

Identifiers

(1) WAN IP Address:

(2) Group Name:

Authentication

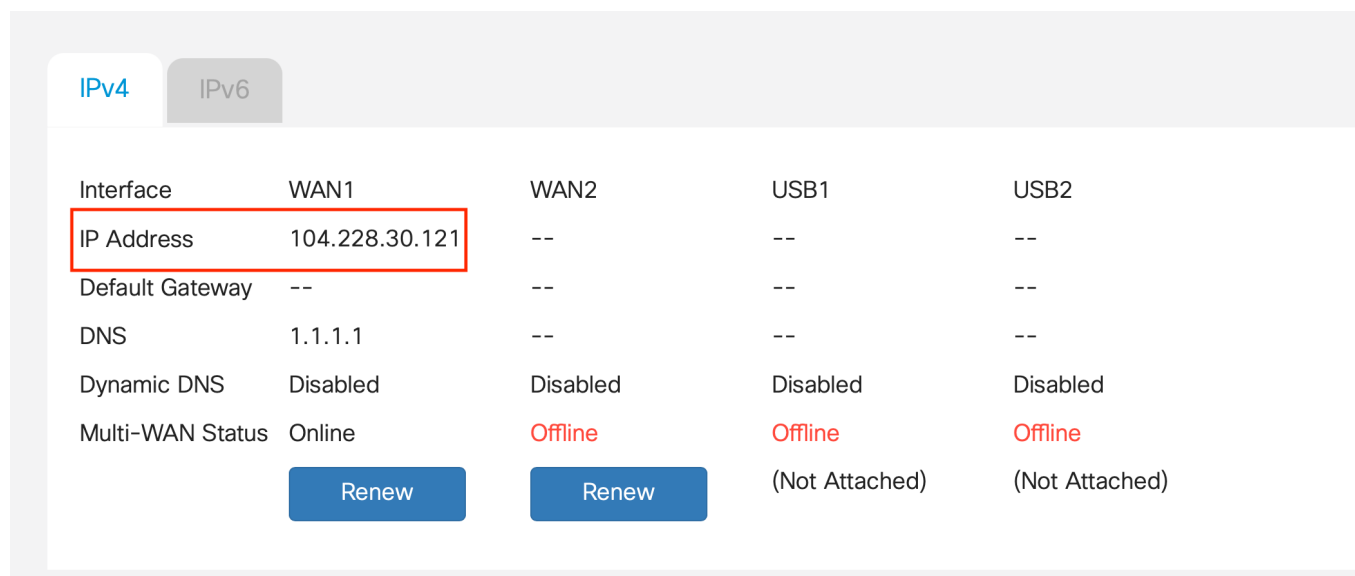
(3) Pre-Shared Key:

Task 1 – Configure your Cisco Small Business VPN Router

This section describes the configuration of your Cisco Small Business device. If you do not yet have VPN configured and in use on your device, please proceed exactly as described in this section.

Step 1 – Retrieve your network settings

- Connect to your Cisco Small Business device's web interface.
- Go to **Status and Statistics > System Summary**
- Scroll down to the **IPv4 tab** and note down your WAN IP address as **(1)** on your Configuration Checklist:



Interface	WAN1	WAN2	USB1	USB2
IP Address	104.228.30.121	--	--	--
Default Gateway	--	--	--	--
DNS	1.1.1.1	--	--	--
Dynamic DNS	Disabled	Disabled	Disabled	Disabled
Multi-WAN Status	Online	Offline	Offline	Offline
	Renew	Renew	(Not Attached)	(Not Attached)

Step 2 - Set up a new VPN tunnel

- Go to VPN > Client to Site
- Click the "+" icon to Add a new tunnel and select Cisco VPN Client
- Fill out the settings for the new tunnel:
 - ◆ **Group Name:** Choose a name to identify the new tunnel (i.e. vpntracker) and note this down as **(2)** in your checklist
 - ◆ **Interface:** Select the local WAN port to be used for the policy (i.e. WAN 1)
 - ◆ **Pre-shared Key:** Set a secure password for your connection and note this as **(3)** in your checklist
 - ◆ **User Group:** Enter the IP address range you want to reserve for your VPN users (i.e. 10.0.1.1 - 10.0.1.100 for 100 users)
 - ◆ **Split Tunnel Table (optional):** Fill out these settings if you want to enable split tunneling for VPN users

The screenshot shows the 'Add a New Tunnel' configuration page. The left sidebar contains navigation options: Getting Started, Status and Statistics, Administration, System Configuration, WAN, LAN, Wireless, Routing, Firewall, VPN (highlighted), VPN Status, IPSec Profiles, Site-to-Site, Client-to-Site, Teleworker VPN Client, PPTP Server, L2TP Server, GRE Tunnel, SSL VPN, VPN Passthrough, and Security.

The main content area is titled 'Add a New Tunnel' and includes the following settings:

- Client Selection:** Cisco VPN Client (selected), 3rd Party Client
- Enable:**
- Group Name:** vpntracker
- Interface:** WAN1
- IKE Authentication Method:** Pre-shared Key (selected). Pre-shared Key: hjj997vvcSSi\$xyQk99! (Strength Meter: Red, Yellow, Green). Minimum Pre-shared Key Complexity: Enable. Show Pre-shared Key: Enable.
- Certificate:** Certificate. User Group: (empty)
- User Group Table:** A table with columns for Group Name and a plus icon for adding new groups.
- Mode:** Client (selected), NEM
- Pool Range for Client LAN:** Start IP: 10.0.1.1, End IP: 10.0.1.100

The screenshot shows the 'Mode Configuration' page with the following settings:

- Primary DNS Server:** 192.168.1.1
- Secondary DNS Server:** (empty)
- Primary WINS Server:** (empty)
- Secondary WINS Server:** (empty)
- Default Domain:** (empty)
- Backup Server 1:** (empty) (IP Address or Domain Name)
- Backup Server 2:** (empty) (IP Address or Domain Name)
- Backup Server 3:** (empty) (IP Address or Domain Name)
- Split Tunnel:**
- Split Tunnel Table:** A table with columns for IP Address and Netmask. One entry is visible: IP Address: 192.168.1.0, Netmask: 255.255.255.0.

Task 2 – VPN Tracker Configuration

After finishing Task 1, you should now have completed a configuration checklist containing your Cisco router's settings. We will now create a matching configuration in VPN Tracker 365.

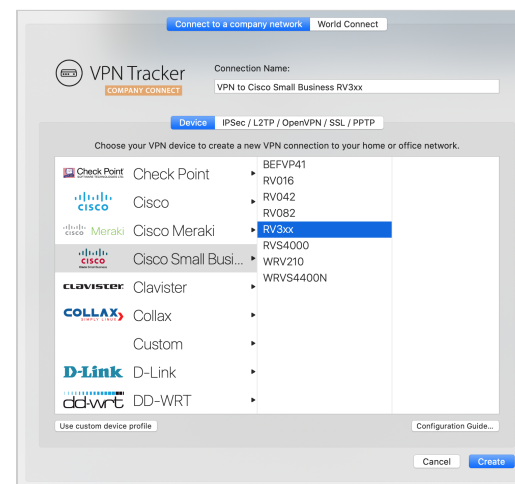
Step 1: Add a connection

- Open VPN Tracker 365.
- Click on the + in the bottom left corner of the app window and select "Create new Company Connection"
- Select **Cisco** from the list.
- Select **RV Series** and enter a name for your connection.

Step 2 – Configure the VPN Connection

You can now configure your connection using the steps outlined in Task 1:

- **VPN Gateway:** Enter your Cisco device's public IP address or its host name **(1)** from your Configuration Checklist.
- **Authentication:** Enter the pre-shared key you set up during the tunnel configuration **(3)** to save time for the future, check the box "Store in Keychain" to save the password in your keychain so you are not asked for it again when connecting the next time.
- **Local Identifier:** Enter the Group Name for your connection **(2)**



Task 3 - Testing the VPN connection

In order to test your connection, you will need to connect from a different location.

For example, if you are setting up a VPN connection to your office, try it out at home, or from an Internet cafe, or go visit a friend.

Connect to your VPN

- Check first of all that your internet connection is working as it should be. Use this link as a test: <http://www.equinux.com>
- Start the VPN Tracker 365 app.
- Click on the On/Off slider to turn on your connection.

IMPORTANT:

If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.

Connected!

Connecting may take a couple of seconds. If the On/Off button turns blue that's great – you're connected!

Now is a great time to take a look at the [VPN Tracker Manual](#). It shows you how to use your VPN and how to get the most out of it.

Troubleshooting

In case there's a problem connecting, a yellow warning triangle will show up.

Click the yellow warning triangle to be taken to the log.

The log will explain exactly what the problem is. Follow the steps listed in the log.

TIP: Press Cmd-L to open the log in a new window. That way, you can have the log side-by-side with your VPN configuration while making changes to troubleshoot a problem

VPN Tracker Manual

The [VPN Tracker Manual](http://www.vpntracker.com/support) contains detailed troubleshooting advice. Answers to frequently asked questions (FAQs) can be found at: <http://www.vpntracker.com/support>

Technical Support

If you're stuck, the technical support team at equinix is here to help. Contact us via <http://www.vpntracker.com/support>

Please include the following information with any request for support:

- A description of the problem and any troubleshooting steps that you have already taken.
- A VPN Tracker Technical Support Report (Log > Technical Support Report).
- Device model and the firmware version running on it.
- Screenshots of the VPN settings on your VPN gateway.

IMPORTANT: A Technical Support Report contains the settings and logs necessary for resolving technical problems. Confidential information (e.g. passwords, private keys for certificates) is not included in a Technical Support Report.