

VPN Tracker 365

User Manual



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

Under copyright law, this manual 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 manual is accurate. equinix is not responsible for printing or clerical errors.

Last revision: July 2021

www.equinix.com

Contents

Introducing VPN Tracker 365	7	Troubleshooting	51
VPN Tracker 365 Plans	9	Missing Settings	51
Installing VPN Tracker 365	10	Connection Errors	51
VPN Tracker 365 Crash Course	12	No Access to the Remote Network	53
Setting up VPN Tracker 365	14	Troubleshooting Remote DNS	55
Connecting to Your New VPN	20	Managing Your VPN Tracker 365 Plan	57
How to connect	20	my.vpntracker.com	57
VPN Shortcuts	21	VPN Tracker 365 for Teams	58
Managing your Connections	23	Creating a VPN Tracker 365 Team	58
Personal Safe	28	VPN Tracker 365 Plans for Teams	58
Saving a VPN Connection in Your Personal Safe	29	Managing VPN Tracker Teams	59
Backing up VPN Shortcuts in Your Personal Safe	30	Enterprise Rollout	60
Managing your Personal Safe	30	TeamCloud	62
Connection Checker	31		
Network Scanner	34		
Accounting	38		
InfiniConnect	40		
Exporting Connections	43		

Introducing VPN Tracker 365

Welcome to VPN Tracker, the leading VPN client on Mac. Whether you are new to VPN or a seasoned VPN guru, this manual will help you get started with VPN Tracker.

Quick Links

New to VPN Tracker?

- Install VPN Tracker and start your free demo in our [→ Installation Guide](#)
- Learn more about VPN Tracker 365 in our [→ VPN Tracker 365 Crash Course](#)

System Administrators and IT Departments

- Learn more about Team Management and other team features in [→ VPN Tracker 365 for Teams](#)

Need Help?

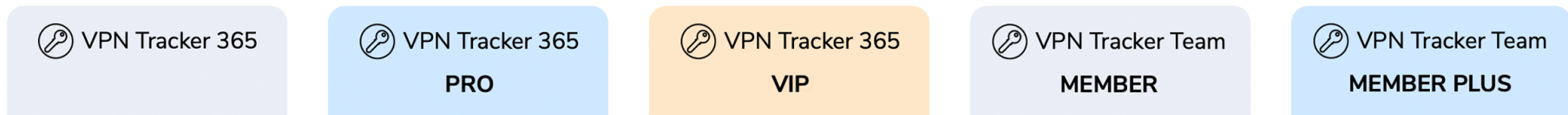
- Get step-by-step advice in our [→ Troubleshooting Guide](#)
- Looking for guidance on using a certain feature or setting in the app? Please refer to the [→ Contents Section](#) of this Manual
- Need to chat to a VPN Tracker expert? Contact our experienced [→ Support Team](#)

Further Resources

- Looking to find the right VPN Tracker 365 plan? Take a look at our [→ Buyer's Guide](#)
- Questions about a specific device or protocol? Refer to our [→ Compatibility Guides](#) for device- or protocol-specific setup instructions
- General questions about VPN Tracker 365? Browse our extensive list of [→ Frequently Asked Questions](#)

VPN Tracker 365 Plans

We offer five different VPN Tracker 365 plan tiers to fit your requirements:



Which plan is right for me?

VPN Tracker 365 Standard: For solo users with basic VPN needs

VPN Tracker 365 Pro: For solo users with advanced VPN needs or admins of smaller teams

VPN Tracker 365 VIP: For admins of larger teams or consultants with advanced VPN needs

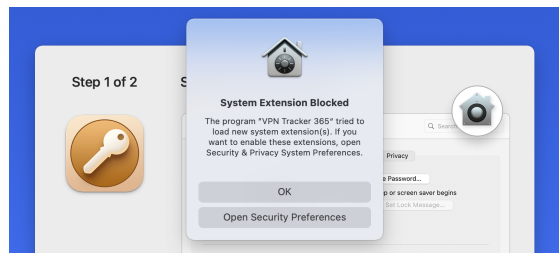
VPN Tracker 365 Team Member and **Team Member Plus** plans are designed to be exclusively used with [→ TeamCloud](#) and users can't configure their own connections - great for teams with many end-users.

Check out our [Buyer's Guide](#) for a full overview of what each plan type offers.

Tip: Regardless of the plan you have purchased, you can always download and use the same copy of the VPN Tracker application. Your license will automatically unlock all the features included in your plan.

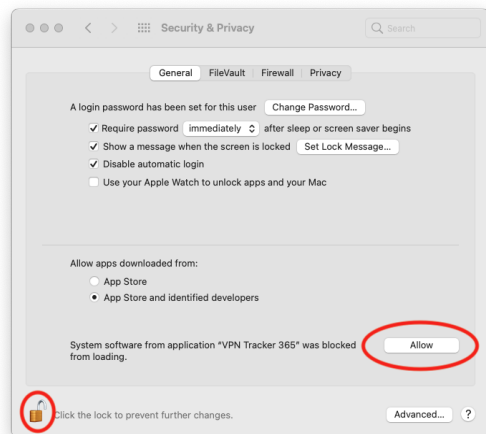
Installing VPN Tracker 365

You can always [download the latest version of VPN Tracker 365](#) from the VPN Tracker 365 website. Once downloaded, move VPN Tracker 365 to your Applications folder.

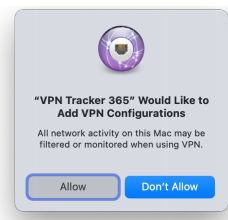


When you first launch VPN Tracker 365 on your Mac, you will be prompted to install the VPN Engine and authorize the System Extensions that lets VPN Tracker's VPN Engine access network packets and do its thing.

This step needs to be done on your Mac with VPN Tracker in your Applications folder and can't be carried out remotely (i.e. via Remote Desktop.)



In the next step, you'll be prompted to open System Preferences → Security & Privacy. Here you need to "Allow" VPN Tracker 365's System Extension.



Finally, you will also need to allow VPN Tracker 365 to add VPN configurations.

Note for Admins: For Enterprise rollouts via MDM, you can also pre-approve the VPN Tracker Kernel Extension using a special profile → [Learn more](#).

Your VPN Tracker 365 account

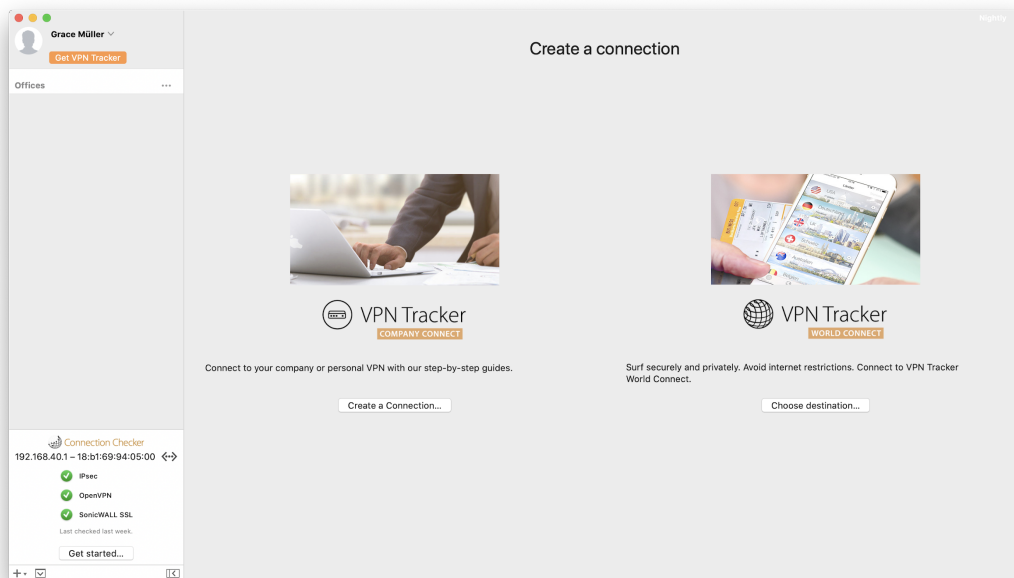
Accessing your VPN Tracker 365 account is quick and easy. You can start using your plan in a few seconds over any internet connection.

How many plans do I need?

VPN Tracker 365 is licensed per-user, so each user that wants to use VPN Tracker needs their own plan.

Testing VPN Tracker

If you want to make sure VPN Tracker 365 works with your connection and meets your expectations before purchasing, you can test the demo version for free. This will give you access to all VPN Tracker Pro features (except exporting connections). All you need to do to get started is create a free account:



Tip: If you set up your VPN connection during your free demo period, VPN Tracker 365 will keep all your settings and details once you purchase a license.

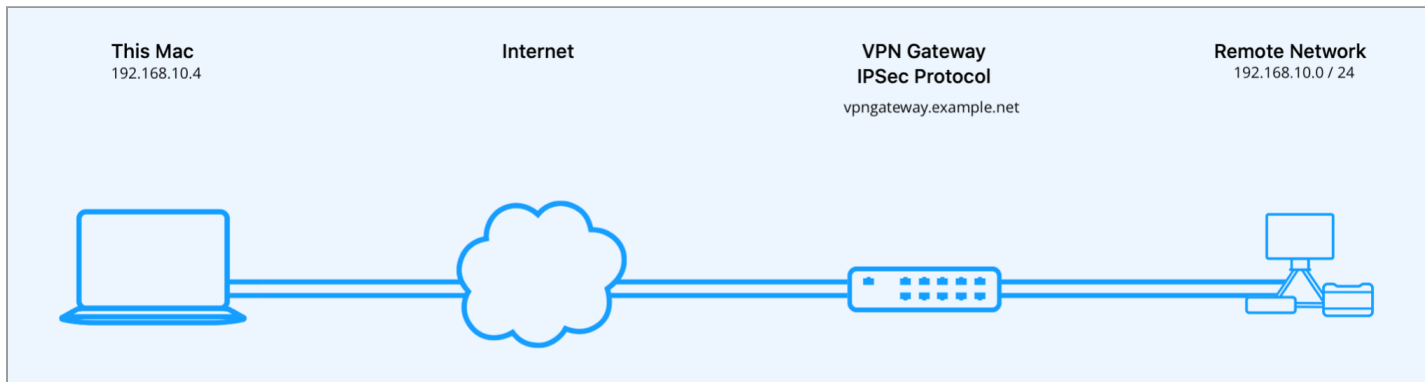
To purchase a license: Visit vpntracker.com/buy

VPN Tracker 365 Crash Course

Is this your first time working with a VPN? Read this chapter to get you up to speed.

What is VPN Tracker 365?

VPN Tracker 365 is the leading VPN client for macOS and allows your Mac to securely connect to a remote network over the Internet. Even if your office is located in San Francisco and you're on a business trip in New York, you can work with your applications and files, as if you were in your office.



How does VPN Tracker 365 work?

As the name implies, VPN Tracker 365 uses VPN (Virtual Private Network) technology to create a connection between your Mac and your remote network. And unlike normal Internet connections, a VPN Tracker connection is encrypted. Think of a VPN as a highly-secure tunnel through the Internet, your very own "secure line" to your office.

In order to use a VPN, you'll need your Mac running VPN Tracker on your end of the connection. On the other end of the connection (the remote side), you need a VPN gateway that accepts your incoming VPN connection.

Once you have set up your connection in VPN Tracker and on the device at your remote location, you are ready to connect and start working remotely using your normal tools and applications.

What do I need to get started?

To create a VPN connection from your Mac, you need three things:

- A VPN Tracker 365 plan
- An Internet connection
- A VPN gateway

About VPN Gateways

A VPN gateway is a hardware device (or in some cases specialized software running on a regular computer) that accepts incoming VPN connections, creating a secure tunnel between its local network and your Mac. In most cases, a VPN firewall or a router with built-in VPN capabilities will act as the VPN gateway.

If there are existing VPN users in your organization you probably already have a properly configured VPN gateway. If not, don't worry – check out [this blog post](#) for some tips on what to look for when buying a VPN gateway.

What kind of VPN connections does VPN Tracker support?

VPN Tracker 365 supports all industry standard VPN protocols:

- IPSec
- OpenVPN
- L2TP
- PPTP
- SonicWALL SSL
- Fortinet SSL
- Windows SSTP
- Cisco EasyVPN
- Sophos SSL

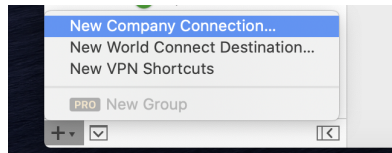
Please refer to the [Buyer's Guide](#) for more information on which protocols are supported in which plans.

Want to configure a VPN connection on your VPN gateway? Our [configuration guides](#) can help you get started with setting up a connection for your chosen VPN protocol.

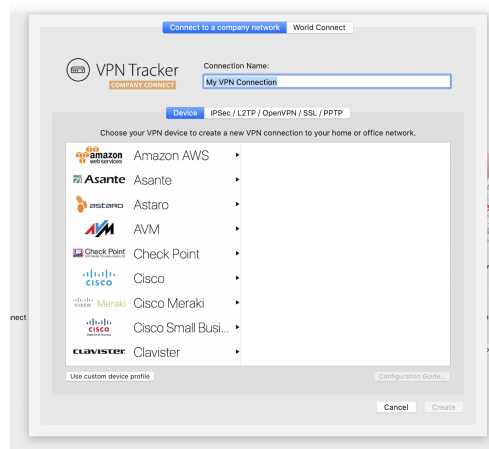
Setting up VPN Tracker 365

Add a New Connection

- Click the button in the lower left hand corner of the VPN Tracker 365 window and select “New Company Connection...”



You will see a list of device profiles. We have device profiles for all the VPN gateways that VPN Tracker has been tested with:



- Select your VPN gateway from the list. If your VPN gateway is not listed, click the button “Use custom device profile”.
- Click “Create” to add the new connection

Basic Settings

Let's take a closer look at the essential settings that VPN Tracker 365 needs to connect to your VPN gateway. Depending on your device, some settings may not be shown.

Connection Icon

Customize the icon by dragging an image onto the default icon, or choose "Edit > Choose Image..." for a new icon.

Device Profile

Click to change the device profile.

VPN Gateway

Enter the public IP address or host name of your VPN gateway, e.g 203.0.113.48 or vpn.example.com

Authentication

Choose whether to use a pre-shared key, certificates or hybrid mode for authentication. Most VPN gateways use pre-shared keys.

Identifiers

Select the type and enter the local and remote identifiers.

Note: The identifiers need to be entered in reverse, e.g. "local" in VPN Tracker is what is configured as "remote" on your VPN gateway.

The screenshot shows the 'NETGEAR VPN' configuration page. At the top, there are tabs for 'Basic', 'Advanced', 'Actions', and 'Notes'. The main content area is divided into several sections: 'Connection Name' (NETGEAR VPN), 'Device Profile' (NETGEAR FVG318), 'VPN Gateway' (Host Name or IP Address), 'Network Configuration' (Protocol: IKEv1, Topology: Host to Network, Local Address: IP Address, Remote Networks: Network Address), 'Authentication' (Pre-shared key), 'Identifiers' (Local: Fully Qualified Domain Name (FQDN), Remote: Fully Qualified Domain Name (FQDN)), and 'DNS' (Use Remote DNS Server). At the bottom, there are buttons for 'Manage Team & Plans...', 'Export Settings...', and 'Export...'. A 'Nightly Done' button is in the top right corner.

Connection Name

Click to change the name of your connection.

Configuration Guide

Click to access the device-specific configuration guide.

Network Configuration

Select manual configuration or one of the automatic configuration options (not available on all devices).

Extended Authentication

VPN Tracker will prompt you for username and password if your VPN gateway requests Extended Authentication (XAUTH).

DNS

VPN Tracker can use a DNS server on the remote network over VPN. It is not necessary to configure remote DNS right away, you can always do so later.

Team Options

Takes you to my.vpntracker.com where you can manage your team's settings.

Export Options

Export your connection to share with team members or colleagues.

Remote Networks

Networks or addresses can be entered into VPN Tracker 365 using the following formats:

- As a single IP address, e.g. 192.168.10.4
- As a single remote network, e.g. 192.168.10.0
- In CIDR notation, e.g. 192.168.10.0 / 24
- With the full subnet, e.g. 192.168.10.0 / 255.255.255.0

Advanced Settings

Your connection settings depend fully on the protocol and device you choose.

In this section, you will find a brief overview of some of the advanced settings that can be configured in VPN Tracker 365. For more information on a specific setting or configuration option, please refer to the FAQ area of the VPN Tracker website, or get in touch with our support engineers.

Encryption Settings (IPsec & OpenVPN)

You likely won't have to modify your encryption settings. However, in some cases, you may need to. For example:

- Your device uses different settings than the factory defaults and/or the settings proposed in the configuration guide, or
- There is no device profile for your device in VPN Tracker

In both cases, the goal is to have VPN Tracker's encryption settings match **exactly** what is set up on your VPN gateway.

The screenshot displays the 'Advanced' settings for a VPN connection named 'Head Office'. The interface is divided into several sections:

- Traffic Control:** Includes a dropdown menu set to 'Always exempt the addresses below from VPN' and a checkbox for 'Force traffic over the VPN if remote networks conflict with local networks'.
- NAT-Traversal:** Set to 'Automatic'.
- Connection Timeout:** Set to '30 seconds'.
- Interoperability:** Contains three checked options: 'Send keep-alive ping every 10 seconds', 'Send INITIAL-CONTACT message', and 'Perform active Dead Peer Detection every 10 seconds if necessary'.
- IPv6:** Includes an unchecked option 'Prefer IPv6 VPN gateway address, if available'.
- Additional Settings:**
 - Direct Link Detection:** Set to 'MAC Address of Remote Network's Router'.
 - MTU:** Includes an unchecked option 'Set MTU for network used by VPN: 1280 bytes'.
 - Credentials:** Includes an unchecked option 'Display credentials prompt for 30 seconds' and three checked options: 'Always prompt for pre-shared key', 'Always prompt for XAUTH credentials', and 'Use stored XAUTH password as passcode'.
 - Delete Payloads:** Includes a checked option 'Cache XAUTH credentials until VPN is disconnected' and an unchecked option 'Treat delete payload in phase 2 as error'.

At the bottom of the settings panel, there are buttons for 'Manage Team & Plans...', 'Export Settings...', 'Export...', and 'Share with Team...'. On the left side of the interface, there is a sidebar with 'My Connections' (listing 'Head Office', 'Berlin Office', and 'London Office') and a 'Traffic' tab showing network statistics and a graph.

Traffic Control

Traffic Control features in VPN Tracker 365 allow you to determine how and where your VPN traffic is routed. With this option you can:

- Select certain networks or addresses that should be exempt from the VPN
- Select certain networks or addresses for which traffic should be sent over the VPN

Networks or addresses can be entered into VPN Tracker 365 using the formats listed in the [→ Remote Networks](#) section.

If you need to add more networks, simply click on the green plus icon to the left of the configuration window. Alternatively, to remove a network or address, just click on the red minus icon.

The screenshot displays the VPN Tracker 365 interface for a user named Grace Müller. The main window is titled 'London Office' and shows the 'Advanced' settings tab. The 'Traffic Control' section is highlighted, showing a dropdown menu set to 'Always exempt the addresses below from VPN'. Below this, two IP addresses are listed: '192.168.10.0 / 24' and '192.168.40.0 / 24'. A checkbox labeled 'Force traffic over the VPN if remote networks conflict with local networks' is checked. Other settings include 'Connection Timeout' set to 20 seconds, 'Interoperability' with 'Perform active Dead Peer Detection every 20 seconds if necessary' checked, and 'IPv6' with 'Prefer IPv6 VPN gateway address, if available' unchecked. The 'Additional Settings' section shows 'Direct Link Detection' set to 'Use Current Router'. A sidebar on the left shows 'My Personal Connections' with 'London Office' selected, and a traffic control icon circled in red with a plus and minus sign. A red arrow points from this icon to the 'Traffic Control' section.

Force traffic over the VPN: You can check this option if your local and remote network(s) overlap and VPN Tracker will attempt to send non-essential local traffic over the VPN.

Please note that even when this option is checked, you will never be able to reach the IP address of your local router, your DHCP server, and your DNS server(s) over VPN.

If you need to reach those IPs over VPN, you will have to manually resolve the network conflict instead of using Traffic Control.

[→ Learn more.](#)

Completing Setup

When you're finished configuring your VPN, click **Done** in the upper right corner to leave edit mode.

Tip: It is **not** necessary to leave edit mode to save the connection or to connect to the VPN. If you make changes while the VPN is connected, reconnect the VPN to apply them.

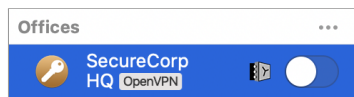
Now that you have a basic idea of how to set up a connection in VPN Tracker 365, you're ready to apply it to your specific situation.

Connecting to Your New VPN

When you're done setting up your VPN, you're ready to connect. To test your VPN, go to a location outside of the network that you want to connect to.

How to connect

Click the on/off slider to connect the VPN:



If you are using VPN Tracker 365 for the first time with your current Internet connection, [Connection Checker](#) will test your connection. Wait for the test to complete.

If prompted, you will need to enter your pre-shared key and Extended Authentication (XAUTH) username and password to get connected. Save these in your Keychain to save entering them every time you connect.

Connected?

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

Continue with the next chapters to find out how to use VPN Tracker 365 and your VPN connection effectively.

Problems?

If there is a problem connecting, VPN Tracker 365 will give you helpful advice and troubleshooting tips. To learn more about this, visit the chapter [→ Troubleshooting](#)

VPN Shortcuts

Shortcuts give you one-click access to the files, documents and applications you need to do your work over your VPN connections.

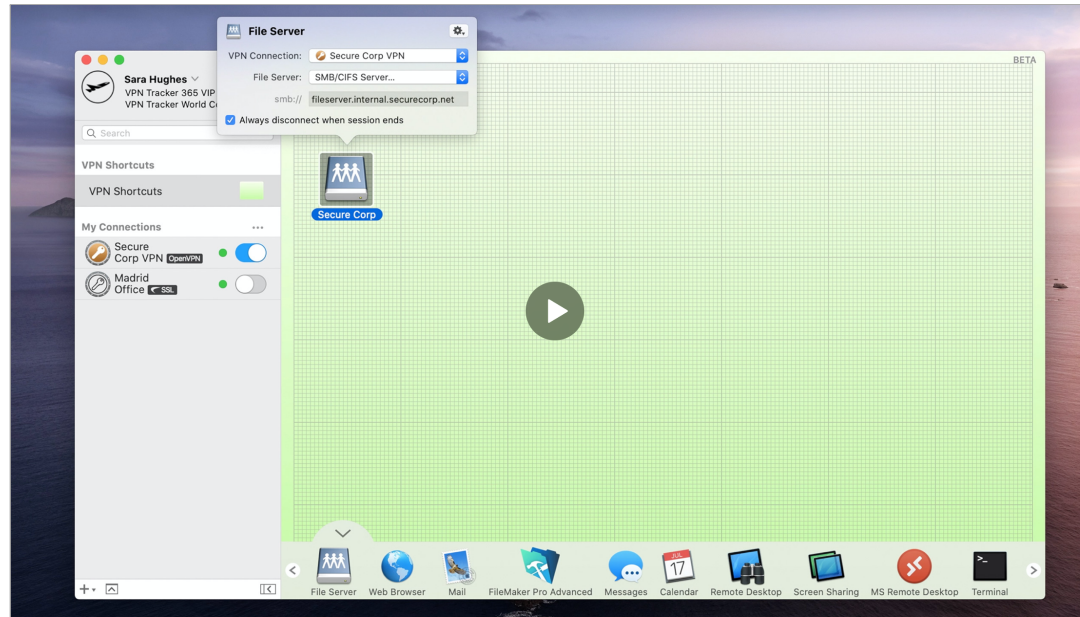
Setting up Shortcuts

This video tutorial shows you how to quickly set up VPN Shortcuts in VPN Tracker 365 and save them in your Personal Safe.



Connecting to a File Server

This video shows you how to easily access file servers over VPN using Shortcuts:

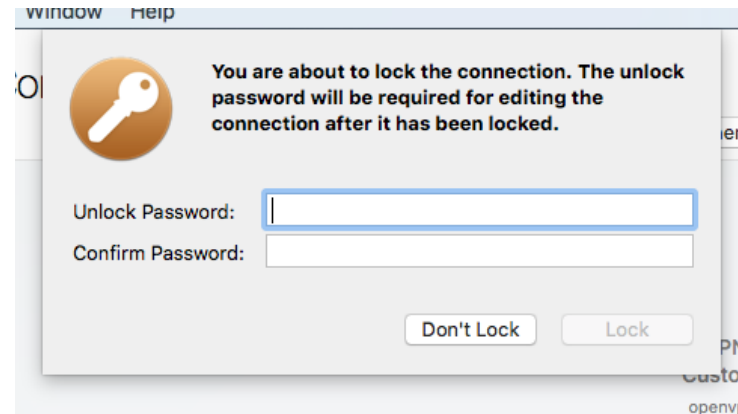
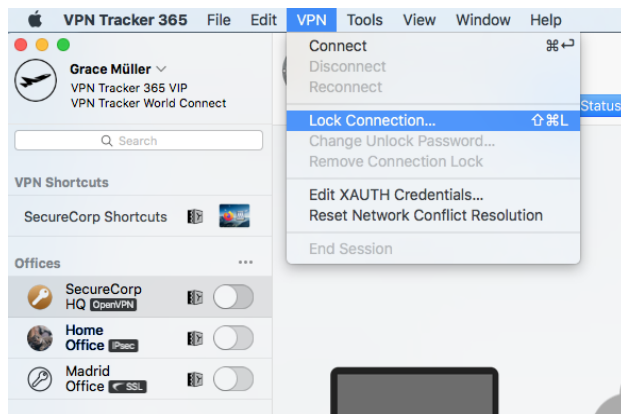


Managing your Connections

VPN Tracker 365 offers many ways to manage your connections and personalize your workflows to suit your needs.

Locking Connections

You can lock a connection to prevent it from being modified (VPN > Lock Connection...). During this step, you will be asked to enter an unlock password which will need to be entered should you or another user need to make changes in the future:



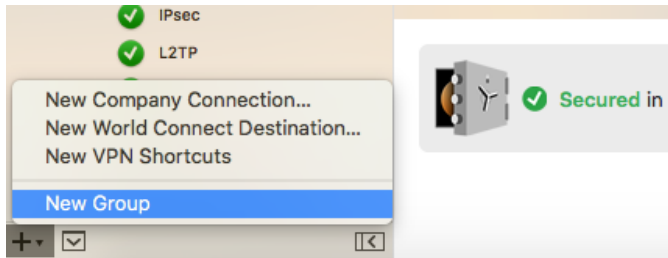
To prevent others from modifying connections you export for them, enable locking in the export settings.

Organizing Connections in Groups

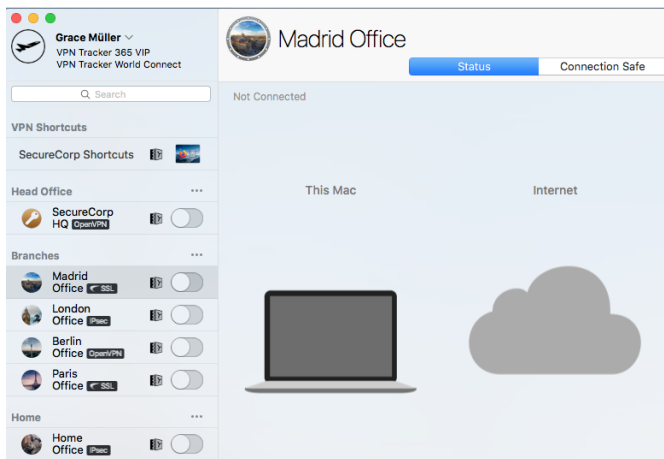
PRO **VIP**

If you have a lot of connections, it will be useful to divide your connections up into groups, e.g. by client, by branch office, by geographical location etc.

To add a new group, click the '+' icon in the lower left hand corner of the window and select 'New Group':



You can drag & drop connections and VPN Shortcuts Collections between groups to rearrange them:



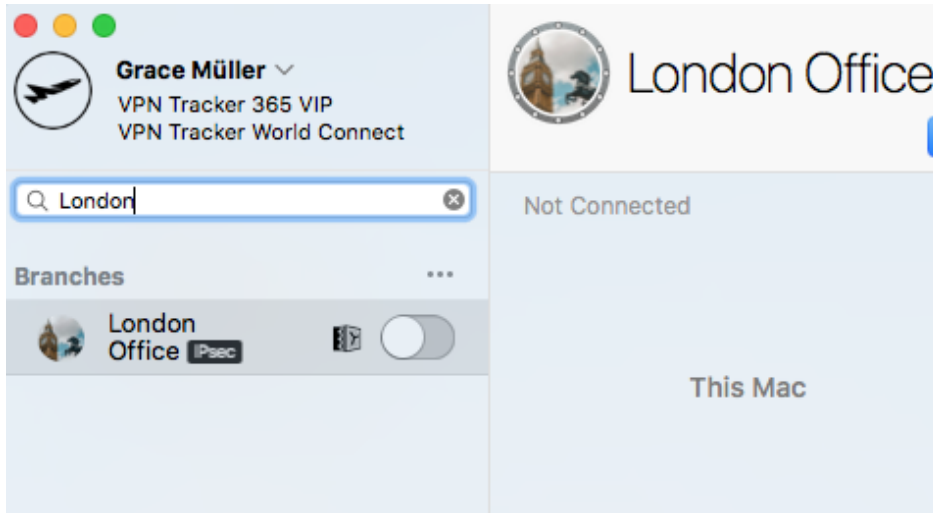
To rename, delete or control a group of connections, use the gear menu on the right side of the group.

Tip: An exported connection knows the group it belongs to, and will recreate it as needed.

Searching Connections

PRO **VIP**

If you are a consultant or admin looking for a specific connection, use the search box at the top of the sidebar to find it:



VPN Connection Stats

When connected to your VPN, you can see statistics for your connection in the sidebar.

The traffic graph lets you know how much data is currently being sent and received over your VPN connection, as well as the total amounts of data transferred, and the maximum throughput seen in the last measurement period.

It also lists the algorithms that are in use and the current network settings.



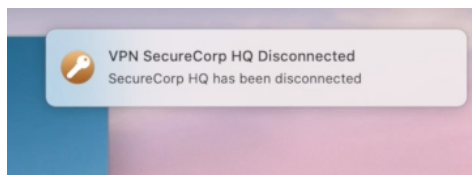
Menu Bar Item

You can also control VPN Tracker 365 directly from your menu bar, allowing you full control over your VPN connection, without having to leave the application you're working in.

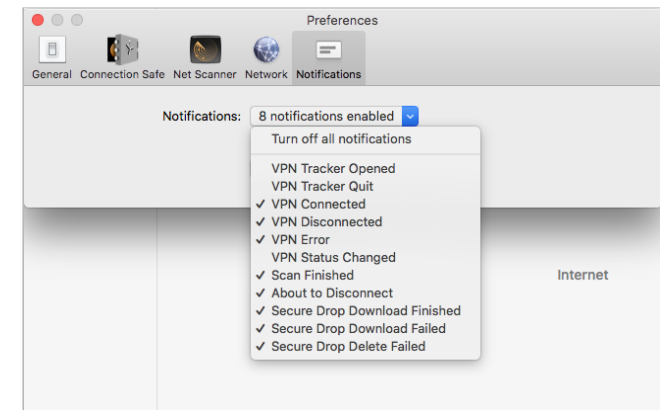


App Notifications

VPN Tracker 365 shows push notifications whenever something interesting happens to your VPN:

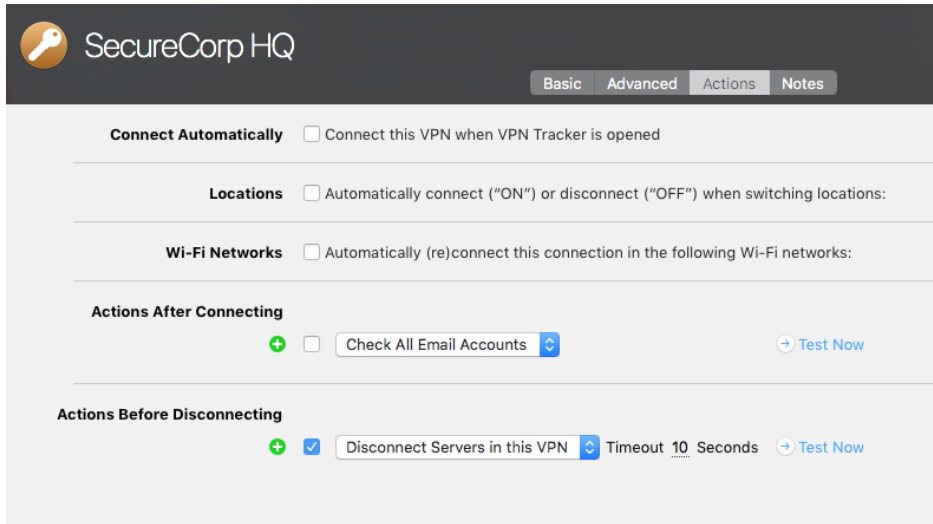


You may customize these notifications in "VPN Tracker 365" > "Preferences" > "Notifications".



Connection Actions

You can configure your VPN connection to carry out certain actions on launch. To get started, go to a connection, click “Configure” and go to “Actions”:



The screenshot shows the configuration interface for a VPN connection named "SecureCorp HQ". The interface has a dark header with the company logo and name. Below the header, there are four tabs: "Basic", "Advanced", "Actions", and "Notes". The "Actions" tab is currently selected. The main content area is divided into several sections:

- Connect Automatically:** A checkbox labeled "Connect this VPN when VPN Tracker is opened" is currently unchecked.
- Locations:** A checkbox labeled "Automatically connect ('ON') or disconnect ('OFF') when switching locations:" is currently unchecked.
- Wi-Fi Networks:** A checkbox labeled "Automatically (re)connect this connection in the following Wi-Fi networks:" is currently unchecked.
- Actions After Connecting:** A section with a green plus icon and an unchecked checkbox. It contains a dropdown menu with "Check All Email Accounts" selected and a "Test Now" button.
- Actions Before Disconnecting:** A section with a green plus icon and a checked checkbox. It contains a dropdown menu with "Disconnect Servers in this VPN" selected, a "Timeout 10 Seconds" field, and a "Test Now" button.

Connect this VPN when VPN Tracker is opened

Enable this option to automatically connect to this VPN whenever VPN Tracker is opened.

Locations

If you use multiple network locations on your Mac (System Preferences > Network), VPN Tracker can automatically connect or disconnect your VPN connection, depending on the current network location.

- Switch the slider to “On” to automatically connect in this location
- Switch the slider to “Off” to automatically disconnect in this location

Wi-Fi Networks

With this action, VPN Tracker 365 will automatically connect to your VPN whenever your Mac connects to the wireless networks you have specified.

Actions After Connecting

VPN Tracker 365 can take care of any tasks that need to be performed after the VPN connects.

For example, if you always need to connect to a file server, enter it here to make sure it's available any time you connect the VPN. Or, if you want to open your company's intranet website whenever you connect, enter it here.

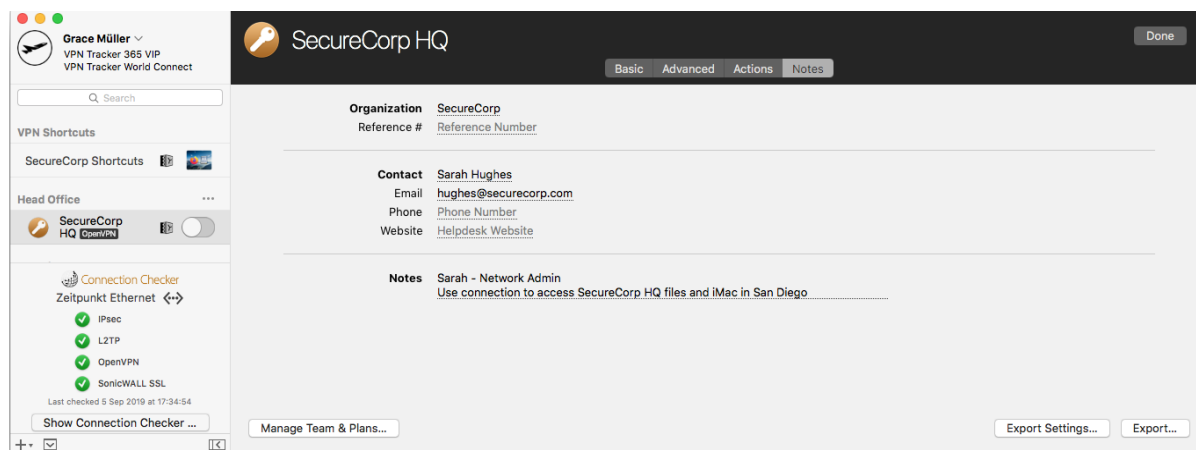
Tip: Actions can help you to be even more productive with VPN Shortcuts. For example, if you have certain applications in your VPN Shortcuts Collection that require a file server to be connected, add that file server here to ensure that it's always available to your VPN Shortcuts items.

Actions Before Disconnecting

If there's anything that needs to be done before the VPN is disconnected, add it here. VPN Tracker 365 automatically adds an action to disconnect all file servers that use the VPN.

Notes

If you would like to make a few notes – for yourself, or for others that you're setting up this VPN for, the Notes tab is the right place:



- Notes are included with exported connections
- When exporting Accounting records, the reference number and organization can be included for use with billing systems
- All information from the Notes tab is displayed on the Status tab

Personal Safe

What is Personal Safe? Use your VPN Tracker 365 Personal Safe to keep your personal VPN connections safe and backed-up. Using state-of-the-art cryptography, your Personal Safe uses secure encryption to tie your connection to your personal equinix ID, so only you can access your connections.

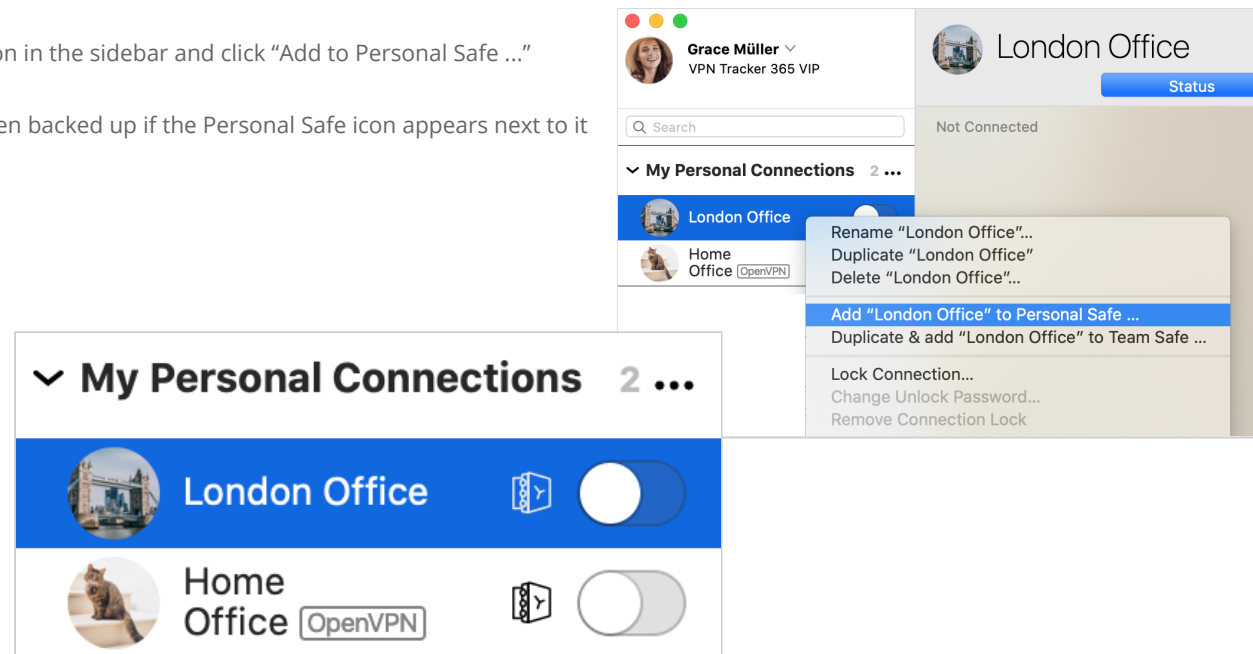
Interested? Visit the VPN Tracker 365 website to [learn more about Personal Safe](#).

Saving a VPN Connection in Your Personal Safe

Once you have set up a VPN connection in VPN Tracker 365, it is best practice to back the connection up in your Personal Safe. This way, you will not have to configure the connection again if you get a new Mac.

To save a connection, right click on the connection in the sidebar and click "Add to Personal Safe ..."

You can see whether or not a connection has been backed up if the Personal Safe icon appears next to it in the sidebar.



Backing up VPN Shortcuts in Your Personal Safe

As well as VPN connections, with a VPN Tracker 365 Pro or VIP plan, you can also save → [VPN Shortcuts](#) to your Personal Safe. This allows you easy access to all your most-used VPN workflows wherever you are working and means you don't have to configure new Shortcuts if you get a new Mac.

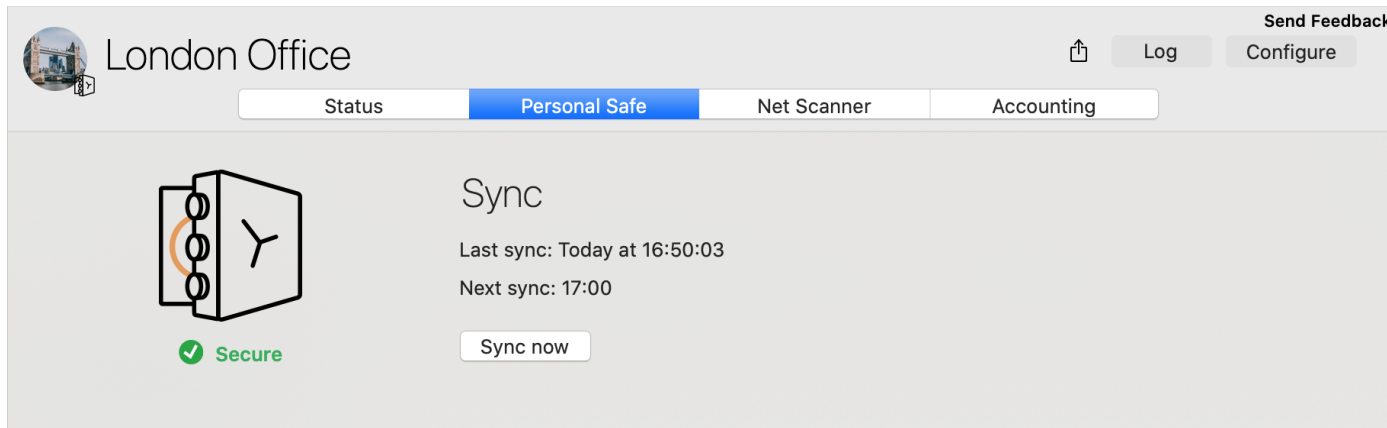
Examples of how you can utilise personal VPN Shortcuts:

- Accessing your home desktop remotely
- Checking your email account on the go
- Accessing private files via an external file server

Just as described above for saving connections, to add a Shortcuts Collection to your Personal Safe, right click on the collection and click "Add to Personal Safe ..."

Managing your Personal Safe

You can view the status of a particular connection by opening the Personal Safe tab:



Here you can add or remove connections and also sync your connection if you have made any changes.

Tip: VPN Tracker 365 will automatically sync with your Personal Safe every 10 minutes.

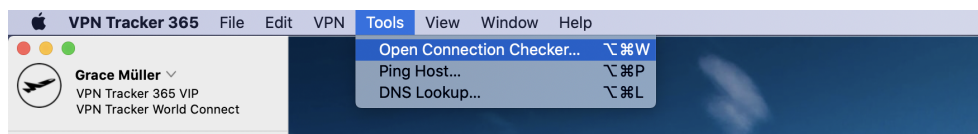
Connection Checker

What is Connection Checker? Connection Checker automatically tests new network environments, figures out which VPN standards are supported and optimizes your connection. Connection Checker quickly connects to VPN Tracker 365 servers and determines which settings to use for successful VPN connections.

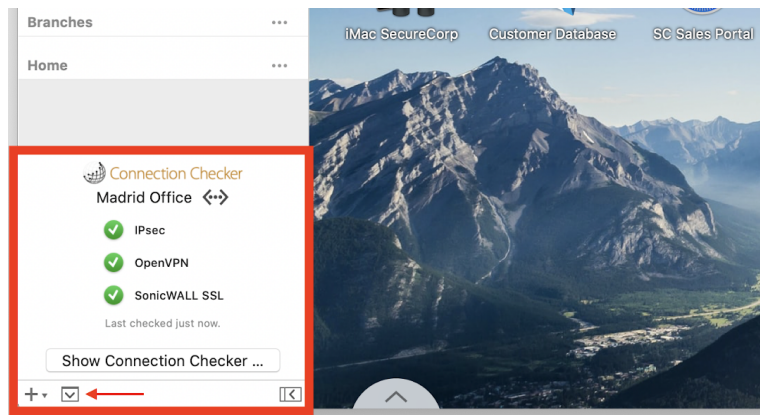
Visit the VPN Tracker website to [learn more about Connection Checker](#).

Accessing the Connection Checker

To open the Connection Checker, go to the “Tools” menu and click “Open Connection Checker”:



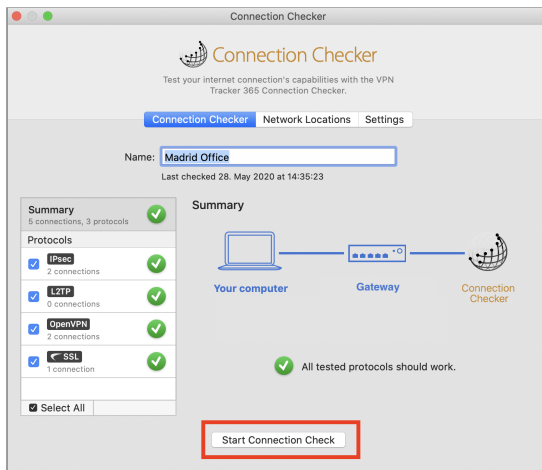
Alternatively, you can open and collapse the Connection Checker widget by clicking on the icon in the bottom left corner of the app window:



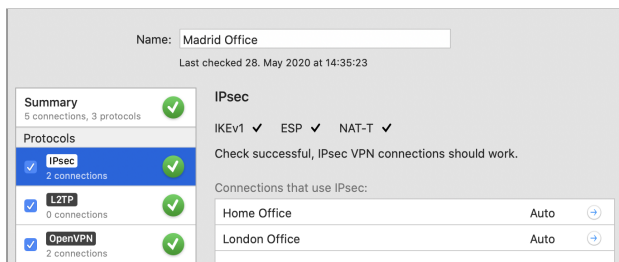
Performing a Connection Check

If you are experiencing difficulties with your internet connection or connecting to a new network for the first time (e.g. at a hotel or cafe), performing a connection check is the best way to diagnose any network issues and determine whether the VPN protocol you need is supported.

Once you have the Connection Checker open, you will see your current network and a list of VPN protocols. Check the box next to the protocols you want to test, or check "Select All" if you want a general overview. Click "Start Connection Check" to test the connection and identify which of the selected VPN protocols are supported.

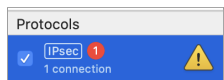


Under each protocol, you will see how many of your saved VPN connections use this protocol. Click on a protocol for more specific detail:



Troubleshooting unsupported protocols

VPN protocols which aren't supported are indicated by a yellow warning icon:



Tracking network locations

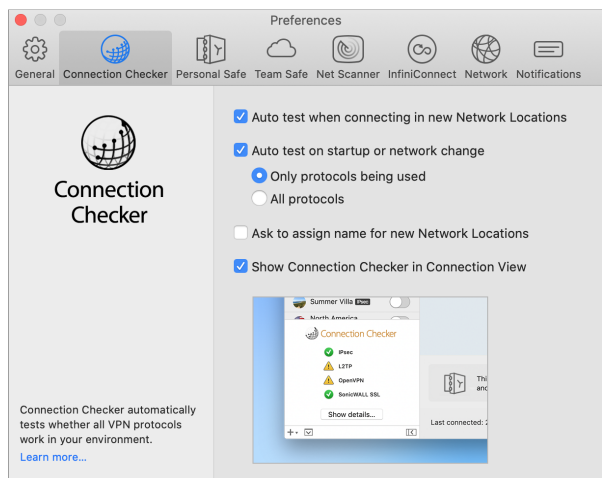
PRO **VIP**

The "Network Locations" tab in the Connection Checker window is a useful reference to help you keep track of all your previously tested networks and their test results.



Adjusting your Connection Checker settings

You can configure Connection Checker in the VPN Tracker 365 Preferences under the Connection Checker tab. Activating options such as "Auto test when connecting in new Network Locations" make your VPN workflow much easier.



Network Scanner

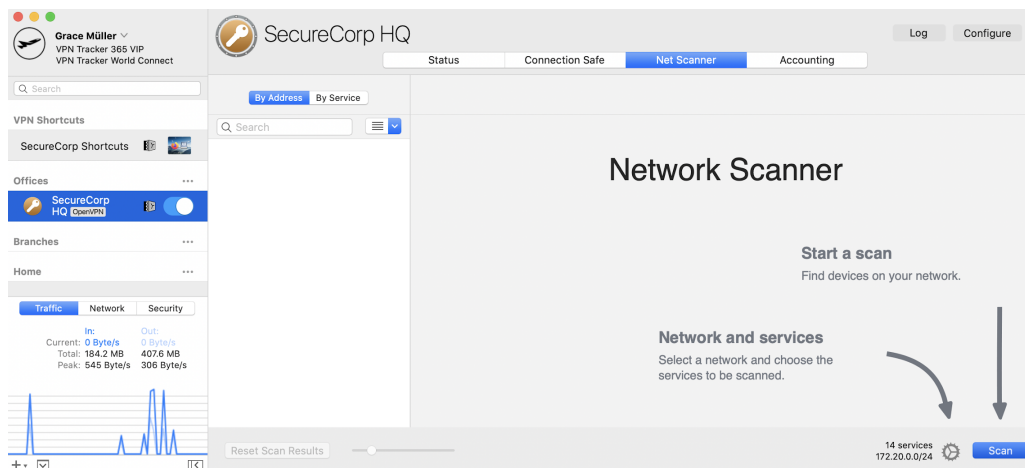
PRO **VIP**

The Network Scanner in VPN Tracker 365 Pro lets you explore the remote network of your VPN, assist users and easily locate available hosts and services.

Scanning Networks

To scan a network, your Mac must be connected to the network via VPN.

- Select the VPN connection in the sidebar and start the connection.
- Go to the “Net Scanner” tab.
- Click the “Scan” button in the bottom right corner to scan the network using a selection of the most popular network services:



If you are connected to a VPN where all network traffic is sent through the VPN (Host to Everywhere), VPN Tracker 365 will ask you to specify the network that you would like to scan.

Depending on the size of the network and your Internet connection, the scan may take a while to complete. You can continue working with VPN Tracker 365 while a scan is in progress. You'll receive a notification when the scan is complete.

Customizing Network and Services

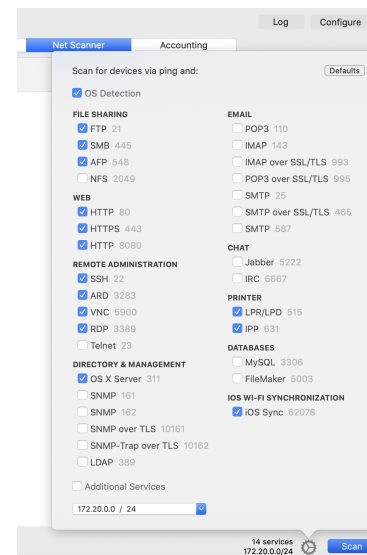
By default, the Network Scanner scans for a selection of the most popular network services.

- To select different services, click the settings icon and check or uncheck the services that you would like VPN Tracker 365 to scan for:
- To turn OS detection* on or off, use the checkbox at the top of the settings.
- To check/uncheck all services, hold down the Option key while clicking a checkbox.
- To restore the default selection of services and networks, click the “Defaults” button at the top of the settings.

***What is OS Detection?** The Network Scanner can detect the type of host (e.g. macOS, Windows, Linux, Network Equipment, Printers) from the services that are available on that host.

- OS detection requires certain services to be included in the scan. If you uncheck a service that is required for OS detection, OS detection will be unchecked as well.

Tip: At the bottom of the settings, you can change the network that is being scanned. Select one of the remote networks of the VPN, or enter a custom range or IP address. The more addresses a scan includes, the longer it will take to complete.



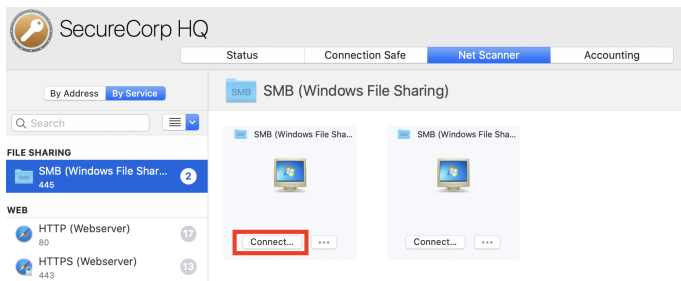
Scan Results

Using Scan Results

Connect to Services

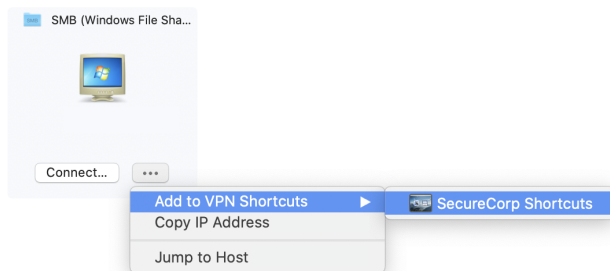
You can connect to a service right from the Network Scanner, or open the app associated with this service on your Mac.

- Display the scan results "By Address" or "By Service".
- On the right side, click the "Connect" or "Open" for the service or host that you would like to connect to:



Add to VPN Shortcuts Collection

- To add a service as VPN Shortcut, click the '...' button for the service that you would like to add to a VPN Shortcuts Collection.
- Choose "Add to VPN Shortcuts" and select the VPN Shortcuts Collection that you want the service to be added to:

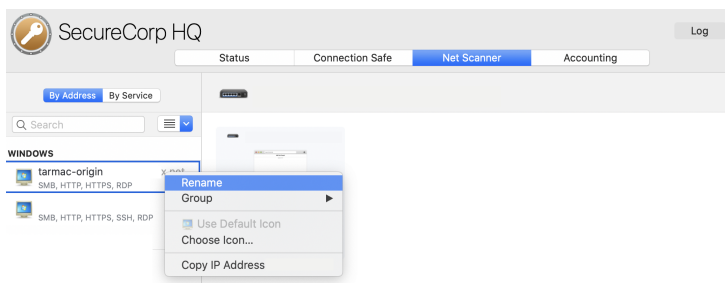


Customizing Scan Results

Renaming Hosts

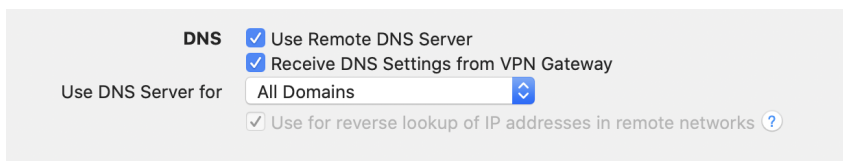
Renaming hosts in the Network Scanner list makes it easy to locate your most important computers and network devices:

- Display the scan results "By Address".
- Right click the host you want to rename.
- Choose "Rename" and enter a name:



Automatic Hostname Lookup

VPN Tracker 365 can automatically look up the hostnames for IP addresses in the Network Scanner. All you need is a Remote DNS server for your VPN that can provide host names for the IP addresses that are being scanned (reverse DNS lookup). Make sure the checkbox "Use for reverse lookup of IP addresses in remote networks" (Basic > DNS) is checked:



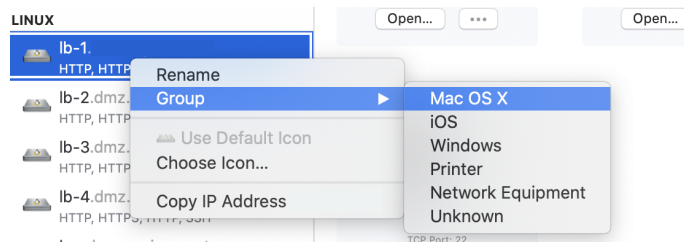
Setting a Custom Icon for a Host

- Display the scan results "By Address".
- Right click the host you want to change the icon for and click "Choose icon..." to set a custom icon for this host.

Change the OS Detection Group

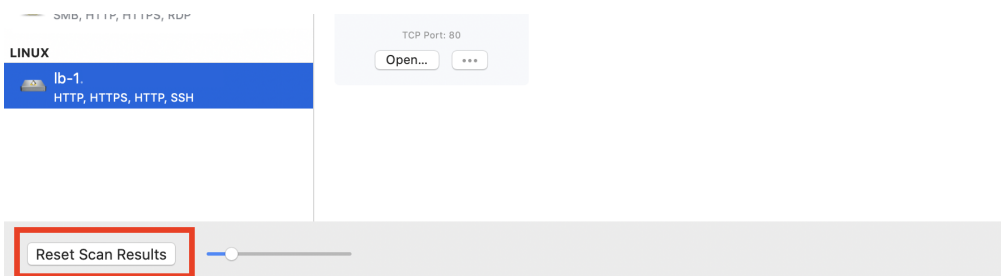
The Network Scanner automatically detects the kind of host – whether it's macOS, Windows or Linux, or a printer or network equipment. OS detection uses the services on a host to determine the most likely type of host. OS detection might put a host into a different group than what it actually is. You can change the group if a host is not detected correctly.

- Display the scan results "By Address"
- Right click the host whose group you want to change.
- Select the new group from the "Group" menu:



Resetting Scan Results

- Click "Reset Scan Results" in order to clear the results. Customized host names, icons, and groups will not be modified – if the host is encountered again in a future scan, the customization will be applied.
- Hold down the Option key while clicking "Reset Scan Results" in order to also reset all customization (names, icons, and groups).



You can configure the Network Scanner's performance and aggressiveness, and manage Web Preview loading by going to "VPN Tracker 365" → "Preferences" → "Net Scanner".

Accounting

PRO **VIP**

If you have a VPN Tracker 365 Pro or VIP plan, you can use the Accounting feature to track the time you were connected to your VPN. It can assist you with billing your clients and documenting your work.

Customize the Display

- To select the month for which data is being displayed, click the back/forward buttons next to the month.
- To select the columns displayed in the Accounting table, right-click the table header and check or uncheck the columns.

		Duration	Rounded	Traffic	
27. May 2020 at 15:08	Wednesday	2 sec	0,25 h	11,13 kB	
27. May 2020 at 15:08	Wednesday	1 min	0,25 h	0,30 MB	
Today at 14:34	Friday	2 h 40 min	2,75 h	581,95 MB	
27. May 2020 at 15:40	Wednesday	2 min	0,25 h	0,60 MB	
27. May 2020 at 15:27	Wednesday	1 min	0,25 h	0,31 MB	
27. May 2020 at 15:21	Wednesday	45 sec	0,25 h	0,30 MB	

Add Comments

You can add a comment for every connection to your client's VPN. This helps you to keep track why you used the connection on this day and also makes billing easier:

		Duration	Rounded	Traffic	In	Out	Comment
Today at 14:34	Friday	2 h 40 min	2,75 h	581,95 MB	192,03 MB	389,92 MB	Updating customer database
27. May 2020 at 15:40	Wednesday	2 min	0,25 h	0,60 MB	0,37 MB	0,23 MB	
27. May 2020 at 15:27	Wednesday	1 min	0,25 h	0,31 MB	0,24 MB	75,32 kB	

Exporting Accounting Data

VPN Tracker 365 Pro not only tracks connection time for you, it also lets you export this data for Numbers or Excel, or to third-party time tracking or billing systems that can import CSV files:

- Click "Export" in the bottom right corner of the "Accounting" tab
- Choose "Export for Numbers..." or "Export for Excel..." depending on with which application you want to use the data with
 - To export data in a customizable CSV format, choose "Custom Export..."

The screenshot shows the 'Accounting' tab in VPN Tracker 365 Pro. An export dialog box is open, allowing the user to export 'Accounting Data - SecureCorp HQ'. The dialog includes fields for 'Tags', 'Where' (Documents), 'Connection' (SecureCorp HQ), and 'Export range' (This Month (May) from 1. 5.2020 to 31. 5.2020). There are 'Cancel' and 'Export' buttons in the dialog. In the background, a table displays connection data with columns for 'Duration', 'Rounded', and 'Traffic'.

	Duration	Rounded	Traffic
27. May 2020 at 15:40	2 sec	0,25 h	11,13
27. May 2020 at 15:27	1 min	0,25 h	0,30
Today at 14:43	2 h 40 min	2,75 h	581,95
27. May 2020 at 15:40	2 min	0,25 h	0,60
27. May 2020 at 15:27	1 min	0,25 h	0,31
27. May 2020 at 15:21	45 sec	0,25 h	0,30
27. May 2020 at 15:17	44 sec	0,25 h	0,49
27. May 2020 at 14:43	23 min	0,50 h	1,42

The export can include data for one or more connections, simply select additional connections from the "Connection" popup.

Reference Number and Organization: To integrate VPN Tracker 365's accounting with your own time tracking or billing system, an organization and a reference number can be set for each of your VPN connections in the "Notes" tab of the configuration window.

InfiniConnect

PRO **VIP**

VPN Tracker 365 InfiniConnect (available in Team Member Plus, Pro & VIP plans) automatically detects connection interruptions and reconnects your VPN, giving you peace of mind to focus on your work.

Accessing InfiniConnect

If you have a VPN Tracker 365 Pro or VIP plan, you can configure InfiniConnect for your most important VPN connections. This helps you stay connected if the VPN connection gets interrupted, for example, if the internet drops out or your network cable becomes dislodged.

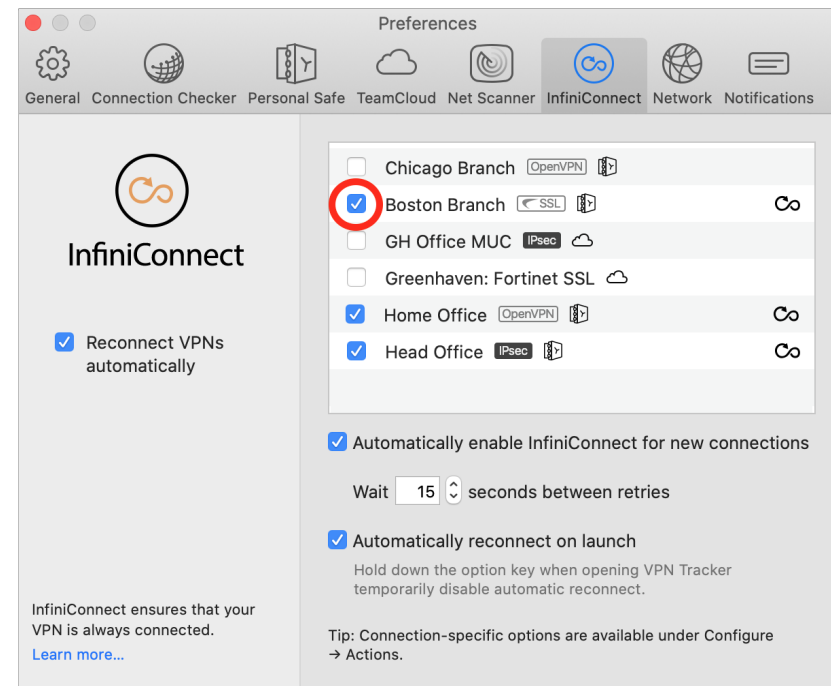
Enable InfiniConnect for a connection

To access your InfiniConnect settings, go to **VPN Tracker 365 > Preferences** and switch to the InfiniConnect tab. Here you will see a list of your current VPN connections. Check the box by a specific connection to enable InfiniConnect for that connection. The InfiniConnect icon indicates whether InfiniConnect is enabled for a particular connection.

InfiniConnect Preferences

In the Preferences window, you can also configure specific options for InfiniConnect, including the amount of time InfiConnect should wait before trying to reconnect and whether InfiniConnect should be automatically enabled for new connections.

Tip: To configure more connection-specific preferences, check the [→ Actions](#) tab.



More Information

Visit the VPN Tracker website to [learn more about InfiniConnect](#) or check out this video to see it in action:



Exporting Connections

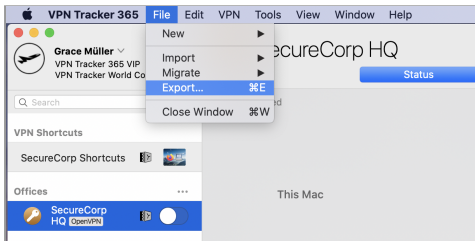
PRO **VIP**

As well as saving your VPN connections and Shortcuts in → [TeamCloud](#) to share with team members, VPN Tracker 365 also gives you the option to export connections and save them locally, should you wish.

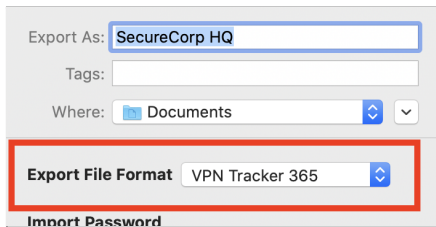
Exporting a Connection

To export a connection

- Select the connection
- Choose “File” > “Export”:



- The export window will now open. If you are exporting a connection for users of previous versions of VPN Tracker 365, be sure to select the appropriate file format from the “Export File Format” menu:



Tip: Not all features are available in previous versions of VPN Tracker. When exporting for earlier versions of VPN Tracker, we recommend testing the exported connection in the respective version before rolling it out to end users.

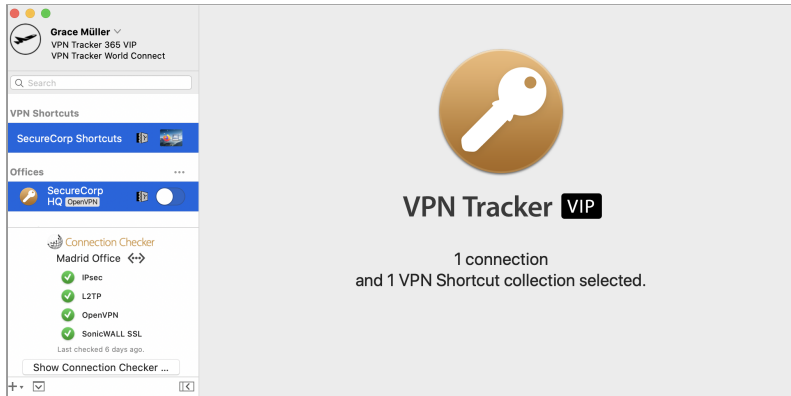
- We recommend you make your export more secure by setting an encryption password for the file. Users of this connection will be required to enter the password once when importing the connection, so be sure to keep a record of the password you choose.

The screenshot shows the 'Export' dialog box in VPN Tracker. It has a light gray background and a white border. At the top, there are three input fields: 'Export As:' with the text 'SecureCorp HQ', 'Tags:' which is empty, and 'Where:' with a dropdown menu showing 'Documents' and a small arrow icon. Below these is the 'Export File Format' section, which has a dropdown menu set to 'VPN Tracker 365'. Underneath is the 'Import Password' section, which includes a short paragraph: 'Exported connections are encrypted. The password will be required to import this connection.' Below the paragraph are two password input fields, both filled with black dots. The first is labeled 'Import password:' and the second is labeled 'Confirm import password:'. At the bottom of the dialog is the 'Remote Connection Wipe' section, which states 'Remote Connection Wipe is not enabled for this'. At the very bottom are two buttons: a white 'Cancel' button and a blue 'Export' button.

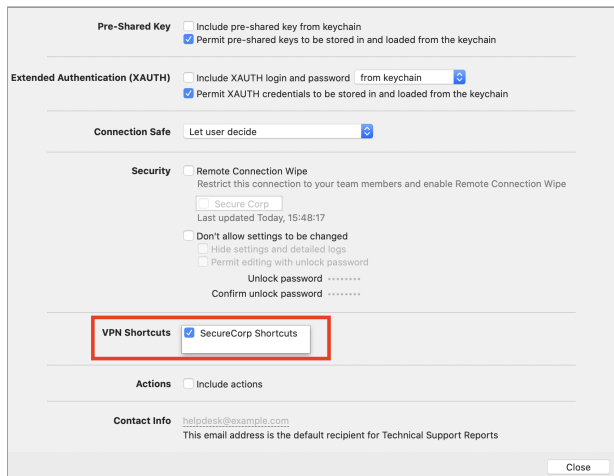
Tip: To export multiple connections in a single file, select the connections you would like to export (hold down the ⌘ key to select more than one), and choose File > Export...

Exporting a VPN Shortcuts Collection

You can also export VPN Shortcuts. When exporting, simply select the Shortcuts Collection in the sidebar along with any VPN connections you wish to export (hold down the ⌘ key to select more than one item in the sidebar):

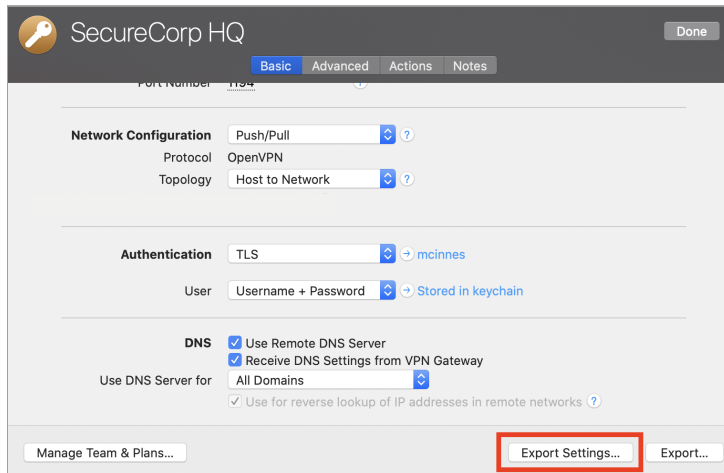


Tip: In the Export Settings, you can choose to automatically export a Shortcuts collection alongside a VPN connection:



Export Settings Explained

VPN Tracker 365 provides admins with a large amount of configuration options when exporting a VPN connection. Access these settings by heading to the “Configure” tab of your connection and clicking “Export Settings” at the bottom of the window:



Pre-Shared Key

- Pre-Shared Key** Include pre-shared key from keychain
The included pre-shared key will be added to the user's keychain.
- Permit pre-shared keys to be stored in and loaded from the keychain


Include pre-shared key from keychain

If you have saved the pre-shared key in your keychain, VPN Tracker 365 can include this pre-shared key with the exported connection.

Permit pre-shared keys to be stored in and loaded from the keychain

Checking this option will (a) move an included pre-shared key into the user's keychain when importing the connection, and (b) permit users to store their pre-shared key in the keychain if none is included with the exported connection.

Extended Authentication (XAUTH)

Extended Authentication (XAUTH) Include XAUTH login and password 

The included XAUTH credentials will be added to the user's keychain.

Permit XAUTH credentials to be stored in and loaded from the keychain

Include XAUTH login and password

If you are using Extended Authentication (XAUTH), you can also include a user's XAUTH credentials (username and password) in the exported connection. Select whether you would like to include the username and password stored in your keychain, or be asked for an XAUTH username and password when exporting the connection.

Permit XAUTH credentials to be stored in and loaded from the keychain

Checking this option will (a) move included XAUTH credentials into the user's keychain when importing the connection, and (b) permit users to store their XAUTH password in the keychain if none is included with the exported connection.

Personal Safe

Personal Safe **Let user decide**

Add to Personal Safe automatically

Prevent adding to Personal Safe

Here you can choose from the options to determine whether or not you want the VPN connection to be stored in the user's Personal Safe.

Security

Security **Remote Connection Wipe**
Restrict this connection to your team members and enable Remote Connection Wipe

Secure Corp
Last updated Today, 16:03:15

Don't allow settings to be changed

Hide settings and detailed logs

Permit editing with unlock password

Unlock password
Confirm unlock password

Remote Connection Wipe (Recommended)

This setting gives you the ability to remotely wipe the VPN connection from a user's account (including their Personal Safe) - i.e. if they leave the company or lose their Mac.

Don't allow settings to be changed

This setting prevents users from making accidental or undesirable changes to their VPN connections. The connection is "locked". Users will be able to see the connection settings, but will not be able to modify them.

Hide settings and detailed logs

Hides the Basic and Advanced tabs, as well as the more detailed log levels. Only basic logging and troubleshooting information is displayed. Technical Support Reports cannot be created unless an unlock password is set.

Temporarily permit editing with unlock password (Recommended)

With an unlock password, the connection can be unlocked temporarily, for example if an administrator needs to make changes at a user's computer.

Tip: If you don't set an unlock password, there will be no way to ever make any changes to the exported connection or use a Technical Support Report to analyze a technical problem.

VPN Shortcuts

VPN Shortcuts SecureCorp Shortcuts

If you have configured a VPN Shortcuts Collection, you can choose to include it with your exported connection.

Use a VPN Shortcuts Collection to access all the services they need VPN for – network shares, internal websites, databases, and applications.

VPN Shortcuts selected here are always included when exporting this connection. If you'd like to export additional VPN Shortcuts, simply select them together with your connection before exporting.

Actions

Actions Include actions

If you have configured actions to be executed when the connection is connected or disconnected, you can include them as well. Any settings you have configured in your connection's "Actions" tab will be included.

Contact info

Contact Info helpdesk@securecorp.com
This email address is the default recipient for Technical Support Reports

If your VPN users run into any issues, they can email you a Technical Support Report with details about their connection settings, local internet connection and VPN logs. The email address you enter as your contact info will be set as the default recipient of the report.

Other Considerations

Unlock Password

Experience has shown that when exporting a locked connection, you'll want to unlock it at one point or the other – whether it's making a quick change at an end user's Mac, accessing an end user's Technical Support Report, or even importing the (locked) connection onto your own Mac and accidentally replacing the (unlocked) original.

- If you do not set an unlock password for a locked connection, there is no way to ever change settings.
- If you do not set an unlock password and hide the settings and logs, there's no way to ever access the settings.

Certificates

If your connection uses certificates for authentication, keep in mind that the certificates are not included with the exported connection. You'll need to distribute the certificates as you would normally do.

VPN Tracker 365 will automatically attempt to use the same certificates on the Mac where the connection is imported. If they are not available, the user will be prompted to select new certificates.

Overwriting Existing Connections

If you have made changes to a connection that you have already distributed to your users, it's a good idea to reuse the same connection when exporting (instead of creating a new one).

That way, your users will be prompted to replace their existing connection with the updated one, instead of ending up with another copy, and in the end not knowing which connection is the current one.

Troubleshooting

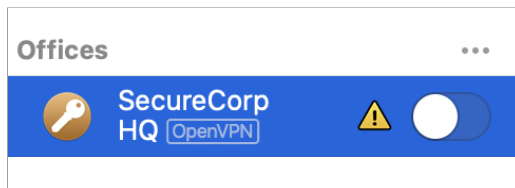
Missing Settings

If you forgot to fill in a setting, VPN Tracker 365 will point it out to you:

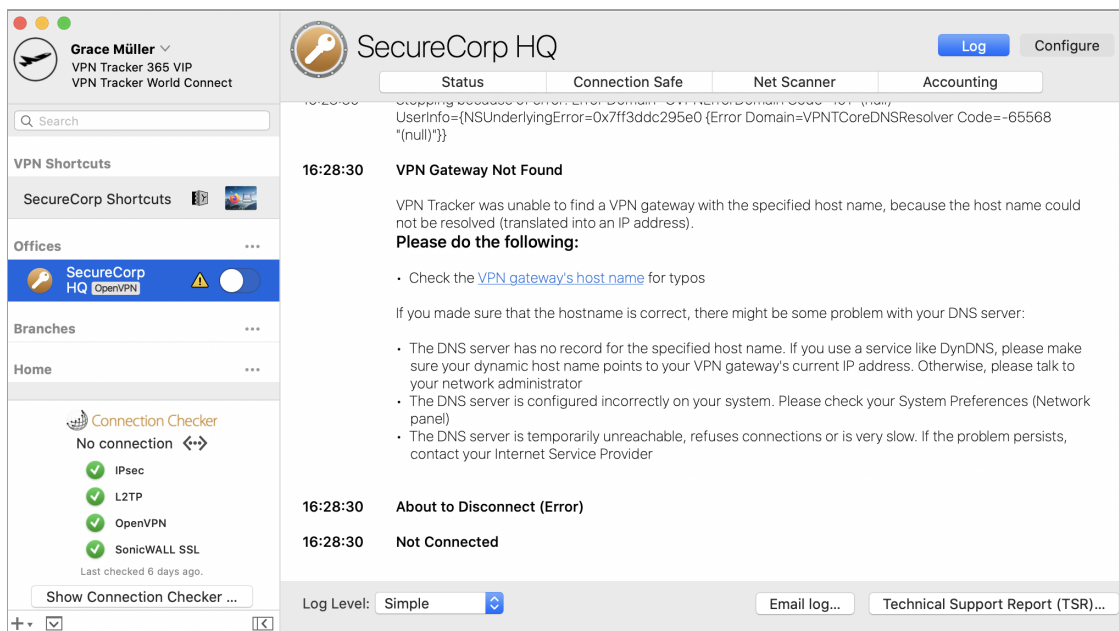


Connection Errors

In case of any other problem, a yellow warning triangle will show up:



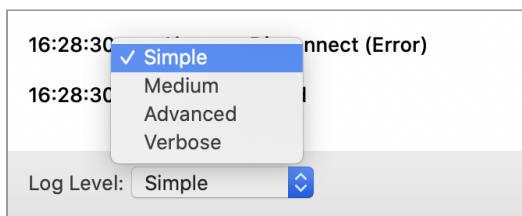
Click on the yellow warning triangle to be taken to the log. The log will explain exactly what the problem is. Follow the steps listed in the log to resolve the problem.



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 window while making changes to troubleshoot a problem.

If you need additional help, you can email the log to your administrator, or send a Technical Support Report (TSR) to equinix or to your network administrator. This contains the settings and logs necessary for resolving technical problems. Confidential information (e.g. passwords, private keys for certificates) is **not** included in the TSR.

Tip: You can use the dropdown menu at the bottom of the “Log” window to change the level of the log depending on how complex the issue is:



No Access to the Remote Network

If your VPN appears to be connected, but you cannot access resources (servers, email, etc.) in the remote network, check the following points to resolve the problem.

Connect to an IP address (instead of a host name)

If you are using a host name (e.g. fileserver.example.com) to connect to the resource, please try using its IP address instead.

If the connection works when using the IP address, but not when using a host name, please make sure that your Mac's DNS server is able to resolve this host name to an IP address, or set up a suitable remote DNS server in VPN Tracker.

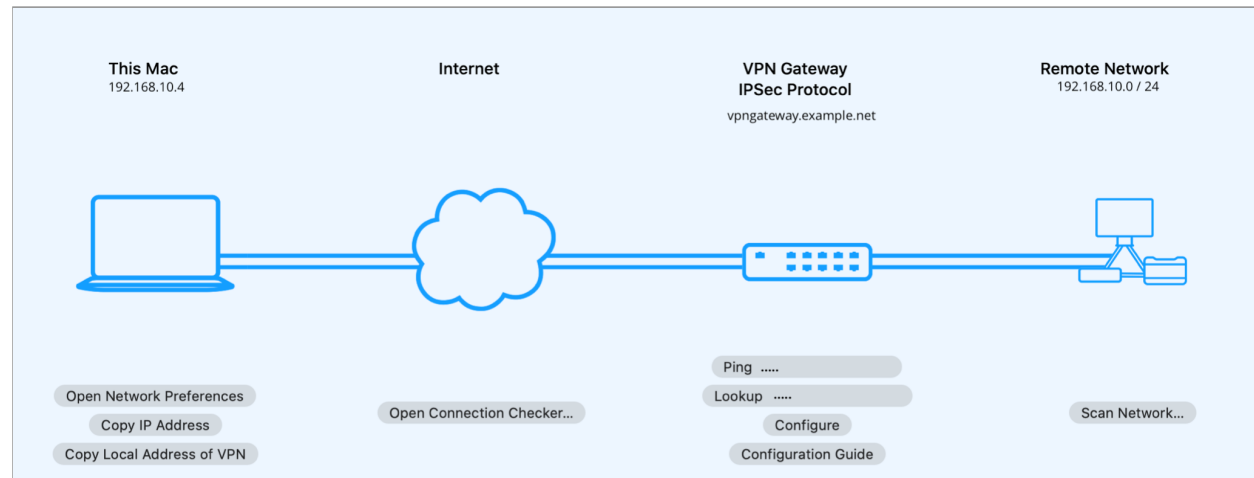
Check that the IP address you are connecting to is part of the VPN's remote network

Check that the IP address you are connecting to is part of the remote network(s) of the VPN. Also double-check the network mask that you have configured for the remote network(s) in VPN Tracker 365. If you're using SonicWALL Simple Client Provisioning or Cisco EasyVPN, the remote network(s) are assigned by your VPN gateway. Refer to the Status tab for this.

Make sure the host you are trying to reach knows where to send replies

Start with checking if your local address is part of the remote network:

- Connect the VPN
- Go to the Status tab
- Compare the IP address listed under "This Mac" (local address) and the networks listed under "Remote Network". Is the local address part of the remote network(s)?



In this example, the local address 192.168.10.4 is part of the remote network 192.168.10.0 / 24

If the local address is part of the remote network(s):

There are exactly three setups where the local IP address may be part of the remote network(s). If your setup is not one of these, you must choose a local address that is **not** part of the remote network(s).

1. When connecting to a SonicWALL using SonicWALL Simple Client Provisioning or DHCP over VPN.
2. When connecting to a Cisco VPN gateway using Cisco EasyVPN.
3. When connecting to a VPN gateway that can act as an ARP proxy for IP addresses assigned through Mode Config, and/or for fixed local addresses.

That third one is a bit tricky to figure out. If you find a reference to ARP Proxy (or Proxy ARP) in the device's documentation, or if the manual specifically instructs to choose the local address or the Mode Config address pool to be part of the remote network, then it's ok for the IP address to be part of the remote network.

In all other cases you must choose an IP address as the local address (or a Mode Config address pool) that is not part of the remote network(s). If you are using Mode Config, you need to change the Mode Config address pool on the VPN gateway. Otherwise, simply change the local address in VPN Tracker (Basic > Local Address).

If the local IP is not part of the remote network(s):

Check if your VPN gateway is the default gateway (router) of its network.

If your VPN gateway is not the default gateway of the remote network, you will have to ensure that responses to all IP addresses used by VPN clients are routed to the VPN gateway. You can do so either by adding a general route on the network's actual default gateway, or by adding individual routes on each host that VPN clients need to communicate with.

Using the troubleshooting tools in the Status view

The connection status view in VPN Tracker 365 also contains helpful troubleshooting tools to help identify possible problems at different stages of the connection process. Click on the buttons to spring to the respective tools and rectify problems (e.g. check your internet connection is functioning correctly by opening → [Connection Checker](#)).

Troubleshooting Remote DNS

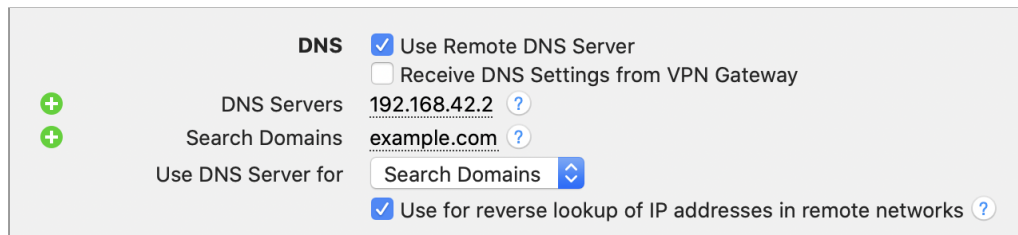
If you can access resources on the remote network using their IP addresses, but not their host names, you will need a suitable remote DNS setup.

Prerequisites for remote DNS:

- A DNS server that is able to resolve those IP addresses exists.
- The DNS server can be reached through the VPN.

To illustrate the steps for debugging remote DNS issues, here's an example setup using remote DNS:

- We have a VPN connection to the remote network 192.168.42.0/24.
- In this network, there's a file server *fileserver.example.com*.
- We can reach this file server using its IP address 192.168.42.10.
- We'd like to reach this file server using its host name *fileserver.example.com*.
- This host name cannot be looked up using public DNS servers, but there is an internal DNS server with IP address 192.168.42.2 that is able to resolve hosts in the *example.com* domain, including *fileserver.example.com*.



The screenshot shows the DNS configuration for a network interface. The 'DNS' section is expanded, showing the following settings:

- Use Remote DNS Server
- Receive DNS Settings from VPN Gateway
- DNS Servers: 192.168.42.2
- Search Domains: example.com
- Use DNS Server for: Search Domains
- Use for reverse lookup of IP addresses in remote networks

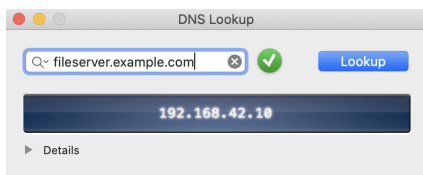
For remote DNS settings to take effect, the VPN needs to be reconnected. We should now be able to connect to *fileserver.example.com* using its host name.

Tip: If you set a remote DNS server for “All Domains” instead of specific “Search Domains”, make sure it is a working DNS server that can resolve hosts on the Internet. Otherwise, your Mac will seem to be cut off from the Internet when the VPN is connected.

Steps to Troubleshoot

If connecting using the host name does not work, the first step is to use the DNS Lookup Tool to verify that the host name can be looked up.

- Connect the VPN, Go to “Tools” > “DNS Lookup” in the menu bar on top of the screen
- Enter the host name (here: *fileserv.example.com*) and click “Lookup”



If the DNS Lookup Tool displays the expected result, remote DNS is configured correctly. In that case, the problem is with the actual connectivity, not DNS. If DNS lookup fails, then the problem is with remote DNS.

The next step is to figure out if the problem is with the remote DNS server itself, or with the remote DNS setup.

- Open a Terminal window (Applications > Utilities > Terminal)
- Enter: `dig <host name> @<remote DNS server>` and press return. In our example: `dig fileserv.example.com @192.168.42.2`

If you see an “Answer Section” with the correct IP address, then both the connectivity to the DNS server, and the DNS server’s response are ok. In that case, the problem lies with the remote DNS setup. Double-check the configuration in VPN Tracker 365.

```
# dig fileserv.example.com @192.168.42.2
; <<> DiG 9.7.6-P1 <<> fileserv.example.com @192.168.42.2
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 30106
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;fileserv.example.com.      IN A

;; ANSWER SECTION:
fileserv.example.com.     3600 IN A  192.168.42.10

;; Query time: 879 msec
```

If you don’t see an “Answer Section” with the correct IP address, then the remote DNS server is not configured to resolve *fileserv.example.com*. If you get a timeout error, then the remote DNS server is not reachable over the VPN or it is not a properly configured DNS server.

Managing Your VPN Tracker 365 Plan

The VPN Tracker 365 service allows you to easily view and update information regarding your VPN Tracker 365 plan online. It also has all the necessary tools in place for network admins to successfully set up and manage multiple plans for a team of VPN users.

my.vpntracker.com

All VPN Tracker 365 plans can be managed via my.vpntracker.com. Here you can view your personal VPN Tracker 365 plan(s), access your Personal Safe, and also access team information and Team Management features.

To get started, log in using your equinix ID and password.

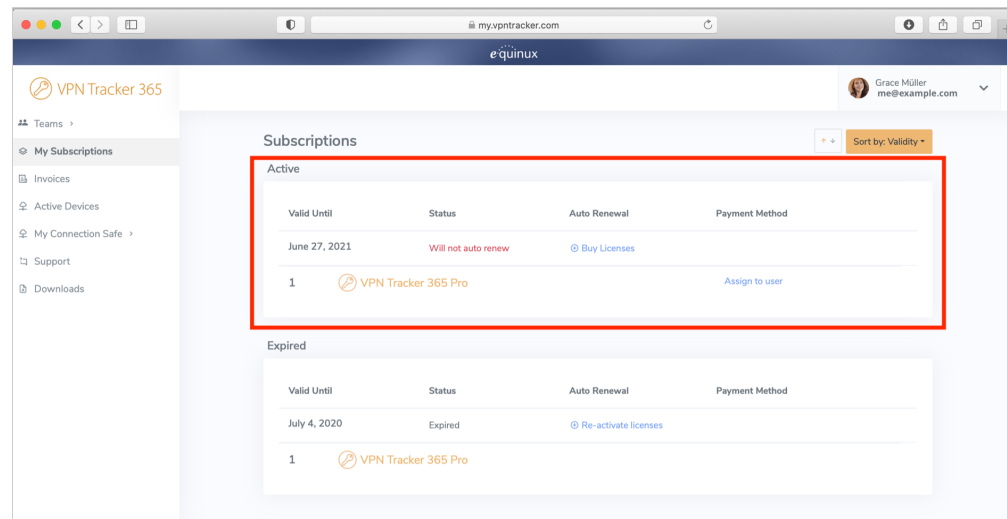
Managing your personal VPN Tracker account

After logging in to my.vpntracker, you will first be shown the Teams overview as a default. Head to "My Subscriptions" in the left sidebar to view your personal VPN Tracker 365 plan(s). Here you can view both active and expired plans:

In this area, you can also:

- View the validity period of your VPN Tracker 365 plan and manage your renewal preferences on plans you have purchased
- Keep track of your active devices and remove any devices which are no longer in use
- Manage your payment methods
- Access and download your past invoices
- My Connection Safe
- Support
- Downloads

To manage your VPN Tracker 365 team(s), go to "Teams" in the sidebar.



VPN Tracker 365 for Teams

VPN Tracker 365 also offers a wide range of features designed for teams and organizations. In this section, we'll take you through some of the core features aimed at team managers and users.

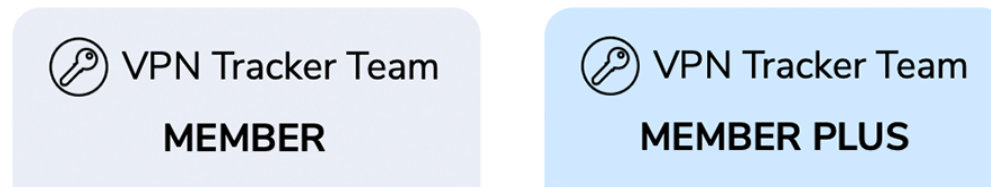
Creating a VPN Tracker 365 Team

Team Management Guide

If you are a Team Manager looking to set up a VPN Tracker team, our step-by-step [Team Management Guide](#) has all the detailed information you need to get started, including inviting team members, assigning plans, accessing invoices, and managing your team's connections.

VPN Tracker 365 Plans for Teams

As mentioned in the → [plans overview section](#), we also offer two VPN Tracker 365 editions exclusively for teams:



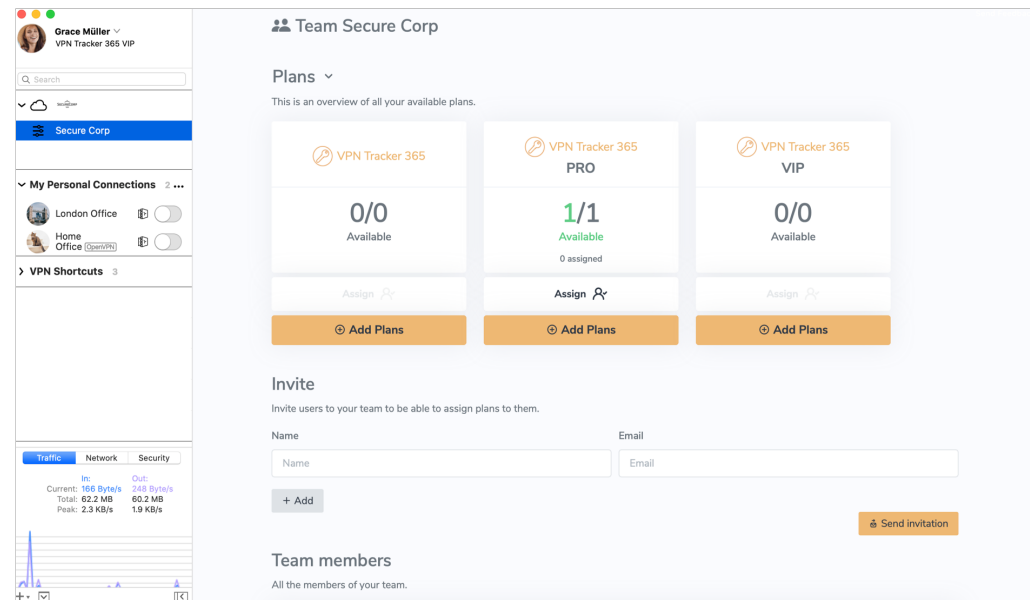
These plans are specifically designed for end-users who only need to *receive* pre-configured VPN connections and Shortcuts and don't need to configure their own connections. Find out specific details about each plan option in our [Buyer's Guide](#).

Managing VPN Tracker Teams

Managing your team is easier than ever thanks to integrated Team Management tools within the VPN Tracker 365 app. On the go? You can also manage your team on the web at my.vpntracker.com.

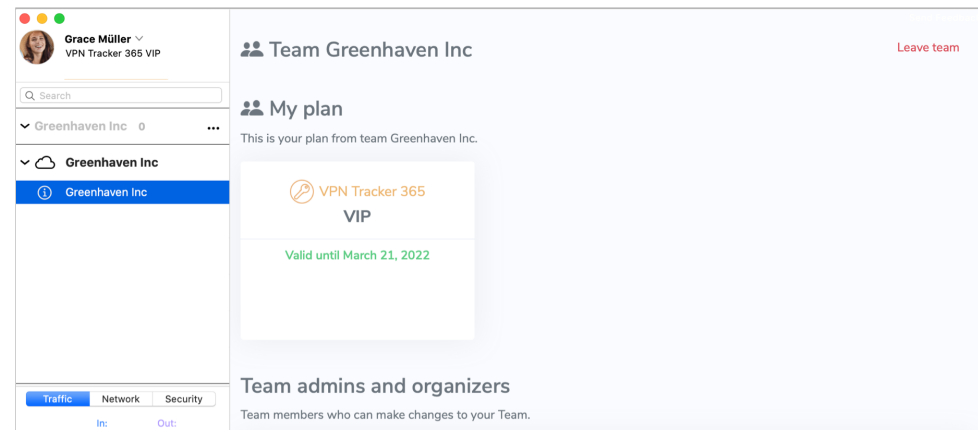
Team Managers can manage VPN Tracker 365 teams directly from within the VPN Tracker 365 app or on the web via my.vpntracker.com.

To access your team in VPN Tracker 365, go to the app sidebar, find your team name, and click the settings icon. Here you can find key information on your available plans, manage team members, update your company logo, and add domains for [Team Discovery](#).



Team Members can also view important information about their team(s) and plan(s) in the VPN Tracker 365 app, as well as their my.vpntracker.com account.

Go to the app sidebar, find your team, and click the information (i) icon. In this view, you can view your current plan, identify your team manager(s), or leave a team.



Enterprise Rollout

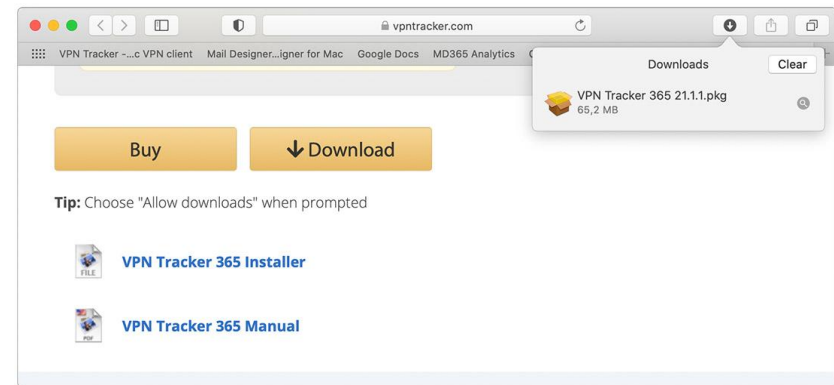
Especially in larger teams, onboarding can be a time consuming process, which is why VPN Tracker 365 offers several useful features to help you get new team members set up quickly and hassle-free.

VPN Tracker 365 Package Installer

If you manage Macs remotely, you can install VPN Tracker 365 using the Package Installer for a more simplified rollout process. This lets you set up VPN Tracker for users that do not have manager access on their Macs.

- [Download the Package Installer file](#) from the VPN Tracker website
- Use Remote Desktop (or similar software) to remotely install VPN Tracker 365 on your team's Macs. This will install all required components, including those that need an administrator password
- Pre-authorize the system extension for team members → [Learn more](#)

VPN Tracker 365 will now be ready to launch without any need for admin privileges. For best results, drag the VPN Tracker 365 app into the user's Applications folder.



Personalized Team Invitation Links

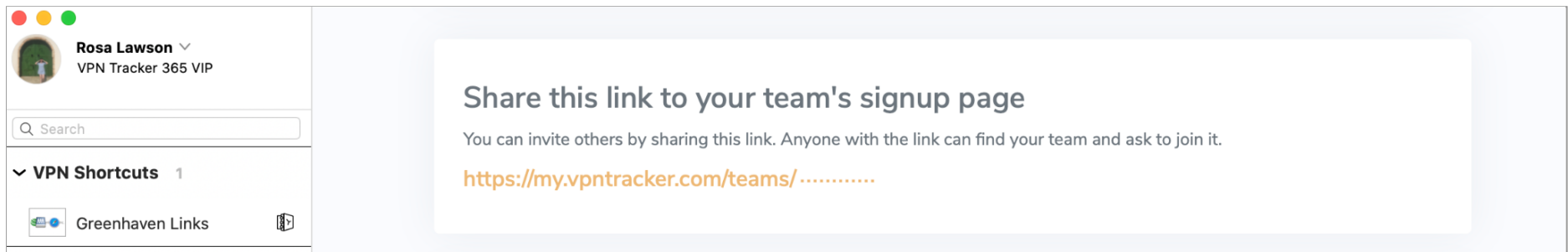
Every VPN Tracker 365 team has a personalized team invitation link which can be used to quickly onboard larger groups of new team members.

Rather than sending out mass invitations, you can share your team link with colleagues in a secure internal chat or post it on the company intranet. Alternatively, you can also include your team's link in an onboarding email when welcoming new staff.

Anyone with this link will be redirected to sign in or create an account before being able to request access to your VPN Tracker team.

Accessing your team's link

You can find your team's invitation link via your team settings in the VPN Tracker 365 app or by going to your team's overview page at [my.vpntracker](#).

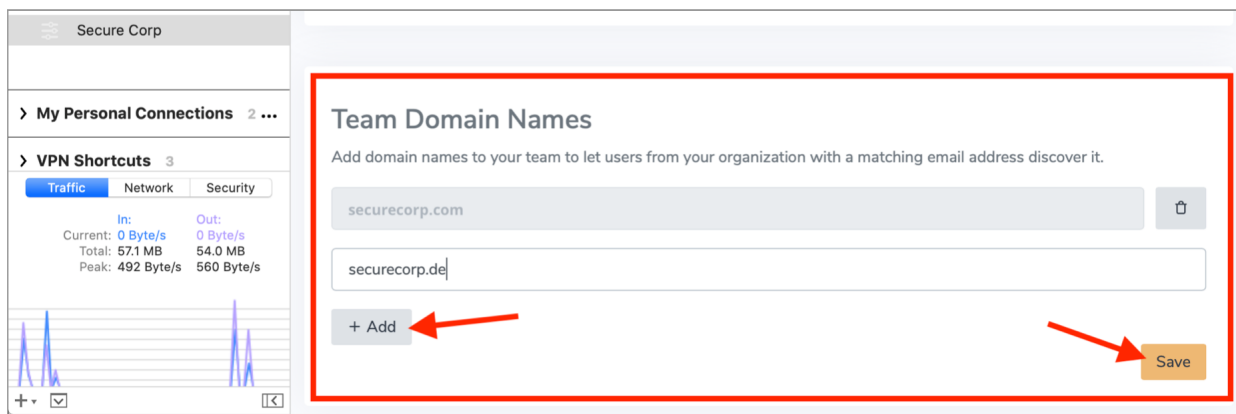


The screenshot shows a user interface for a VPN Tracker 365 team. On the left, there is a sidebar with a user profile for Rosa Lawson (VPN Tracker 365 VIP), a search bar, and a section for VPN Shortcuts (1) containing Greenhaven Links. The main content area displays a message: "Share this link to your team's signup page" followed by "You can invite others by sharing this link. Anyone with the link can find your team and ask to join it." Below this is a placeholder for a team link: <https://my.vpntracker.com/teams/.....>

Team Discovery

Team Discovery via email domain is another way for new team members to request access to a team using their company email address.

As a Manager or Organizer, you can enter all associated company domain names to your team's profile. Access this field via your team settings in the VPN Tracker 365 app or via your team's overview page at [my.vpntracker](#).



Once you have done this, new team members that have signed up for a VPN Tracker account with one of the recognized email domains will instantly be shown available teams when they first sign in to VPN Tracker 365 and can request access, speeding up the onboarding process for everyone.

Tip: Remember to enter all variations of a domain if your company has multiple email addresses. E.g. securecorp.com, securecorp.co.uk, and securecorp.de. To add multiple domains, simply click the "Add button" then save your changes once finished.

TeamCloud

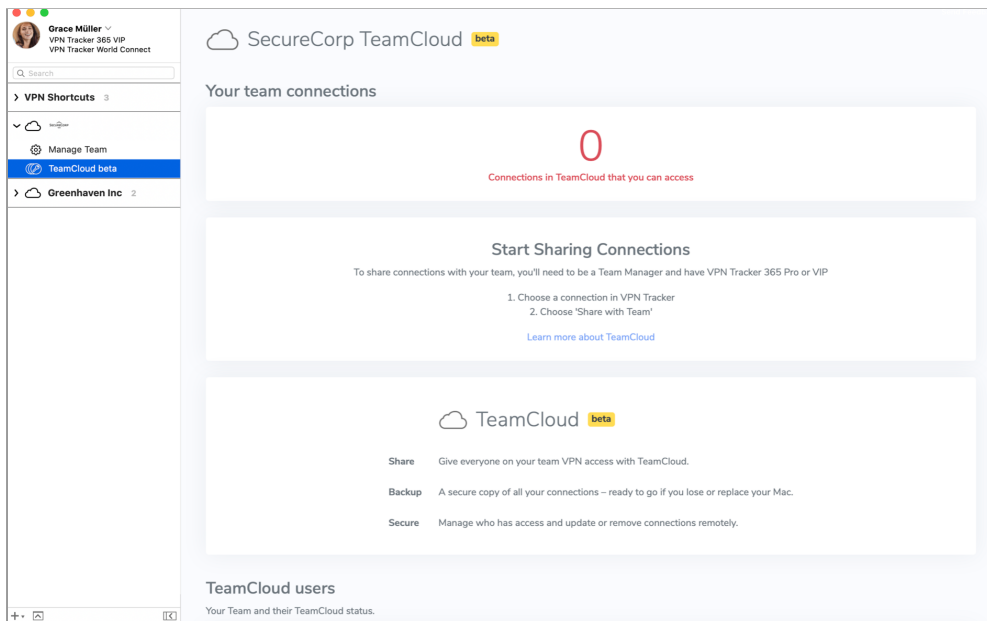
What is TeamCloud? TeamCloud is a centralized security management solution for teams - exclusively available in VPN Tracker 365.

Just like → [Personal Safe](#), you can use TeamCloud to securely store and sync VPN connections and Shortcuts for your team, as well as to determine advanced endpoint security settings (*coming soon*). Where your Personal Safe offers backup and sync for just one user, TeamCloud allows you to share pre-configured connections with other users. Everyone keeps their own username and password - making the onboarding process even easier.

Visit the [VPN Tracker 365 website](#) to learn more about the benefits of Team Cloud.

Accessing TeamCloud

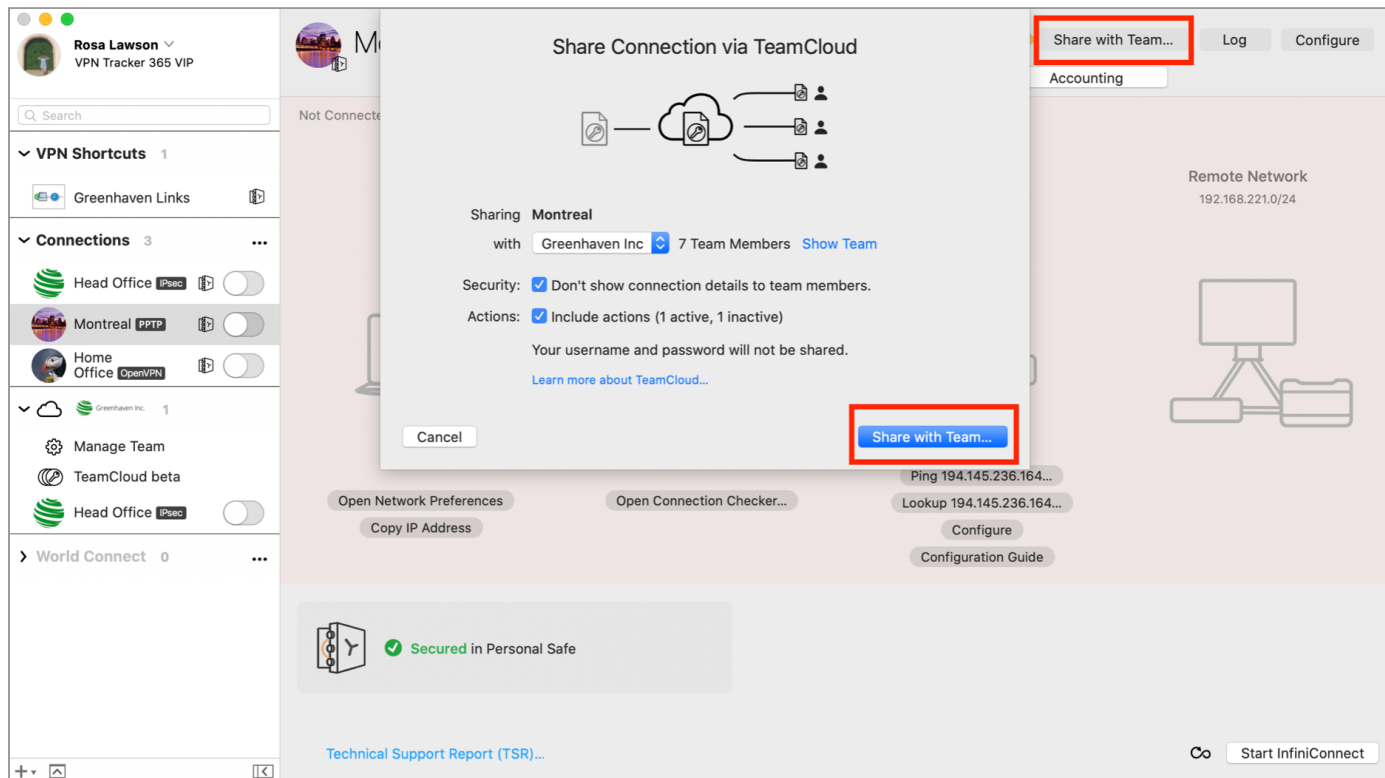
TeamCloud can be viewed and accessed via the sidebar in the VPN Tracker 365 app or on your team's page at [my.vpntracker](#):



Here, you can view your saved connection(s) and also see your TeamCloud members.

Sharing VPN connections via TeamCloud

To share a VPN connection via TeamCloud, click on a connection in the sidebar to open the Status view and click **Share with Team...** in the top of the window. You will then be given the opportunity to review your settings before sharing the connection with all team members:



By **Security**, you can also opt to hide confidential connection information from other team members before sharing the connection.

Sharing VPN Shortcuts with TeamCloud

Similarly, to share VPN Shortcuts with your team via TeamCloud, go to a Shortcuts collection and click Share with Team... in the top right of the window:

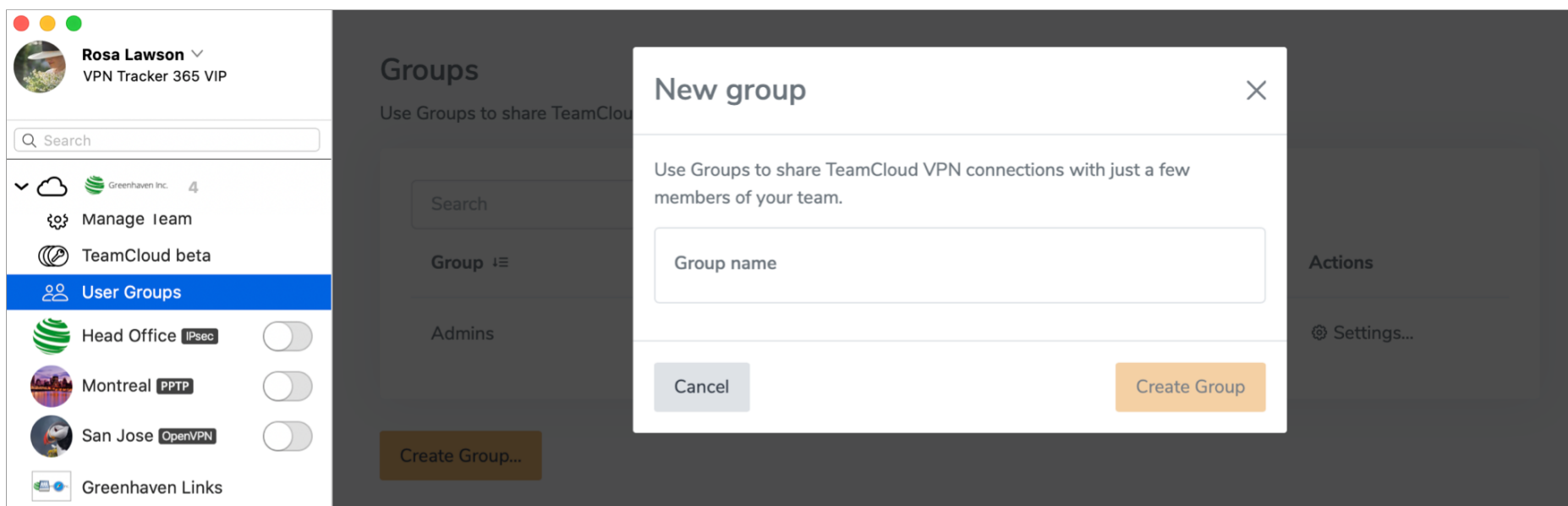


Setting up TeamCloud Groups

With TeamCloud, you can also set up dedicated groups to share connections exclusively with selected team members (e.g. just admins or just the marketing team).

To create and manage User Groups directly in the VPN Tracker 365 app or at my.vpntracker via the **Groups** tab, you will need a VPN Tracker 365 VIP plan and Manager or Organizer status. To receive group connections, you need a Team Member Plus or VIP plan.

Go to your Team in the VPN Tracker 365 sidebar menu and select **User Groups**. Here you will see an overview of your current groups and can create new groups for specific use cases. Click **Create Group...** to get started:



Once you have set up Groups, you will see them on the overview page. Click on a Group to manage its settings or add members. Once you have set up connections for certain groups, you will be able to view them here under **Group connections**.

The screenshot displays the VPN Tracker interface. On the left is a sidebar with the user profile 'Rosa Lawson' (VPN Tracker 365 VIP) and a search bar. Below are sections for 'VPN Shortcuts' (Greenhaven Links), 'Connections' (Head Office IPsec, Montreal PPTP, San Jose OpenVPN), and 'User Groups' (Head Office IPsec, Montreal PPTP, San Jose OpenVPN, Greenhaven Links). At the bottom of the sidebar are 'World Connect' and 'equinux staff' sections, and a 'Connection Checker' button.

The main area is titled 'Groups' and includes the instruction: 'Use Groups to share TeamCloud VPN connections with just a few members of your team.' Below this is a table of groups:

Group	Members
Admins	2 members
Marketing	0 members

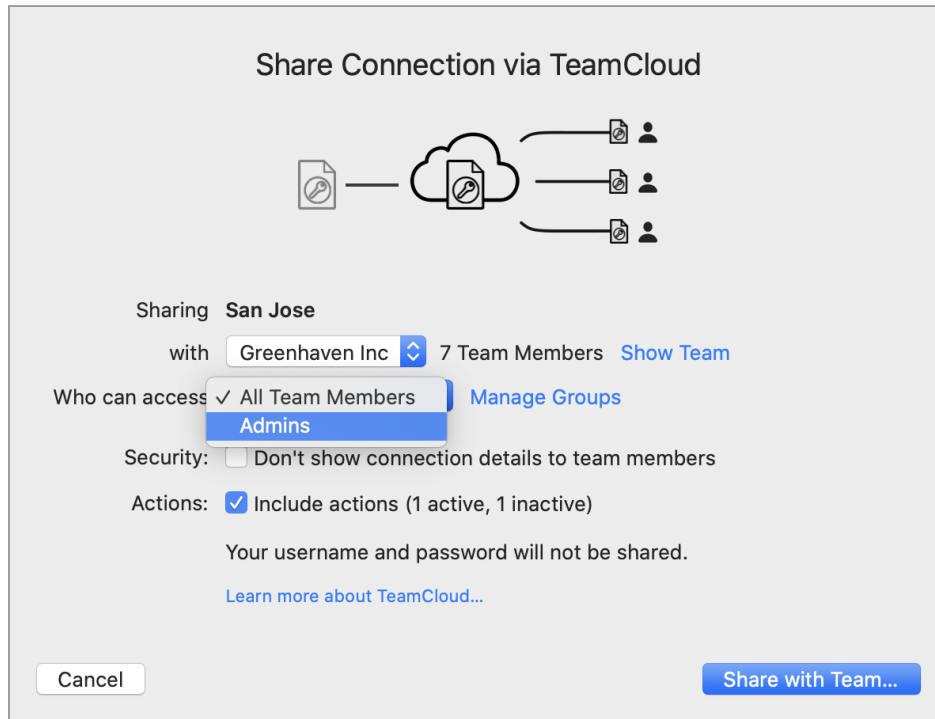
A 'Create Group...' button is located below the table. The 'Marketing' group is selected, opening a modal window titled 'Group "Marketing"'. This modal has tabs for 'Details' and 'Settings'. The 'Details' tab is active and shows a search bar, a 'Manage group members...' button, and a table for group members (currently empty with 'No results'). Below the members table is a 'Manage connections...' button and another table for group connections (also empty with 'No results'). The 'Settings' tab is also visible and contains options to 'Rename group' (with a 'Marketing' input field and a 'Rename' button) and 'Delete group'. A warning message states: 'Once you delete a team, there is no going back. Please be certain. Note: VPN connections that are locked to this group might get deleted.' Below the warning is a red 'Delete' button.

Click on **Manage group members** to select the Team Members you want to add to the User Group.

Sharing a VPN connection with a User Group

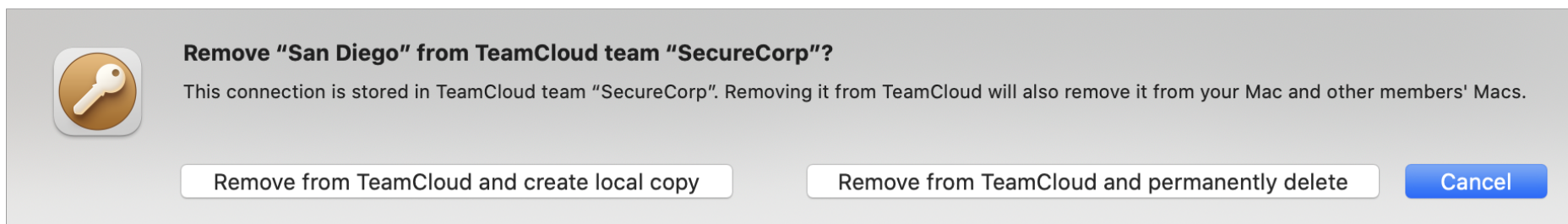
After you have set up a User Group, you can go ahead and share VPN connections and Shortcuts with them. To do so, click Share to open the share panel, then go to **Who can access:** and select a group from the dropdown list. The connection will now be made available to these Team Members only.

Tip: If you want to set up another new User Group, click **Manage Groups** to go to the configuration.



Removing connections from TeamCloud

In order to fully remove a connection from your TeamCloud, you can right-click the connection and select **Remove from TeamCloud**. You will then be given the option to save a local copy or to permanently delete:



As soon as a connection or Shortcuts collection is removed from TeamCloud, team members will not have access.

Please note: If you don't opt to save a local copy of the connection, you will also no longer have access to it outside of TeamCloud.

Configuring a connection in TeamCloud

As a Team Manager or Organizer, you are able to update and configure connections within TeamCloud to remotely rollout and sync changes across your team.

In order to do this, simply click on a connection in the TeamCloud, go to the **Configuration** window and carry out the changes you need. Once you've clicked **Done**, your connection will automatically sync the changes to TeamCloud.