

Manage Umbrella Roaming Client and VPN Compatibility

Contents

[Introduction](#)

[Overview](#)

[How the Umbrella Roaming Client Operates with VPN Clients](#)

[Umbrella Roaming Client Incompatibilities](#)

[Incompatibility Reasons for VPN Clients](#)

[Virtual Appliances and Protected Networks](#)

[Special Considerations for Standalone and Cisco Secure Client + Roaming Security Module](#)

[DNS Binding Order VPN Compatibility Mode for Windows 10 and 11](#)

[Example resolv.conf output](#)

[Special Considerations for Third-Party VPNs](#)

[Always-On VPN](#)

[Solutions](#)

[Viscosity VPN](#)

[Configure Viscosity](#)

[Tunnelblick](#)

[Tunnelblick VPN Disconnect Issues](#)

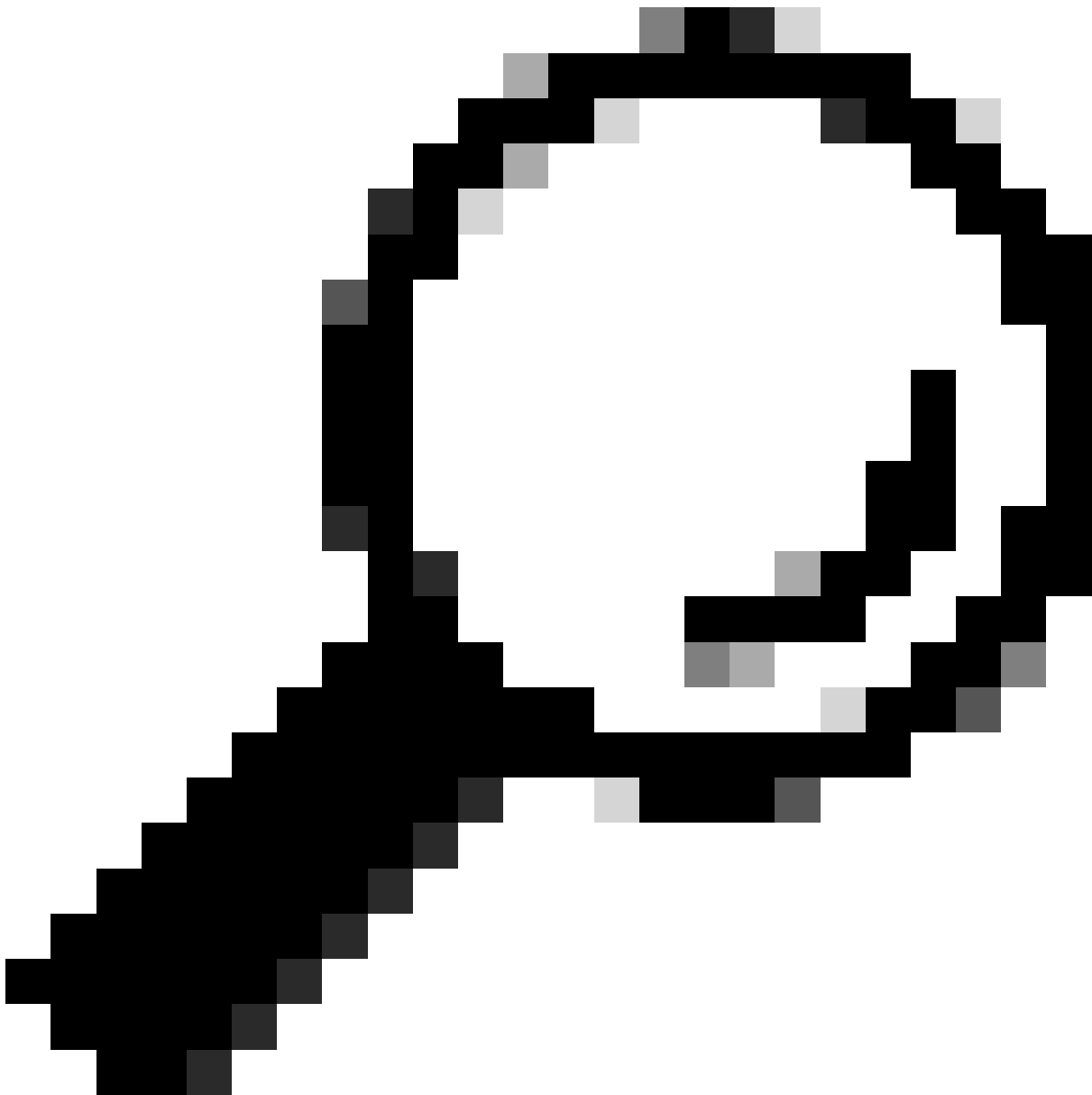
[Lightspeed Rocket](#)

Introduction

This document describes the interaction and compatibility of the Cisco Umbrella Roaming Client with various VPN software.

Overview

The Cisco Umbrella Roaming Client works with most VPN software, but additional steps can be required for expected operation. Cisco Umbrella recommends deploying the Cisco Secure Client and Roaming Security module for maximum compatibility. This module can be deployed without the VPN components.



Tip: This document serves as general guidance and does not serve as an official list of supported software. Cisco Umbrella does not test, validate, or certify functionality with any third-party software or VPN client.

This document provides technical information and additional context for specific VPN clients that can require further configurations. For a list of known incompatible VPN software, refer to the **Umbrella Roaming Client Incompatibilities** section. DNS incompatibility with the Roaming Client can also cause Cisco Secure Client + Roaming Security module with SWG to fail, as the SWG client also depends on successfully establishing a DNS connection.

How the Umbrella Roaming Client Operates with VPN Clients

The Umbrella Roaming Client binds to all network adapters and changes DNS settings on the computer to 127.0.0.1 (localhost). This allows the Umbrella Roaming Client to forward all DNS queries directly to Umbrella while allowing the resolution of local domains through the Internal Domains feature. Upon

establishing a connection to a VPN server, the Umbrella Roaming Client detects a new network connection in the system and changes the connection DNS settings to point toward the Umbrella Roaming Client. The Umbrella Roaming Client relies on performing DNS lookups to Umbrella AnyCast DNS IP addresses (208.67.222.222/208.67.220.220).

If a user connects to a VPN, the firewall associated with the VPN must allow access to Umbrella.

Umbrella Roaming Client Incompatibilities

The Umbrella Roaming Client currently delivers DNS layer enforcement. The DNS layer is the primary function of the Roaming Client, applying DNS-based security policies on any network. This function of the Roaming Client can experience known software incompatibilities. The DNS Layer of the Umbrella Roaming Client is incompatible with the clients listed below, based on support team testing. Cisco Umbrella Engineering does not verify or test these clients, and all entries are subject to review. This article refers to the standalone Umbrella Roaming Client. For a companion article on the Umbrella Roaming Security Module for Cisco Secure Client (and legacy), refer to the relevant documentation.

VPN Client	Issue/Incompatibility	Resolution
Pulse Secure	On disconnect, saved local DNS can remain VPN values rather than WiFi/Ethernet values due to Pulse modification during VPN connection.	Resolved with the Umbrella module - included in most licenses.
Avaya VPN	Incompatible.	Resolved with the Umbrella module - included in most licenses.
Windows VPN (notably Always On VPN)	Can result in local DNS failing to resolve to the internal answer despite the DNS hostnames being on the internal domains list.	Resolved with the Umbrella module - included in most licenses.
VPN "apps" built on top of the Windows Universal Platform	These apps must utilize a Microsoft connection API that requires DNS to be sent to the local NIC, not 127.0.0.1. Therefore, the app displays an error indicating it cannot connect.	Resolved with the Umbrella module - included in most licenses.
OpenVPN	Incompatible.	No fix available.
Palo Alto GlobalProtect VPN	Does not work with any standalone roaming client version after 3.0.110.	Fixed by using the Umbrella module - included in most licenses.
F5 VPN	Incompatible.	Fixed by the Umbrella module - included in most licenses.
Checkpoint VPN	macOS Only, Split-tunnel mode only.	Disable split-tunnel on macOS.

VPN Client	Issue/Incompatibility	Resolution
SonicWall NetExtender	Incompatible.	Fixed by the Umbrella module - included in most licenses.
Zscaler VPN	Incompatible.	Fixed by the Umbrella module - included in most licenses.
Akamai endpoint protection (ETPclient)	Incompatible.	Fixed by the Umbrella module - included in most licenses.
NordVPN	Use workaround.	<p>Two options exist for adding compatibility:</p> <ol style="list-style-type: none"> 1. Use the OpenVPN connection method as outlined in How to set up a manual connection on Windows using OpenVPN 2. Allow custom DNS under Advanced settings. Set DNS to 208.67.220.220 and 208.67.222.222.
Azure VPN	Incompatible.	Fixed by the Umbrella module - included in most licenses.
AWS VPN	Use workaround.	Edit the config file (downloaded from AWS manually) to have a second line of pull-filter ignore "block-outside-dns".
Pritunl VPN	Incompatible.	Fixed by the Umbrella module - included in most licenses.

Incompatibility Reasons for VPN Clients

Some VPN clients have DNS behavior similar to the Umbrella Roaming Client. If the VPN connection DNS server changes to an unexpected value, the VPN software changes the system DNS settings back to the value the VPN set when initially connected. The Umbrella Roaming Client also performs the same operation, changing any DNS servers back to 127.0.0.1. This back-and-forth behavior creates a conflict between the VPN and the Umbrella Roaming Client. This conflict causes an endless cycle of the DNS servers for the VPN connection resetting. The Roaming Client detects this and disables itself to maintain the VPN connection if possible.

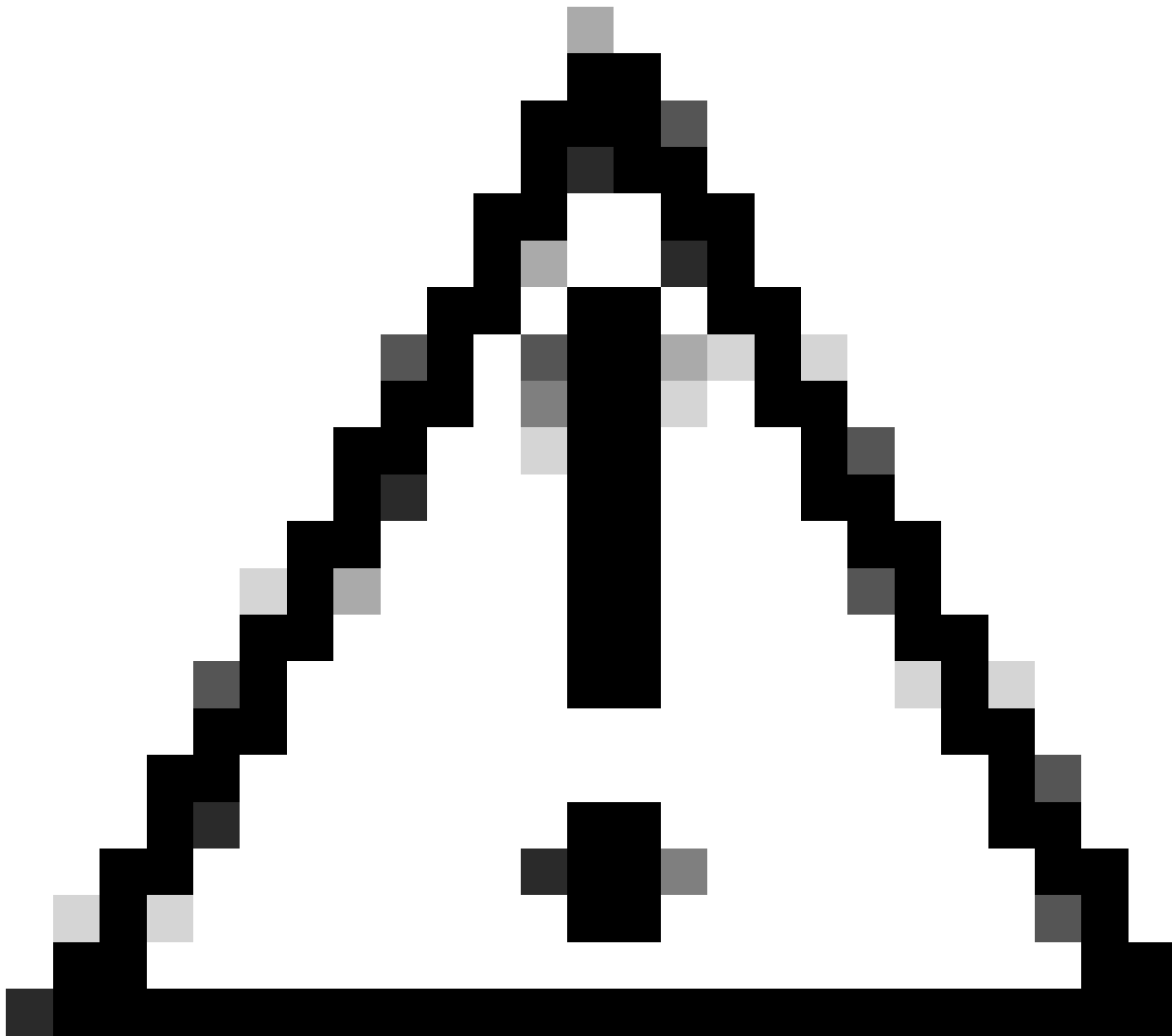
Virtual Appliances and Protected Networks

The Umbrella roaming client behaves differently when connected to a network that utilizes the Umbrella Virtual Appliances (VA) or the Protected Networks feature. This applies whether a user connects to the network locally or through a VPN. For more information, refer to [Roaming Client and Virtual Appliances or Protected Networks](#) documentation.

Special Considerations for Standalone and Cisco Secure Client + Roaming Security Module

The information provided here is specific to the standalone Umbrella Roaming Client and does not extend to the Cisco Secure Client (CSC) + Roaming Security Module. Users seeking an easy plugin installation can use Umbrella Roaming integrated into CSC. Cisco Secure Client VPN users must migrate to the CSC + Roaming Security Module if a functional issue with the VPN occurs. Cisco Umbrella requires validation on the CSC + Roaming Security Module and recommends a full migration.

The Cisco Secure Client VPN software provides options for how the system handles DNS when a VPN connection establishes. See the article [Behavioral Differences Regarding DNS Queries and Domain Name Resolution in Different OSs](#) for additional details. This information is based on experience using Cisco Secure Client and the Umbrella Roaming Client. Testing the Umbrella roaming client with Cisco Secure Client VPN enabled is recommended to ensure internal and external DNS resolution functions as expected.



Caution: Cisco requires that you use the CSC + Roaming Security Module if you are also using Cisco Secure Client for DNS service compatibility. The provided steps are for the non-integrated Roaming Client only if required. These steps are not required for the CSC + Roaming Security Module.

In both full and split tunnel modes, special instructions are required to allow the Roaming Client to work while Cisco Secure Client is connected. This is required in order to allow DNS to flow to the roaming client rather than being overridden by kernel driver. For full tunnel, the symptom is that the client is forced to disable. For split tunneling, the symptom is a loss of internal DNS while connected to the VPN.

DNS Binding Order VPN Compatibility Mode for Windows 10 and 11

A limited set of Windows 10 users encounter a specific issue where the local LAN is prioritized instead of the VPN NIC for DNS. In this event, local DNS on the internal domains list for the roaming client fails to resolve while public DNS functions without issue. This affects versions 2.0.338 and 2.0.341 (by default) and all later versions. The issue did not occur on version 2.0.255.

The previously impacted VPN clients include:

- AnyConnect 3.x
- AnyConnect 4.x (AnyConnect Umbrella or CSC + Roaming Module is not impacted)
- Sophos VPN
- Some Palo Alto GlobalProtect configurations on older versions
- WatchGuard Mobile VPN
- Shrew Soft VPN
- Barracuda VPN

Resolution

Toggle the Roaming Client setting **Enable legacy VPN compatibility mode** to enabled.

Roaming Computers Settings

Umbrella Roaming Client

- ☐ Disable DNS redirection while on an Umbrella Protected Network. ⓘ
- ☒ Enable Active Directory user and group policy enforcement and internal IP address visibility.
- ☒ Enable legacy VPN compatibility mode. [Learn More](#)

360027547111

To confirm if this is the issue, run the diagnostic test and click on the results for `resolv.conf`s. If the VPN adapter is listed first, the issue does not impact the user. If the VPN adapter is listed second, the issue can impact the user.

Example resolv.conf output

Results for: `resolv.conf`s

```
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Local Area Connection
nameserver 192.168.2.1
```

```
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Cisco AnyConnect Secure Mobility
nameserver 10.1.1.27
nameserver 10.1.1.28
```

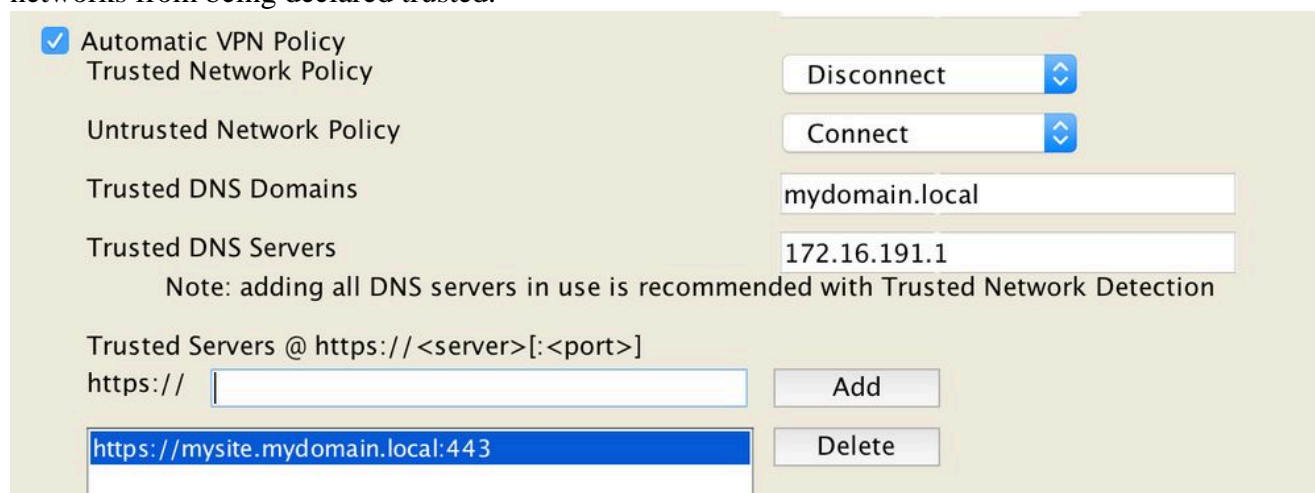
Special Considerations for Third-Party VPNs

Always-On VPN

The standalone roaming client is incompatible with the Cisco Secure Client **Always On VPN setting** when Trusted DNS servers are defined. When active, the standalone roaming client always sets DNS to 127.0.0.1, eliminating all trusted DNS servers from the NIC settings. The Roaming Client can be disabled on the network to restore DHCP settings; however, all Roaming Client-related protections cease when configured. Contact Umbrella support to learn more about disabling the client on a trusted network.

Solutions

- The CSC + Roaming Security Module (Roaming Client for Cisco Secure Client) is not affected and functions effectively with an Automatic VPN policy.
- Add 127.0.0.1 to the trusted DNS servers list.
- Ensure that alternate methods of trusted detection are defined (DNS names and servers) to prevent all networks from being declared trusted.



The screenshot shows the Cisco Secure Client configuration window for an Always-On VPN policy. The 'Automatic VPN Policy' checkbox is checked. The 'Trusted Network Policy' is set to 'Disconnect' and the 'Untrusted Network Policy' is set to 'Connect'. The 'Trusted DNS Domains' field contains 'mydomain.local' and the 'Trusted DNS Servers' field contains '172.16.191.1'. A note below these fields states: 'Note: adding all DNS servers in use is recommended with Trusted Network Detection'. The 'Trusted Servers @ https://<server>[:<port>]' section shows a list of servers. The first entry is 'https://mysite.mydomain.local:443', which is highlighted in blue. There are 'Add' and 'Delete' buttons next to the list.

Trusted Servers @ https://<server>[:<port>]	Action
https://	Add
https://mysite.mydomain.local:443	Delete

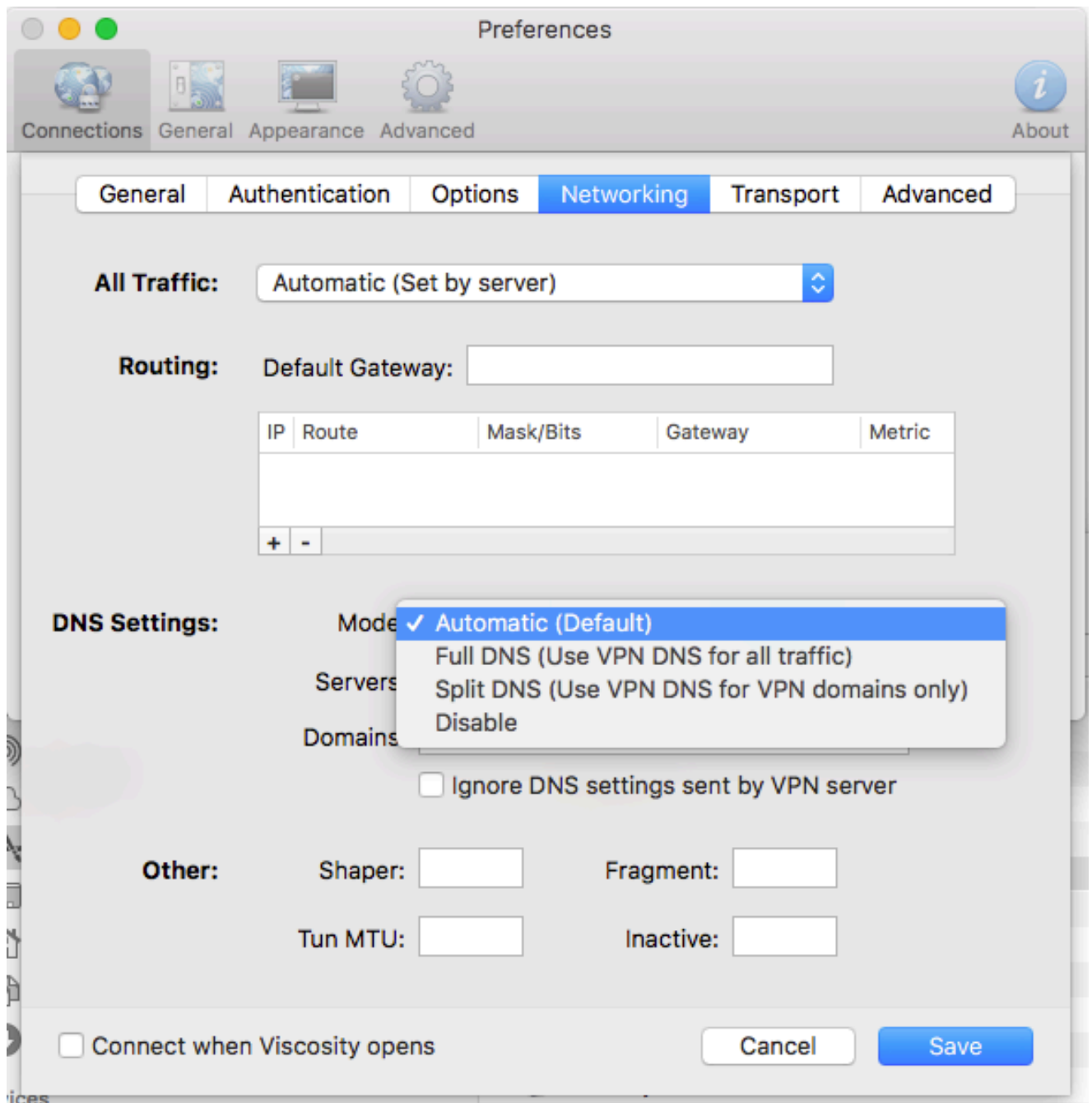
360031250911

Viscosity VPN

Viscosity VPN requires a change in settings to work with the Umbrella roaming client. If this change is not made, Viscosity default behavior mimics that of other incompatible VPNs. This change instructs Viscosity to use the DNS settings pushed via the Umbrella server for all domains in the search domain, and 127.0.0.1 continues to be used for any other requests.

Configure Viscosity

1. In Viscosity, navigate to **Preferences > Connections > <your connection> (site specific) > Networking > DNS Settings**.
2. Select **Automatic (Default)**.



115013433283

When using an OpenVPN server, ensure that **persist-tun** is not enabled server-side to ensure network changes trigger on disconnect or reconnect.

Tunnelblick

Tunnelblick requires two changes to:

- Allow changing of the DNS servers for the adapter.
- Apply DNS settings after the tunnel establishes.

By ensuring the provided settings in the **Advanced** menu, Tunnelblick functions with the Umbrella Roaming Client:

In the **Connecting and Disconnecting tab**, enable these two settings:

- Flush DNS cache after connecting or disconnecting (default)
- Set DNS after routes are set instead of before routes are set

In the **While Connected** tab, change this setting to **Ignore**:

- DNS: Servers > **When changes to the pre-VPN value, When changes to anything else.**

When using an OpenVPN server, ensure that **persist-tun** is not enabled server-side to ensure that network changes trigger on disconnect or reconnect.

Tunnelblick VPN Disconnect Issues

With some Tunnelblick versions, the Roaming Client cannot properly identify the correct Internal DNS servers after a VPN Disconnect. If problems with **Internal Domains** occur after a VPN disconnect, Umbrella recommends these steps:

This change causes Tunnelblick to bring the primary network interface down and up after the VPN disconnect. This is managed on the **Settings** tab of the Tunnelblick configuration panel:

- In older versions of Tunnelblick (prior to 3.7.5beta03), use the **Reset the primary interface after disconnecting** checkbox.
- On newer versions of Tunnelblick (3.7.5beta03 and higher), set both the **On expected disconnect** and the **On unexpected disconnect** settings to **Reset Primary Interface**.

Lightspeed Rocket

Lightspeed Rocket has select features that are not compatible with the Roaming Client. Specifically, the DNS modification for **No SSL Search** and **SafeSearch** CNAME redirection of www.google.com to nossllsearch.google.com and forcesafesearch.com respectively causes all www.google.com DNS resolution to fail as long as Lightspeed Rocket DNS redirection is enabled.



Note: This article refers to the standalone Umbrella Roaming Client. For a companion article on the Umbrella Roaming Security Module for Cisco Secure Client and legacy software, refer to the relevant documentation.
