

Configure Umbrella Roaming Client on a Company Network

Contents

[Introduction](#)

[Overview](#)

[Goals](#)

[Operating Modes](#)

[Using the Umbrella Roaming Client with an Umbrella Virtual Appliance](#)

[Cisco Umbrella AnyConnect Roaming Security Module](#)

[More Information](#)

Introduction

This document describes the configuration of the Umbrella roaming client on your company network.

Overview

The Umbrella roaming client is a great tool for protecting remote users but it can also protect users on your corporate network, adding another layer of security. Depending on the needs of the business some admins want the continued protection of the Umbrella roaming client on the corporate network, whereas other admins prefer to have the Umbrella roaming client 'back off' in favor of other Umbrella policies.

Umbrella offers flexibility on how the Umbrella roaming client operates when it enters your network. This article outlines these different approaches.

Goals

Q). Why would I disable the Umbrella roaming client on my company network?

There is normally no need to disable the Umbrella roaming client to have internal and external DNS work. The Umbrella roaming client uses the [Domain Management](#) feature to direct your internal DNS traffic to your normal DNS servers. This allows you to retain both protection and connectivity while the Umbrella roaming client runs on your endpoints on the network.

However, there are sometimes reasons to consider disabling the Roaming Client protection...

- To provide a different '*on-network*' and '*off-network*' policy to roaming users who leave the network.
- Using an internal DNS server on a company network offers some benefits in terms of caching and reduced outgoing DNS traffic.
- The Umbrella roaming client periodically sends [probe messages](#) to verify the connection to Umbrella. This additional traffic may be unwanted when you have a very large number of clients.

Q) Why would I want the Umbrella roaming client to remain enabled on my company network?

On the other hand, there are some very good reasons to keep the roaming client enabled at all times:

- Ensure the Umbrella roaming client computer uses the same policy at all times.
- Always having the Umbrella roaming client's hostname identifiable in reports (instead of the network identity) - for granular reporting.
- The Roaming Client uses 'Encrypted DNS' traffic for enhanced privacy
- For Secure Web gateway users (using AnyConnect) the client must remain enabled to provide SWG web filtering.

Operating Modes

Always ON

The Umbrella roaming client can remain on even when used on the company network. In this mode, policies are configured using the Umbrella roaming client Identity, and this Identity appears in reports.


Policy	The Umbrella roaming client Identity is used always.
Reporting	The Umbrella roaming client Identity always appears in reports offering per-machine granularity
DNS Traffic	<ul style="list-style-type: none">• The Umbrella roaming client continues to send DNS queries directly to Umbrella, even when on a company network.• Queries sent to Umbrella are encrypted, providing additional security.• Queries for 'Internal Domains' are routed to your normal DNS servers and not sent to Umbrella.
Probe Messages	The Umbrella roaming client continues to send probe messages to determine the availability of Umbrella.

How to configure the '**Always ON**' mode:

1. Navigate to **Identities > Roaming Computers**.
2. Click the **(Roaming client settings)** icon.
3. Clear **Disable DNS redirection while on an Umbrella Protected Network** and click **Save**.
4. Create a separate policy for your Umbrella roaming clients and ensure that it is the highest priority (the very top of the list). Your Umbrella roaming client policy must be at a higher precedence than any policies based on Network Identities.

Use Regular Network Policy

The Umbrella roaming client is enabled and continues to talk directly to Umbrella, however, the Network Identity is used for both policy and reporting purposes. This mode is activated simply by placing the network policy at a higher precedence than the Umbrella roaming client policy.

Policy	The network policy is used when on the protected network. This allows for different on/off network policies.
Reporting	<ul style="list-style-type: none"> Reporting is associated with the Network Identity as the primary identity. Reporting still allows you to search via Umbrella roaming client hostname to filter results for that client only. 
DNS Traffic	<ul style="list-style-type: none"> The Umbrella roaming client continues to send DNS queries directly to Umbrella, even when on a company network. Queries sent to Umbrella are encrypted, providing additional security. Queries for 'Internal Domains' are routed to your normal DNS servers and not sent to Umbrella.
Probe Messages	The Umbrella roaming client continues to send probe messages to determine the availability of Umbrella.

How to 'Use Regular Network Policy':

1. Navigate to **Identities > Roaming Computers**.
2. Click the **(Roaming client settings)** icon.
3. Clear **Disable DNS redirection while on an Umbrella Protected Network** and click **Save**.
4. Create a separate policy for your Network(s). Ensure the policy for your Network(s) is at a higher precedence than any policies based on the Roaming Client.

Disable behind Protected Networks (Ideal for smaller networks)

The Umbrella roaming client can 'back-off' when it detects that it is on a protected network. This means that Network Identity is used for both policy and reporting purposes.

This mode is similar in behavior to the 'Use Regular Network Policy' mode except that the Umbrella roaming client actually disables itself and does not interfere with DNS traffic.

Policy	The network policy is used when on the protected network. This allows for different on/off network policies.
Reporting	When on the protected network there is no per-machine granularity to the reporting. Reporting is associated with the Network Identity only.
DNS Traffic	When on the protected network the Umbrella roaming client does not interfere with DNS queries and they go to the normal internal DNS server.
Probe Messages	The Umbrella roaming client continues to send probe messages to determine that it is on a protected network.

How to configure **Disable behind protected networks**:

1. Navigate to **Identities > Roaming Computers**.
2. Click the **(Roaming client settings)** icon.
3. Select **Disable DNS redirection while on an Umbrella Protected Network** and click **Save**.
4. Navigate to **Policies > Policies List**.
5. Create a separate policy for your Network(s). Ensure the policy for your Network(s) is at a higher precedence than any policies based on the Umbrella roaming client.
6. Your local DNS servers must be forwarding to Umbrella resolvers and must be correctly registered in the Umbrella dashboard.
7. For this feature to work, the egress IP used by the client workstation must be registered to the same network identity as the egress IP used by your internal DNS servers. For full details, see [this article](#).

Disable behind trusted network domain (ideal for larger networks)

It is now possible to choose a customer-configured 'Trusted Network Domain'. The client attempts to resolve this DNS Domain (A record) and disable protection when the domain resolves successfully. This is intended to be an internal-only DNS record that only resolves when the client is on the company network.

Policy	The client backs-off whenever the Trusted Domain is detected and does not necessarily receive Umbrella policy or filtering. We would recommend to add other Umbrella features (eg. Network protection) to ensure policy is still applied on the company network.
---------------	--

Reporting	The client backs-off whenever the Trusted Domain is detected and does not necessarily receive Umbrella policy or filtering. If the network is protected by other Umbrella features (eg. Network protection) then traffic appears in reports under the network identity.
DNS Traffic	When on the trusted network the Umbrella roaming client does not interfere with DNS queries and they go to the normal internal DNS server.
Probe Messages	The Umbrella roaming client disables the majority of its DNS 'probe' tests in this state, greatly reducing the amount of traffic generated by Roaming Clients.

How to configure **Trusted Network Domain**:

1. Create a DNS A record on your internal DNS servers (eg. magic.mydomain.tld).
 1. The record must be a "sub-domain" (3 DNS labels minimum)
 2. The record must resolve to an internal RFC-1918 address
 3. Take care to ensure the record does not exist publicly
2. Navigate to **Identities > Roaming Computers**.
3. Click the **(Roaming client settings)** icon.
4. Select **Trusted Network Domain** option and enter the domain name (eg. magic.mydomain.tld).
Click **Save**.


Using the Umbrella Roaming Client with an Umbrella Virtual Appliance

As part of the Umbrella 'Insights' product ([in the Platform and Insights packages](#)) we provide a [Virtual Appliance](#) (VA) which acts as a DNS forwarder within your network. This VA is the key to gaining visibility about the source of DNS requests on your network and is also required for our Active Directory integration.

By Default, The Umbrella roaming client **disables itself** if it detects that a VA is being used for DNS forwarding. If the VA has been assigned as the DNS server (either using DHCP or static settings) then the Umbrella roaming client detects this and disable itself.

VA Backoff

Policy	<p>With VA Backoff enabled, the VA Identity is used to decide the chosen policy. Policies can be created based on these Identities:</p> <ul style="list-style-type: none"> • AD User (only if AD integration is enabled) • AD Computer (only if AD integration is enabled) • Internal Network
---------------	--

	<ul style="list-style-type: none"> • Umbrella Site Name. <p>Click here for more information on policy precedence.</p>
Reporting	<p>With VA Backoff enabled the Umbrella roaming client is disabled when behind a VA and is not be shown in reports. Reporting is logged as either:</p> <ul style="list-style-type: none"> • AD User (only if AD integration is enabled) • AD Computer (only if AD integration is enabled) • Internal Network • Umbrella Site Name. <p>In addition, the internal client IP address is logged for each request.</p> 
DNS Traffic	<ul style="list-style-type: none"> • The Umbrella roaming client does not interfere with DNS queries and they go to the virtual appliance. • The VA forwards external DNS queries to Umbrella (encrypted). • The VA routes internal DNS queries as appropriate and forwards them to the configured internal DNS servers.
Probe Messages	<p>The Umbrella roaming client still sends probe messages to Umbrella but does so at a reduced rate.</p>

How to configure **VA Backoff**:

1. This feature is enabled by default but you can check its status (and optionally disable it)
2. Navigate to **Identities > Roaming Computers**.
3. Click the **(Roaming client settings)** icon.
4. Select **VA Backoff** option

Cisco Umbrella AnyConnect Roaming Security Module

The Umbrella module for Cisco AnyConnect supports all the same operating modes as described above. Two additional AnyConnect specific modes are also available. Both of these modes can be enabled in your Umbrella Dashboard on the **Identities > Roaming Computers** page, however, additional configuration is required within the AnyConnect VPN profile.

- **Respect AnyConnect Trusted Network Detection.**
This feature causes the Umbrella Security module to disable when Cisco AnyConnect determines it is on a Trusted Network. This relies on AnyConnect's *Trusted Network Detection* feature to identify the network. Trusted domains, DNS servers, and URLs can be used to identify your company network. For more information please see the [AnyConnect documentation](#).
- **Disable Roaming Client while full-tunnel VPN sessions are active**
With this feature enabled, the Umbrella module is disabled when AnyConnect is connected to a Full

Tunnel (or Tunnel All DNS) VPN.

When disabled the Roaming Client does not filter DNS traffic, so it is important to ensure that your network is covered by other security like our Network Protection feature.

More Information

If you wish to disable the Roaming Client on your company network but need more control, or wish to discuss other options, please contact Cisco Umbrella support.