

Umbrella Roaming Security

The Umbrella Roaming Security module requires a subscription to a Umbrella Roaming Security service with either the DNS Security Essentials, DNS Security Advantage, SIG Essentials, or SIG Advantage. Umbrella Roaming Security provides DNS-layer security when no VPN is active, and a Cisco Umbrella subscription adds Intelligent Proxy. Additionally, Cisco Umbrella subscriptions provide content filtering, multiple policies, robust reporting, active directory integration, and much more. The same Umbrella Roaming Security module is used regardless of the subscription.

The Umbrella Roaming Security module profile (OrgInfo.json) associates each deployment with the corresponding service, and the corresponding protection features are enabled automatically.

The Umbrella Dashboard provides real-time visibility into all of the Internet activity originating from the Umbrella Roaming Security module. The level of granularity in policies and reports depends on the Umbrella subscription.

Refer to https://umbrella.cisco.com/products/packages for a detailed comparison of which features are included in which service level subscriptions.

- Umbrella Module for Cisco Secure Client (for Android OS), on page 1
- Umbrella Module for Cisco Secure Client (for Windows or macOS), on page 2

Umbrella Module for Cisco Secure Client (for Android OS)

The Umbrella Module for Cisco Secure Client for Android OS is a roaming client for managed Android devices that provides DNS-layer protection, and this protection extends to both apps and browsing covered by the Android work profile.

A mobile device management system (MDM) is required to deploy this client to Android devices and to push the Umbrella configuration to the Android devices. For a list of supported MDMs and other prerequisites, see Prerequisites for Deploying the Umbrella Module for AnyConnect on Android OS.

Some Cisco Secure Client features may have limitations in functionality with Umbrella on Android:

- Per-app VPN does not work with the Umbrella Module because of an OS restrictions. If remote access VPN is active, Umbrella protection will only apply to DNS traffic that is intercepted by the VPN tunneled. If remote access is configured for per-app VPN, Umbrella protection only applies to DNS traffic for the tunneled applications.
- You should not use always-on VPN with the lockdown (Fail Close) option. It stops the internet access when the VPN server is not reachable. Refer to your MDM guide to turn off the lockdown setting when always-on VPN is set to On.

For an explanation of the complete Umbrella feature set, refer to the Umbrella Module for AnyConnect (Android OS) documentation.

Prerequisites for Deploying the Umbrella Module for Cisco Secure Client on Android OS



Note Cisco Secure Client monitors traffic generated from apps and browsers within the work profile created in an MDM and blocks or allows browsing accordingly. Any traffic generated outside the work profile by apps and/or browsers is not monitored.

- Mobile device management system (MDMs) for deploying the software and pushing the Umbrella configuration to the mobile devices. Current tested versions are Mobile Iron, Meraki, VMWare workspace 1 (Airwatch), or Microsoft Intune.
- Android (Samsung/Google Pixel) mobile devices with Android OS version 6.0.1 and above.
- Umbrella license to configure DNS policies, manage registered Android devices, and for reporting.
- Umbrella organization ID for enabling the feature.
- For Trusted Network Detection (TND):
  - If the Umbrella module detects a virtual appliance (VA) with HTTPS enabled, it deactivates itself; however, if the VA does not support HTTPS, the Umbrella module continues.
  - All VA FQDN in umbrella_va_fqdns must be enabled.

Umbrella Module for Cisco Secure Client (for Windows or macOS)

Obtain Cisco Umbrella Account

The Umbrella dashboard (http://dashboard.umbrella.com/) is the login page where you can obtain the profile (OrgInfo.json) for the Umbrella Roaming Security module to include in your deployment. From there you can also manage policy and reporting for the activity of the roaming client.

Download the OrgInfo File From Dashboard

The OrgInfo.json file is specific information about your Umbrella dashboard instance that lets the Umbrella Roaming Security module know where to report and which policies to enforce.

You must obtain the OrgInfo.json file from the Umbrella dashboard (http://dashboard.umbrella.com/) .

Click on **Roaming Computers** in the Identities menu structure and then click the + sign in the upper-left corner of the page. Scroll down to Umbrella Roaming Security Module and click **Module Profile**. Refer to

the Cisco Secure Client Deployment Overview for specific installation/deployment steps and package and file specifics.



Note When you deploy the OrgInfo.json file for the first time, it is copied to the data subdirectory (/umbrella/data), where several other registration files are also created. Therefore, if you need to deploy a replacement OrgInfo.json file, the data subdirectory must be deleted. Alternatively, you can uninstall the Umbrella Roaming Security module (which deletes the data subdirectory) and reinstall with the new OrgInfo.json file.

Get Umbrella Roaming Security Up and Running

When you deploy Cisco Secure Client, the Umbrella Roaming Security module is one of the optional modules that you can include to enable extra features.

To interpret the status and conditions of the Umbrella Roaming Security Module, refer to The AnyConnect Plugin: Umbrella Roaming Security Client Administrator Guide.

Configure the OrgInfo.json File

The OrgInfo.json file contains specific information about your Umbrella service subscription that lets the Umbrella Roaming Security module know where to report and which policies to enforce. You can deploy the OrgInfo.json file and enable the Umbrella Roaming Security module from the Secure Firewall ASA or ISE using CLI or GUI. The steps below describe how to enable from the Secure Firewall ASA first and then how to enable from ISE:

Secure Firewall ASA CLI

1. Upload the OrgInfo.json that you obtained from the Umbrella dashboard (https://dashboard.umbrella.com) to the Secure Firewall ASA file system.
2. Issue the following commands, adjusting the group-policy name as appropriate for your configuration.

```
webvpn
 anyconnect profiles OrgInfo disk0:/OrgInfo.json

group-policy DfltGrpPolicy attribute
 webvpn
  anyconnect profiles value OrgInfo type umbrella
```

ASDM GUI

1. Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
2. Choose **Add**.
3. Give the profile a name.
4. Choose the Umbrella Security Roaming Client type from the Profile Usage drop-down menu. The OrgInfo.json file populates in the Profile Location field.
5. Click **Upload** and browse to the location of the OrgInfo.json file that you downloaded from the dashboard.

6. Associate it with the DfltGrpPolicy at the Group Policy drop-down menu. Refer to Enable Additional Cisco Secure Client Modules to specify the new module name in the group-policy.

ISE

Follow these steps to enable from ISE:

1. Upload the OrgInfo.json from the Umbrella dashboard https://dashboard.umbrella.com.
2. Rename the file OrgInfo.xml.
3. Follow steps in Configure ISE to Deploy Cisco Secure Client.

Configure Security Policies and Review the Reports

You must have a Cisco Umbrella account to receive protection, see reporting information, and configure policies. For in-depth explanations, visit https://docs.umbrella.com/product/umbrella/ or https://support.umbrella.com for additional information.

After installation, the Roaming Computer is visible in your Umbrella Dashboard within 90 minutes to 2 hours. Navigating and authenticating to https://dashboard.umbrella.com and then going to **Identities > Roaming Computers** shows a list of Roaming Clients (both active and inactive), as well as details about each installed client.

Initially, a default policy with a base level of security filtering is applied to your Roaming Computers. This Default Policy is found in the Policies section of the dashboard (or Configuration > Policy for Cisco Umbrella accounts).

Reporting for the Roaming Clients is found under the Reports section. Check the Activity Search report to see DNS traffic from computers with the Umbrella Roaming Security module installed and the VPN turned off.

Interpret Diagnostics

You should run a DART report to diagnose any Umbrella Roaming Security module issues. Refer here for instructions on how to run. Refer to Cisco Umbrella Troubleshooting for Umbrella concerns and troubleshooting details.

SWG Debug Logging

By copying an SWGConfigOverride.json file into the SWG folder, you can enable debug logging. If there is a value present for SWGConfig.json, the configuration value in SWGConfigOverride.json will override its log level {"logLevel":"1"} and autotuning {"authtuning:"1"} configurations. The locations of the SWG folder are as follows:

- Windows (Secure Client)— C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG
- macOS (Secure Client)— /opt/cisco/secureclient/umbrella/swg

You will need to restart the SWG service (or Umbrella service) after the override file is copied.

After you have copied the SWGConfigOverride.json file to the appropriate SWG folder, do the following to enable debug logging:

- For macOS—Refer to https://support.umbrella.com/hc/en-us/articles/230561067#Roaming-Client-for-OS-X5 for steps to stop and start the Secure Client agent.
- For Windows—Restart, or stop and start, the Secure Web Gateway (acswgagent in 4.10.x builds /csc_swgagent in 5.x builds) service via the Services MMC snap-in (Start > Run > Services.msc).

Umbrella Roaming Security Module

While the Umbrella Roaming Security module provides DNS layer security, the Cisco Secure Client Umbrella Secure Web Gateway (SWG) Agent module provides a level of security on the endpoint that increases flexibility and potential for more deployment scenarios. Umbrella Secure Web Gateway allows you to authenticate and redirect web traffic securely in both off prem and on prem scenarios. This implementation requires a SIG Essentials or SIG add-on subscription from Umbrella.

The Secure Web Gateway client inserts encrypted headers into HTTP requests, and the headend extracts the header, decrypts it, and uses its user data for identity and policy determination and enforcement. Similarly, for HTTPS traffic, the Secure Web Gateway client initiates HTTP connect requests with the SWG headend, and the connect request carries encrypted headers, which are extracted, decrypted, and used for the identity/policies determination and enforcement.

By default, Secure Web Gateway intercepts HTTP or HTTPS traffic on ports 80 and 443. You can add non-standard ports (beyond 80 and 443) with Umbrella Cloud configuration. When it is configured, Secure Web Gateway listens for HTTP/HTTPS traffic on these additional ports in addition to the default standard ports.

With Trusted Network Detection, users can choose to inactivate Secure Web Gateway when on a trusted network. When this setting is configured in the Umbrella Cloud, the Secure Web Gateway functionality is disabled if on a trusted network when an AnyConnect VPN tunnel state is active. The Web Protection Status shown in the UI Statistics window reflects any change in the state.



Note Configuring this setting also inactivates Secure Web Gateway in the case of certain errors (such as when the Umbrella Resolvers are unreachable), which are determined by Umbrella's DNS protection state.

Any domain or IP address that should not be proxied can be defined in the Umbrella dashboard under Deployments > Domain Management. Wildcards are not supported, but Umbrella will match any subdomain belonging to a parent domain; for example, if example.com is entered into the domain management list, then www.example.com will also match and be bypassed. You enter IP addresses in the Classless Inter-Domain Routing (CIDR) notation.

If Cisco Secure Client cannot open a connection to an Umbrella proxy, Cisco Secure Client fails open by default, allowing direct access to the user. You cannot configure this hard-coded behavior.

Refer to the Cisco Umbrella SIG User Guide for additional information on all of these Umbrella UI configurations.

Limitations of Secure Web Gateway

- In scenarios where the local host with Cisco Secure Client installed is also configured with a proxy auto-configuration (PAC) file, the PAC file takes priority over Cisco Secure Client.
- Local proxies are not supported.

- After installation, it may take up to 50 minutes for the Umbrella Secure Web Gateway Agent to synchronize with the Umbrella cloud and receive its configuration. However, the default web policy should apply until the synchronization occurs.

Installation and Upgrade for Umbrella SWG

The Cisco Secure Client Umbrella Secure Web Gateway module is available for Windows or macOS only. You have the option to disable VPN functionality and hide the VPN tile on Secure Client's UI. If the AnyConnect VPN is installed with the Cisco Secure Client Umbrella Secure Web Gateway Agent, you must enable the *AllowLocalProxyConnections* setting in the VPN profile.

Both predeploy and web deploy over Secure Firewall ASA or ISE are supported.

Umbrella SWG Log Files and Messages

Umbrella sends the configuration information to the Cisco Secure Client SWG module in the form of a SWGConfig.json file. The config file SWGConfig.json is stored in the following locations:

- Windows—C:\ProgramData (x86)\Cisco\Cisco Secure Client\Umbrella\SWG
- macOS—/opt/cisco/secureclient/umbrella/swg/

Status in Umbrella Roaming Security Tile

You can verify the state of Secure Web Gateway in the Advanced Statistics window. In the Umbrella Roaming Security tile of that window, the Web Protection Status indicates one of the following:

- Disabled—the Umbrella service is down
- Protected—cscswgagent is running
- Unprotected—cscswgagent is not running
- Config Error—incorrect value in SWGConfig.json
- Cloud Service Unavailable—Umbrella proxy not reachable
- Disabled (VPN Connection)—If the endpoint is connected to a full-tunnel VPN, a "disabled due to vpn" message will be sent, and SWG will be disabled with this status.
- Disabled (Trusted Network)—If the endpoint is connected to Secure Client or a customer-trusted network, a "disabled due to a trusted network" will be sent by the SWG Agent, and SWG will be disabled with this status.

For detailed statistics on the Umbrella Secure Web Gateway Agent, open the Cisco Secure Client UI and navigate to the Umbrella Roaming Security branch to see the number of HTTP requests redirected to the umbrella proxy, the number of HTTPS requests redirected to the umbrella proxy, the number of requests that we were unable to redirect to proxy, and the Umbrella proxy Cisco Secure Client connected to. Errors and informative messages are logged in the message history.

Troubleshooting Umbrella Secure Web Gateway

When you run a DART bundle, it will include the SWGConfig.json and SWG-related logs if you have Cisco Secure Client Umbrella Roaming Secure Module checked on the Log File Selection window. Go to

http://httpbin.org/ip to check if traffic is getting to an Umbrella proxy. If you encounter a connection reset, send an HTTP request to see the response code:

- If the HTTP response code is 452, check if the client's clock is synchronized or if the timestamp is incorrect. A malicious user could be trying to replay the headers.
- If the HTTP response code is 401, the keys are not current. Check the last synchronization time for the device on the Umbrella dashboard.