Umbrella Roaming Security

The Umbrella Roaming Security module requires a subscription to a Cisco Umbrella Roaming service with either the Professional, Insights, Platform, or MSP package. Cisco Umbrella Roaming 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 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 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 AnyConnect for Windows or macOS, on page 1

Umbrella Module for AnyConnect for Windows or macOS

Umbrella Roaming Client and Umbrella Roaming Security Module Incompatibility

The Umbrella Roaming Security module and the Umbrella Roaming Client are incompatible. If you are deploying the Umbrella Roaming Security module, any existing installation of the Umbrella Roaming Client will be detected and removed automatically during installation of the Roaming Security module to prevent conflicts. If the existing installation of the Umbrella Roaming Client is associated with an Umbrella service subscription, it will automatically be migrated to the Umbrella Roaming Security module *unless* an OrgInfo.json file is co-located with the AnyConnect installer, configured for web-deployment or predeployed in the Umbrella module's directory. You may also wish to manually uninstall the Umbrella Roaming Client prior to deploying the Umbrella Roaming Security module.

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 AnyConnect 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 Roaming Security module know where to report and which policies to enforce.

To prepare for deploying the Umbrella Roaming Security module, you must obtain the OrgInfo.json file from the Umbrella dashboard (https://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 AnyConnect Umbrella Roaming Security Module and click **Module Profile**. Refer to the AnyConnect 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 AnyConnect, 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 Security Module, refer to The AnyConnect Plugin: Umbrella Roaming Security Client Administrator Guide.

For Windows 7 SP1 users, we recommend that you install Microsoft .NET framework 4.0 before installation or initial use. At startup, the Umbrella service checks if .NET framework 4.0 (or newer) is installed. If it is not detected, the Umbrella Roaming Security module is not activated, and a message is displayed. To go and then install the .NET Framework, you must reboot to activate the Umbrella Roaming Security module.

Configure the OrgInfo.json File

The OrgInfo.json file contains specific information about your Umbrella service subscription that lets the Security Roaming 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 ASA or ISE using CLI or GUI. The steps below describe how to enable from the ASA first and then how to enable from ISE:

ASA CLI

1. Upload the OrgInfo.json that you obtained from the Umbrella dashboard (https://dashboard.umbrella.com) to the 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 AnyConnect 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 AnyConnect.

Cloud Update

The Umbrella Roaming Security module can provide automatic updates for all installed AnyConnect modules from the Umbrella Cloud infrastructure. With Cloud Update, the software upgrades are obtained automatically from the Umbrella Cloud infrastructure, and the update track is dependent upon that and not any action of the administrator.

By default, automatic updates from Cloud Update are disabled. To enable Cloud Updating for Umbrella Roaming Security and the rest of AnyConnect, log in to the Umbrella Dashboard. Under the **Identities > Roaming Computers>** Settings icon (the gear icon), check **Automatically update AnyConnect, including VPN module, whenever new versions are released.** Updates will not occur while VPN is active. By default, this option is unselected.

Consider the following regarding Cloud Update:

- Only the software modules that are currently installed are updated.
- Customizations, localizations, and any other deployment types are not supported.
- The updates occur only when logged in to a desktop and will not happen if a VPN is established.
- With updates disabled, the latest software features and updates will not be available.
- Disabling Cloud Update has no effect on other update mechanisms or settings (such as web-deploy, deferred updates, and so on).

- Cloud Update ignores devices having newer, unreleased versions of AnyConnect (such as interim releases and patched versions).

Configure Security Policies and Review the Reports

You must have a Cisco Umbrella Roaming 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 Cisco Umbrella Roaming Security module issues. Refer to https://docs.umbrella.com/umbrella-user-guide/docs/appendix-c-troubleshooting for Umbrella concerns and troubleshooting details.