Securely Connecting Customers to the Cisco Secure Internet Gateway (SIG)

Managing Umbrella with Cisco Defense Orchestrator

Umbrella is Cisco's cloud-based Secure Internet Gateway (SIG) platform that provides you with multiple levels of defense against internet-based threats. Umbrella integrates secure web gateway, firewall, DNS-layer security, and cloud access security broker (CASB) functionality to protect your systems against threats. By utilizing SIG and DNS protection, the ASA devices are protected with both the local DNS inspection policy on your device and the Umbrella cloud-based DNS inspection policy. By providing several ways to inspect and detect incoming traffic, Umbrella makes the ASA device comparable to FTD next-generation firewall (NGFW).

At this time, CDO only supports ASA integration with an Umbrella organization.

Build a Bridge with SASE

Secure Access Service Edge (SASE) is a forward-thinking framework in which networking and security functions converge into a single integrated service that works at the cloud edge to deliver protection and performance. This effort provides a way to consolidate services safely and securely, regardless of your location, and allows you to control and manager your network no matter the size of your organization. Reduced complexity and an agile take of management means your deployments are simple, scalable, and and secure.

What is an Umbrella Organization?

An Umbrella organization is a group of users with varying user roles that are associated with a single license key; a single user can have access to multiple Umbrella organizations. Every Umbrella organization is a separate instance of Umbrella and has its own dashboard. Organizations are identified by their name and their organization ID (Org ID). The Org ID is used to identify your organization for deploying components such as virtual appliances, and sometimes support may request your Org ID.

What is a SIG Tunnel?

A Secure Internet Gateway (SIG) tunnel is an instance of a SIG IPSec (Internet Protocol Security) tunnel that occurs between the ASA and Umbrella, where all internet-bound traffic is forwarded to Umbrella SIG for

inspection and filtering. This solution provides centralized management for security so network administrators do not have to separately manage security settings for each branch.

When you onboard an Umbrella organization that has tunnels configured, these tunnels are listed in CDO's Site-to-site VPN page. To create a SASE tunnel for your Umbrella organization from the CDO UI, see Configure a SASE Tunnel for Umbrella.

Note If you onboard an Umbrella organization and its peer devices, the Site-to-site VPN page combines all the devices to the tunnel associated with that organization into a single entry. To manually refresh the Tunnels page and read in any changes made from the Umbrella dashboard, see Read Umbrella Tunnel Configuration.

How does CDO Communicate with Umbrella?

You must onboard the Umbrella organization as well as any ASA devices associated with the organization.

When an ASA device is associated with an Umbrella cloud, the connection requires a site-to-site VPN SIG tunnel to create a secure connection between the device and the cloud. CDO communicates with both the Umbrella organization and the ASA devices. This dual-communication method allows CDO to instantly detect changes in configuration or tunnel changes, and immediately alert you to an out-of-bound changes, errors, or unhealthy states for Umbrella, the ASA, and the tunnels.

When you onboard an Umbrella organization to CDO, you onboard with the organization's API key and Secret, both of which are unique to the organization and the ASA devices associated with that organization. CDO communicates to the Umbrella cloud with the Umbrella API, using the API key and Secret used to onboard the organization to request and send information about the ASA devices. This level of communication does not compromise the SIG tunnel that exists between the ASA and the Umbrella cloud.

Once an Umbrella organization is onboarded, the **Inventory** page displays any detected ASA devices associated with the org as "peers", and notes whether the devices are onboarded to CDO or not. If a peer device is not already onboarded, you have the option to onboard directly from that page by clicking Onboard Device. When an ASA device that is associated with an Umbrella organization is onboarded to CDO, the **Inventory** page displays the relationship and the VPN Tunnels page shows the tunnels between the device and the organization. If an ASA device that is associated with an organization is not onboarded to CDO, the tunnels associated with the device are displayed in the VPN Tunnels and you can opt to onboard the device directly from this page.

How do I access the Umbrella Cloud from CDO?

Once the Umbrella organization is successfully onboarded onto CDO, you can cross-launch to the organization's dashboard or to the Umbrella Tunnels page from the CDO UI.

See Cross-launch to the Umbrella dashboard, on page 6 and Cross-launch to the Umbrella Tunnels Page, on page 8 to access the Umbrella Cloud from the CDO UI.

Prerequisites

Supported Hardware and Software

Umbrella organizations are cloud-based and thusly version-less. Note that when you onboard an Umbrella organization to CDO, you are only able to associate that organization with an ASA device.

For Umbrella integration, CDO supports ASA devices running 9.1.2 and later. See Cloud Device Support Specifics for a list of ASA device models and software that CDO supports.

Licensing Requirements

In order to successfully onboard an Umbrella organization to CDO, you must have one of the following license packages selected:

- Umbrella SIG Essentials
- SIG Advantage

Onboarding

To successfully manage an Umbrella account, you must onboard both the Onboarding an Umbrella Orgnization and the ASA devices associated with it. Once you onboard an Umbrella organization, CDO reads any existing ASA tunnels associated with the organization and monitor the health status of these tunnels as well as any additional tunnels you create and associate with the organization. Before you onboard an Umbrella organization, review the general device requirements and onboarding prerequisites.

If you happen to onboard an Umbrella organization before onboarding any ASA devices associated with it, you can view the ASA peer from the **Site-to-site VPN** page and onboard the device from the VPN page.

Note If you have an ASA pair configured for failover, you must **only** onboard the active device of the two peers. Onboarding both the active and the standby devices to CDO may generate duplicate tunnel information for SASE tunnels that are already configured in Umbrella.

Monitoring Your Network

CDO provides reports summarizing the impact of your security policies and methods of viewing notable events triggered by those security policies. CDO also logs the changes you make to your devices and provides you with a way to label those changes so you can associate the work you commit in CDO with a help ticket or other operational request.

Change Log

The change log continuously captures configuration changes as they are made in CDO. This single view includes changes across all supported devices and services. Because Umbrella is a cloud-based product, changes are immediately deployed.

These are some of the features of the change log:

- Side-by-side comparison of changes made to device configuration.
- Plain-English labels for all change log entries.
- Records on-boarding and removal of devices.
- Detection of policy change conflicts occurring outside of CDO.
- Answers who, what, and when during an incident investigation or troubleshooting.
- The full change log, or only a portion, can be downloaded as a CSV file.

Note Note that when you create, edit, or delete a SASE tunnel associated with an Umbrella organization, the request and configuration changes appear for the Umbrella organization and any ASA device associated with it.

Umbrella Documentation

- Umbrella Help
- Umbrella and Cisco ASA Configuration
- Connect to Cisco Umbrella Through Tunnel
- Cisco Umbrella API

Onboarding an Umbrella Organization

Umbrella License Requirements

In order to successfully onboard an Umbrella organization to CDO, you must have one of the following license packages selected from the Umbrella dashboard:

- Umbrella SIG Essentials
- SIG Advantage

To verify the licenses that are currently enabled, log into the Umbrella dashboard and navigate to **Admin** > **Licensing**.

Generate an API Key and Secret

Generate a new API key and retrieve **both** the **API Key** and the corresponding **Secret** before you onboard an Umbrella organization to CDO.

If you do not currently have an API key, use the following procedure to create one:

Before you begin

The management API key from Umbrella is used for the following Umbrella services:

- Networks and Domains
- Network Tunnels
- Users and Roles
- Destination Lists
- Service Providers

You cannot onboard an Umbrella organization without allowing CDO access to these services.

Procedure

Step 1 Access the Cisco Umbrella dashboard and log into your organization.

Step 2 In the Umbrella dashboard, click **Admin** in the left navigation pane and select **API Keys**.

Step 3 Click **Create API Key**.

If you already have an API key but do not have the secret saved, navigate to the **Admin** > **API Keys**screen and click **Refresh** to update the key and secret.

Step 4 To create a new API key and Secret, click the + button.

Step 5 Enter a **Name** and add the following scopes to the API key:

- Deployments.
- Policies.

Step 6 Click **Generate Key**.

Step 7 Copy the API Key and the corresponding Secret. We recommend temporarily pasting it into a note or .txt file until you are ready to use it.

Umbrella Organization ID

You must use the Umrbrella organization's locate the organization ID and use that along with the login credentials to successfully onboard the organization to CDO:

Procedure

Step 1 Access the Cisco Umbrella dashboard and log into your organization/

Step 2 The page URL will contain a numeric identifier. For example, the Organization ID for https://dashboard.umbrella.com/o/**123456**/#/overview is **123456**.

Step 3 Copy the Organization ID from the URL. We recommend temporarily pasting it into a note until you are ready to use it.

Onboarding an Umbrella Orgnization

Use the following procedure to onboard an Umbrella organization to CDO:

Before you begin

Read the Umbrella License Requirements, on page 4 before you onboard this environment.

Procedure

Step 1 In the Umbrella dashboard, locate the Umbrella Organization ID, on page 5 and Generate an API Key and Secret, on page 4. Have these items available during this procedure.

Step 2 Log into CDO.

Step 3 In the navigation bar, click **Inventory**

Step 4 Click the blue plus button to begin onboarding the device.

Step 5 Click **Umbrella Organization**.

Step 6 Enter the Umbrella Network Device's **API Key** and corresponding **Secret** that you generated from the Umbrella dashboard, and the **Organization ID** from your Umbrella dashboard's URL.

Step 7 Click **Next**.

Step 8 (Optional) Add unique **Labels** for the device. You can later filter your list of devices by this label.

Step 9 Click **Go to Inventory**.

Reconnect an Umbrella Organization to CDO

Warning CDO cannot successfully deploy or read configuration changes to or from an Umbrella organization if the stored credentials are invalid, but CDO may successfully deploy or read changes from any ASA devices associated with the org. This may cause issues once the credentials are updated and validated. We recommend updating the organization credentials prior to deploying any configuration changes.

If the API key and secret to an Umbrella Organization has been refreshed or has timed out, you have to manually reconnect the Umbrella organization to CDO. Use the following procedure to reconnect:

Procedure

Step 1 Go to the Umbrella Dashboard. Click **Admin** in the left navigation pane and select the existing Umbrella Management **API Keys**.

Step 2 Click **Refresh**. Confirm that you want to refresh the API key and secret.

Step 3 Copy the API Key and the corresponding Secret.

Step 4 Log into CDO.

Step 5 Navigate to the **Inventory** page.

Step 6 Use to the filter or search bar to locate the Umbrella Organization.

Step 7 In the **Device Actions** pane, click **Reconnect**. CDO confirms the stored API Key and secret are no longer valid.

Step 8 Paste the API key and Secret into the appropriate pop-up window.

Step 9 Click **Continue**.

Step 10 Once CDO confirms the new key and secret are valid, click **Close**.

Cross-launch to the Umbrella dashboard

Once the ASA device and the Umbrella organization are successfully onboarded onto CDO, you can cross-launch to the organization's dashboard from the CDO UI.

Use the following procedure to cross-launch to your device's Umbrella dashboard:

Procedure

Step 1 Log into CDO.

Step 2 Click **Inventory**.

Step 3 Locate, or filter, for the Umbrella organization.

Step 4 Click **Manage Umbrella Organization** in the **Management** pane. CDO launched a new tab in your browser that opens to the Umbrella dashboard associated with the selected organization.

Delete a Device from CDO

Use the following procedure to delete a device from CDO:

Procedure

Step 1 Log into CDO.

Step 2 Navigate to the **Inventory** page.

Step 3 Locate the device you want to delete and check the device in the device row to select it.

Step 4 In the **Device Actions** panel located to the right, select **Remove**.

Step 5 When prompted, select **OK** to confirm the removal of the selected device. Select **Cancel** to keep the device onboarded.

Configure an Umbrella Organization

Read Umbrella Tunnel Configuration

Once an Umbrella organization is onboarded to CDO, you can manually force CDO to request and update the tunnels configuration from Umbrella. This includes tunnels that were added, deleted, or modified.

Warning If a tunnel is deleted from CDO while the Umbrella organization credentials are considered invalid, or have changed since you onboarded the organization, CDO can only deploy the tunnel configuration to the ASA devices associated with the organization. Upon updating the credentials, CDO reads the Umbrella configuration and repopulates any tunnels that were deleted. Due to the tunnel existing in the Umbrella organization but not any of the ASA devices, there will be a synchronization issue and the ASA devices may not appear as peers to organization.

Procedure

Step 1 Log into CDO.

Step 2 In the left pane, click **Inventory** > **Devices**.

Step 3 Click the **ASA** tab.

Step 4 Select the Umbrella organization so it is highlighted.

Step 5 Under **Actions**, select **Read Tunnels**.

Cross-launch to the Umbrella Tunnels Page

Once the ASA device and the Umbrella organization are successfully onboarded onto CDO, you can cross-launch to the Umbrellas dashboard for tunnels from the CDO UI.

Use the following procedure to cross-launch to your device's Umbrella tunnels page:

Procedure

Step 1 Log into CDO.

Step 2 Navigate to the VPN window. Select **Site-to-Site VPN**.

Step 3 Select the desired tunnel so it is highlighted.

Step 4 In the **Actions** pane, click **Manage Tunnel in Umbrella**. CDO launches a new tab in your browser that opens to the Tunnels overview page.

Configure a SASE Tunnel for Umbrella

Use the following procedure to create a SASE tunnel for an Umbrella organization:

Before you begin

Note that the Umbrella organization and the ASA device you want to create the tunnel for **must** already be onboarded to CDO.

If the ASA or Umbrella organization associated with the tunnel you just deployed is in an unhealthy state, CDO may not be able to successfully deploy the tunnel. If you experience any issues, contact Cisco TAC.

Procedure

Step 1 Log into CDO.

Step 2 Navigate to the **VPN** window. Select **Site-to-Site VPN**.

Step 3 Click the blue plus button and select **Create SASE Tunnel**.

Step 4 Enter the Umbrella Peer information:

- **Select Umbrella** - Select the **Umbrella** organization of your choice.
- **Datacenter** - Select a head-end datacenter. We recommend selecting a datacenter that is geographically close to the ASA associated with the Umbrella organization.

Step 5 Enter the ASA Peer information:

- **Select ASA Device** - Select an ASA device that is associated with the Umbrella organization from the drop-down list and then click **Select**.
- **Public Facing Interface** - Select an IPv4 address that is static and publicly routable. The address used should not be used for NAT.
- **LAN Address** - Select the LAN interfaces that controls the LAN subnet. You must select at least one interface for LAN.
- **Virtual Tunnel Interface** - This field is automatically filled once you select the Umbrella organization and the ASA peer device. If necessary, you can manually enter an IP address that will be used as the new VTI.

Step 6 The **Passphrase** is automatically filled once you select the Umbrella organization and the ASA peer device. The **Confirm Passphrase** is also automatically filled. You can manually enter these fields if necessary.

Step 7 (Optional) The **Deploy changes to ASA immediately** toggle at the bottom of the pop-up window is enabled by default. When enabled, the SASE tunnel configuration is immediately deployed to the ASA peer selected in the tunnel configuration. If you want to stage changes and deploy later, manually toggle the option to disable.

Step 8 Click **Deploy**. Optionally, click **Deploy and Create Another** to simultaneously deploy this SASE tunnel and create another tunnel. Once deployed, the tunnel will appear in the VPN Tunnels page. If you choose to **Deploy and Create Another SASE tunnel**, CDO saves both the Umbrella organization selection and the **Deploy changes to ASA immediately** toggle setting and automatically applies these selections to the next tunnel configuration. You can manually alter these selections prior to deploying.

Edit a SASE Tunnel

Use the following procedure to modify an existing SASE tunnel:

Procedure

Step 1 Log into CDO.

Step 2 Navigate to the **VPN** window. Select **Site-to-Site VPN**.

Step 3 Select the tunnel you want to modify.

Step 4 In the Actions pane, select **Edit**.

Step 5 Edit the following fields of the SASE tunnel:

- **Name** - Change the name of the SASE tunnel as it appears in CDO and the Umbrella dashboard.
- **Umbrella Peer's Datacenter** - Select a new head-end datacenter form the drop-down menu.
- **ASA Peer's Public Facing Interface** - Select a new IPv4 address from the drop-down menu.

- **ASA Peer's LAN Interfaces** - Select one or more new LAN interfaces from the drop-down menu.
- **ASA Virtual Tunnel Interface (VTI) Address** - Manually edit the VTI.
- **Passphrase** - Manually modify the passphrase for the tunnel.
- **Confirm Passphrase** - Manually modify this entry to match the passphrase and confirm the new value.

Step 6 (Optional) The **Deploy changes to ASA immediately** toggle at the bottom of the pop-up window is enabled by default. When enabled, the SASE tunnel configuration is immediately deployed to the ASA peer selected in the tunnel configuration. If you want to stage changes and deploy later, manually toggle the option to disable. If you opt to stage changes and deploy later, the ASA peer status in the **Inventory** page appears as `Deploy Pending`.

Step 7 Select **Save Updates**.

Delete a SASE Tunnel from Umbrella

Use the following procedure to delete a SASE tunnel on CDO:

Before you begin

To delete a SASE tunnel, the ASA associated with it must have a synced status in CDO. You cannot delete a tunnel if the device is uhealthy.

Note that if you delete a SASE tunnel from CDO, the tunnel is removed from both the ASA device and the Umbrella organization associated with it.

Warning If you delete a tunnel from CDO while the Umbrella organization credentials are considered invalid, or have changed since you onboarded the organization, CDO can only deploy the tunnel configuration to the ASA devices associated with the organization. Upon updating the credentials, CDO reads the Umbrella configuration and repopulates any tunnels that were deleted. Due to the tunnel existing in the Umbrella organization but not any of the ASA devices, there will be a synchronization issue and the ASA devices may not appear as peers to organization. We recommend confirming the Umbrella credentials prior to deleting any tunnels associated with the organization.

Procedure

Step 1 Log into CDO.

Step 2 In the left pane, click **VPN** > **Site-to-Site VPN**.

Step 3 Select the tunnel you want to delete from CDO.

Step 4 Under **Actions**, click **Delete**.

Step 5 Confirm you want to delete the tunnel and click **OK**.