

Cisco Umbrella and Meraki MR

Simple and effective protection for corporate and guest Wi-Fi

What if you could protect every user on your Meraki network in minutes and you could do it without an additional appliance? That's the magic of combining the Meraki MR wireless access points and Cisco Umbrella.

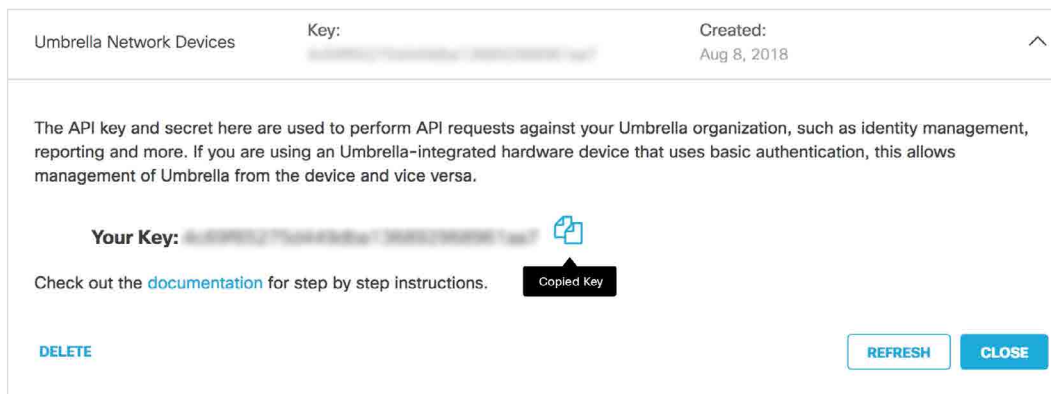
A match made in the cloud

This integration brings together two cloud-managed solutions to simplify deployments and deliver effective protection for users. Now, you can deploy Umbrella in minutes across your access points and instantly gain protection against threats like malware, ransomware, and C2 callbacks. For additional control and convenience, you can apply Umbrella policies directly in the Meraki dashboard. You'll experience a faster and more intuitive deployment of Umbrella, and the convenience of applying policies without leaving the Meraki dashboard.

How it works


Step 1 - Link accounts

Simply input the API key and secret from Umbrella into the Meraki dashboard.



Umbrella Network Devices Key: [redacted] Created: Aug 8, 2018

The API key and secret here are used to perform API requests against your Umbrella organization, such as identity management, reporting and more. If you are using an Umbrella-integrated hardware device that uses basic authentication, this allows management of Umbrella from the device and vice versa.

Your Key: [redacted] 

Check out the [documentation](#) for step by step instructions. **Copied Key**

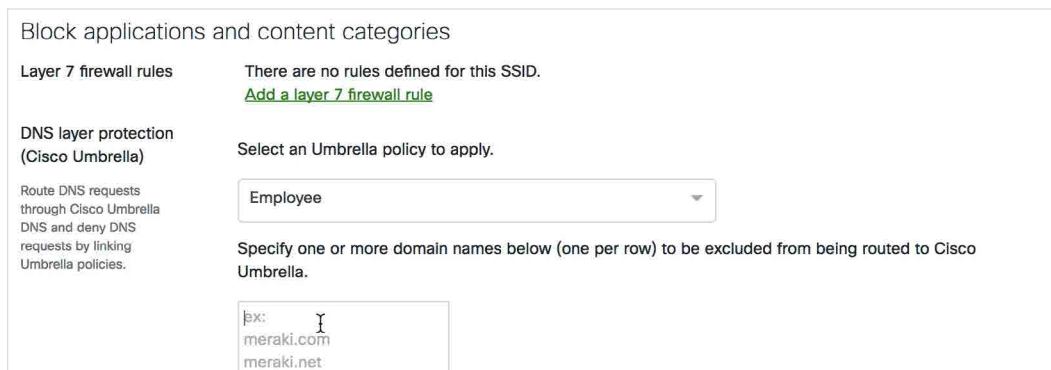
[DELETE](#) [REFRESH](#) [CLOSE](#)

Step 2 - Create Umbrella policies

If you're new to Umbrella, we recommend you create policies for your organization. The intuitive Umbrella policy wizard walks you through each step.

Step 3 - Select Umbrella policies

In the Meraki dashboard, assign Umbrella policies per SSID or using Meraki Group Policies.



Block applications and content categories

Layer 7 firewall rules There are no rules defined for this SSID. [Add a layer 7 firewall rule](#)

DNS layer protection (Cisco Umbrella) Select an Umbrella policy to apply.

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Employee

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

Ex: meraki.com
meraki.net

Why use the integration?

It's the fastest and easiest way to deploy Umbrella across your Meraki network.

Let's you conveniently enable Umbrella policies directly within the Meraki dashboard.

Create the most granular policies on a per-SSID basis or by using Meraki group policies by using Meraki group policies.



NEW TO MERAKI MR?

A series of 100% cloud-managed wireless access points.

- Manage your IT infrastructure from a single dashboard
- Provides visibility into application, device, and usage statistics
- No controller hardware to install or maintain



NEW TO UMBRELLA?

A secure internet gateway that provides the first line of defense against threats on the internet.

- Protection against threats like malware, ransomware, & C2 callbacks with no added latency
- Visibility into internet activity across all locations and users.
- No hardware to install or software to manually update.

FEATURES	WHY IT MATTERS
Meraki APs will automatically redirect DNS traffic to Umbrella resolvers.	Ensures all devices and users on the network are protected by Umbrella.
Within the Meraki dashboard, customers can assign Umbrella policies to their Cisco Meraki wireless networks on a per-SSID basis or using Meraki Group Policies.	Provides convenience to enable policy without leaving the Meraki dashboard, and gives customers more granular policy control.
Appends EDNS (Device ID and Client IP) to the DNS packet.	Enables Umbrella to enforce the right policies for the right devices (Device ID) and provides visibility in the Umbrella dashboard (Client IP).
Supports split DNS to exclude internal DNS requests from being sent to Umbrella resolvers.	Allows users to reach your network's local resources (computers, servers, printers, etc.) on internally-hosted domains that rely on local DNS servers.
Supports DNSCrypt proxy to encrypt the DNS traffic	Secures DNS traffic from eavesdropping and man-in-the-middle attacks.

Contact an Account Manager for more information.



Business Solutions 1.800.800.0014	Enterprise Solutions 1.800.369.1047	Public Sector Solutions 1.800.800.0019
--------------------------------------	--	---

www.connection.com/Cisco