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.
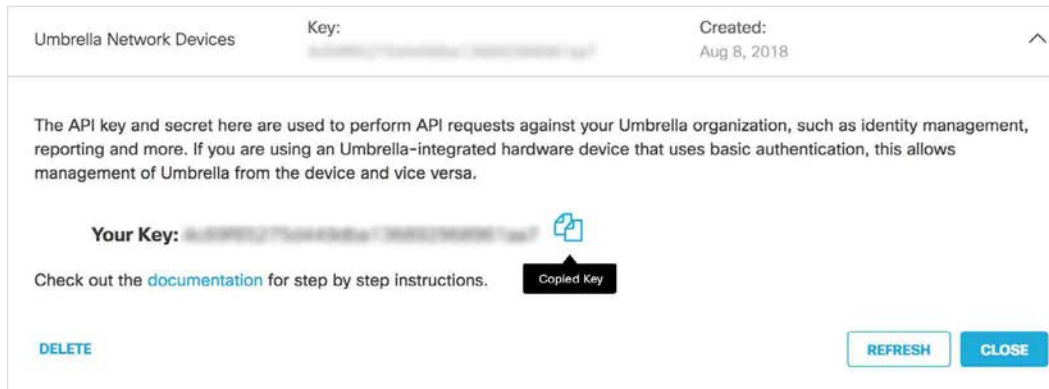
A match made in the cloud

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.
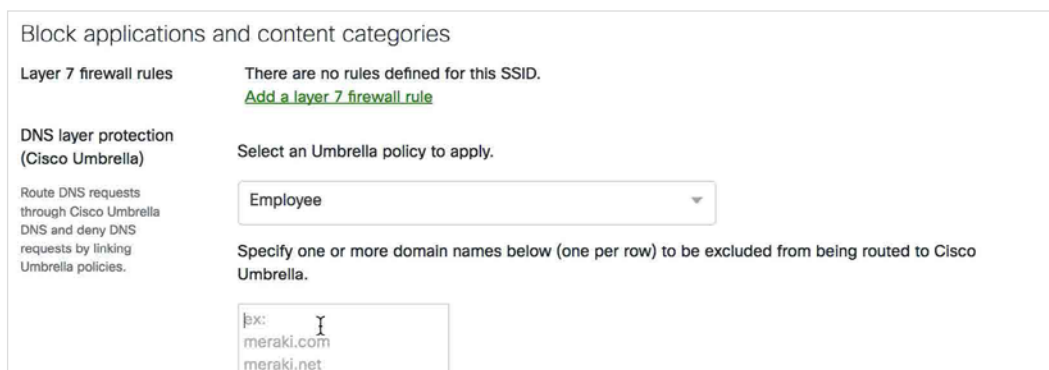

Step 2 – Create Umbrella policies
If you're new to Umbrella, we recommend you create policies for your organization. The intuitive Umbrella policy wizard walks you through each step.

Step 3 – Select Umbrella policies
In the Meraki dashboard, assign Umbrella policies per SSID or using Meraki Group Policies.

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.

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.

Take a test drive

There are three ways to try Meraki: you can request free trial gear, get a free access point by attending a webinar, or view an instant demo.

Connection
we solve IT®

1.800.800.0014
www.connection.com/brand/cisco/meraki

CISCO Cisco Umbrella