Central Web Authentication (CWA) with Cisco ISE

Cisco Identity Services Engine may be used for guest management when paired with Meraki Access Points. Cisco ISE is another option for authorizing users enabling many additional business use cases.

The Meraki APs will pass necessary information over to Cisco ISE using MAC-based authentication and honor a URL redirect that is received from the Cisco ISE Server. Using CoA the Cisco ISE server can ensure that the correct authorization is applied to the end user devices based on the authentication status.

Configuration

The following sections of this guide will outline a configuration example with using Cisco ISE as the guest management system which is also hosting the Captive portal.

Meraki Access Point Dashboard Configuration

The Meraki Access Point configuration is outlined below all on the Access Control Page for a particular SSID (Wireless > Configure > Access Control).

Configure MAC-Based Authentication

Select MAC-Based Authentication from the association requirements section of the access control page.

Enter the details for the RADIUS server including the IP address, port, and secret. If using Group Policies select Airspace-ACL-Name for the RADIUS attribute specifying the group policy name. The Airspace-ACL-Name must match the name of one of your group policies configured under Network-wide > Group Policies.
Configure CWA for Splash page

Select Cisco Identity Services Engine (ISE) Authentication in the Splash Page section of the access control page. This setting will honor the cisco custom url-redirect attribute sent from Cisco ISE.

Configure the Walled Garden

The IP address of the Cisco ISE server needs to be added to the walled garden to ensure that a client will be permitted through the walled garden before being authenticated by the Cisco ISE server.
Disable CNA

As of Cisco ISE 2.2, Apple CNA is supported for Guest and BYOD. **Beginning July 26th, 2017,** Apple CNA and Android captive portal detection are enabled by default on Cisco Meraki MR access points. On iOS 7+ and OS X, the client will automatically launch a mini-browser (CNA) that takes the user to the splash page to complete authentication and gain access to the network. Android devices will display a notification on the device prompting the user to sign into the Wi-Fi network. Tapping the notification will launch the device browser and direct the user to the splash page. To disable CNA and captive portal detection, append the following 17.0.0.0/8 IP range and domain names to the walled garden as shown below:

Disabling CNA will require that users manually open their web browser before being presented with the splash page.
Applications on the user’s device that require Internet connectivity will not function as expected until the user has opened their web browser and completed authentication via the splash page.

Cisco ISE Configuration

The following sections focuses on Cisco ISE 1.3. Configuration may vary based on the version of Cisco ISE. The Cisco ISE configuration details have been sourced from the ISE configuration example by Michal Garcarz and Nicolas Darchis from Cisco TAC (http://www.cisco.com/c/en/us/support/re-ise-00.html).

Create the Guest Portal

Navigate to Guest Access > Configure > Guest Portals, and create a new portal type. In this example we are using Self Registered Guest Portal and all splash page settings are left as default. The Portal name configured here will be used in other sections of the configuration outlined in this document. There are a number of customization options that can be configured on the Cisco ISE guest portal but are outside the scope of this document.

Create the Authorization Profile

On the ISE, the authorization profile must be created. Then, the authentication and authorization policies are configured. The individual Meraki APs should already be configured as a network devices.
Guest Captive Portal Authorization Profile

- Select the ACCESS_ACCEPT option for Access Type
- Check the Web Redirection check box, and choose Centralized Web Auth from the drop-down list.
- Choose the name of splash page you would like to redirect users. (This example is using Self-Registered Guest Portal which was built in the previous section)
- A custom IP address or host name can be defined that points to the Cisco ISE server. If left unchecked ISE will use the hostname and domain name defined during the system setup

Guest Internet Access Authorization Profile

- Select the ACCESS_ACCEPT option for Access Type
- Check the optional Airspace ACL Name check box, and define the name of a custom group policy configured on the Meraki Dashboard. This example used a group policy named internet.
Create a Authentication Rule

Ensure that the ISE accepts all of the MAC authentication from the Meraki AP and make sure it will pursue authentication even if the user is not found.

Under the Policy menu, click Authentication.

The next image shows an example of how to configure the authentication policy rule. In this example, a rule is configured that triggers when MAB is detected.

- Enter a name for your authentication rule. This example uses MAB, which already exists by default on ISE Version 1.2.
- Select the plus (+) icon in the If condition field.
• Choose **Compound condition**, and then choose **Wired_MAB OR Wireless_MAB**.
• Click the arrow located next to **and** ... in order to expand the rule further.
• Click the + icon in the Identity Source field, and choose **Internal endpoints**.
• Choose **Continue** from the **If user not found** drop-down list.

---

**Create a Authorization Policy**

In order to verify the authorization rules, navigate to **Policy > Authorization**. In ISE Version 1.3 by default for failed MAC Authentication Bypass (MAB) access (MAC address not found) authentication is continued (not rejected). This is very useful for Guest Portals because there is no need to change anything in default authentication rules.

New users who associate to the Guest SSID are not yet part of any identity group. This is why they match the second rule, which uses the Guest authorization profile to redirect them to the correct Guest Portal.

After a user creates an account and logs in successfully, ISE sends a RADIUS CoA and the WLC performs re-authentication. This time, the first rule is matched along with authorization profile PermitInternet and returns the ACL name that is applied on the WLC.
Add Meraki APs to Cisco ISE

Add the Meraki AP management IPs or subnet as a Network Access Device from Administration > Network Resources > Network Devices