Integrating Meraki Networks

With Cisco Identity Services Engine

Author: Timothy Abbott II

Current Document Version: 1.0

July 29, 2013

Table of Contents

Introduction

This configuration example illustrates how to use Cisco Identity Services Engine (ISE) to authenticate users attempting access to Meraki wireless, wired and VPN networks. ISE will use predefined Meraki Group Polices to assign network users an access policy based upon group membership in Microsoft's Active Directory (AD), Guest user credentials or Endpoint information. The example will use the following Identity Groups: Employees, Contractors, Guests and Workstations. Using these groups, the document will outline the steps necessary to configure 802.1X, MAC Authentication Bypass (MAB), Local Web Authentication (LWA) Remote Access (RA) VPN and Profiling where applicable.

Compatibility Matrix

Feature	Wireless Compatibility	VPN Compatibility	Wired Compatibility	Details
IEEE-802.1X	Compatible	Compatible	Compatible	
MAC Authentication By-Pass	Compatible	Not Compatible	Not Compatible*	Wireless only.
Enforcement	Compatible	Not Compatible	Not Compatible	Preconfigured Group policy (wireless).
Local Web Authentication	Compatible	Not Compatible	Not Compatible	Local captive portals (wireless).
Profiling Probes	Limitations	Limitations	Limitations	DHCP and RADIUS (Wireless). RADIUS (Wired).
Posture Assessment	Limitations	Limitations	Limitations	Requires Inline Posture Node.
Guest Services	Limitations	Limitations	Limitations	Sponsored guest accounts (wireless). Guest VLAN (Wired).
Security Group Access	Not Compatible	Not Compatible	Not Compatible	
Central Web Authentication	Not Compatible	Not Compatible	Not Compatible	No URL-Redirect with session information.
RADIUS Change of Authorization	Not Compatible	Not Compatible	Not Compatible	

* At the time of this writing, MAB with Cisco Meraki switches are not possible. However, a future software update from Cisco Meraki will allow compatibility.

Overview

This guide assumes that both ISE and a Meraki networks have been installed and are functioning properly. A step-by-step guide on how to set up Meraki networks is available at http://docs.meraki.com. The Meraki wireless networks should be configured with three SSIDs. The Meraki wired network should be configured with Employee and Guest VLANs. A subnet for RA VPN clients should also be identified. Cisco ISE will use AD as an external identity source for user authentication and differentiated authorization policy assignment. Any AD groups intended for use in authorization policy should be preconfigured in the ISE as well as Sponsored Guest Policy. Reference the ISE User Guide for more information or how to configure Sponsored Guests and to integrate ISE with AD.

Components

- Cisco ISE 1.2
- Cisco Catalyst 3560-X Switch
- Cisco Meraki MR16 Access Point
- Cisco Meraki MS42P Switch
- Cisco Meraki MX90 Security Appliance
- Cisco Meraki Cloud Management Platform
- Microsoft Active Directory 2008 R2

Network Diagram

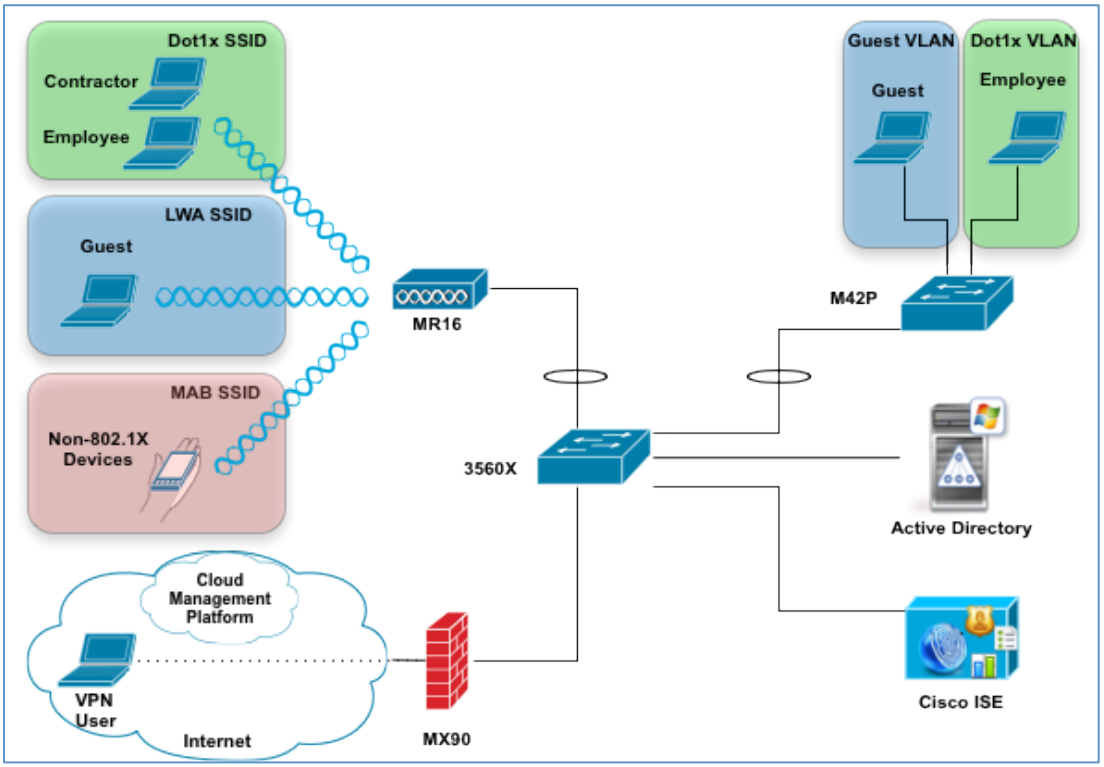

Figure 1

Meraki Cloud Platform Configuration

Wireless Network Configuration

Using Meraki Group Policies configure a Group Policy for the Employee and Contractor groups in AD. Then add ISE as the RADIUS server for the Dot1x, LWA and MAB SSIDs. Users who belong to the Employee or Contractor AD group will be able to connect to the Dot1x SSID. Users with Guest credentials will be able to connect to the LWA SSID and devices belonging to the Workstation Endpoint Identity Group in ISE will be able to associate to the MAB SSID.

Procedure 1 Configure Meraki Wireless Group Policy

Step 1 Select the wireless network for use with ISE from the **Network:** drop down menu.

Step 2 Select **Configure ➔ Group policies** in the Meraki dashboard.

Step 3 Select **Add a group**.

Step 4 Name the group policy **Employee**.

Step 5 If needed, configure any group policy settings. Leave **Splash** as **Use SSID Default**.

Step 6 Click **Save Changes**.

Step 7 Repeat steps 1 through 6 for the **Contractor** Group Policy

Step 8 Repeat steps 1 through 6 for the **Workstation** Group Policy

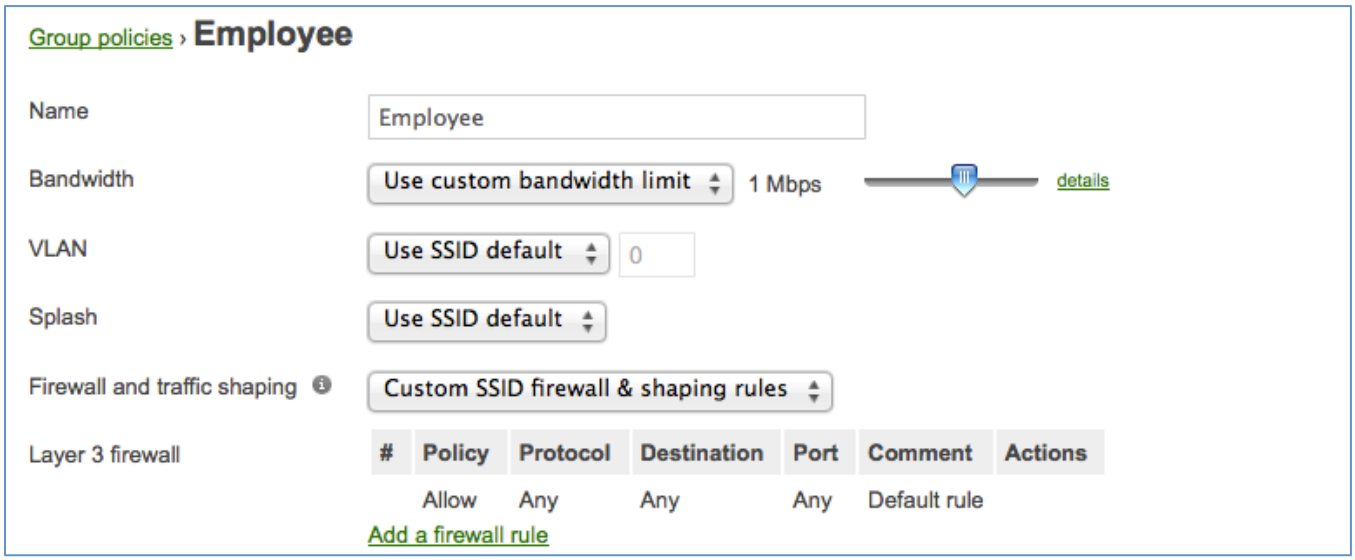

Figure 3

This section shows an example configuration for an 802.1X-protected SSID using ISE as the RADIUS server. During authentication, ISE will tell the Cloud Management Platform which Group Policy to assign using the Airespace-ACL-Name RADIUS vendor specific attribute (VSA).

Procedure 2 Add ISE as a RADIUS Server for Dot1x SSID

Step 1 Under the **Configure** menu in the Meraki dashboard, select **Access control**.

Step 2 Select the SSID from the drop down menu that will be used by the Employee Identity Group.

Step 3 Ensure the **WPA2-Enterprise** radio button is selected along with **my RADIUS server** in the drop down menu.

Step 4 Select **None (direct access)** for **Splash Page**.

Step 5 In the **RADIUS servers** field, enter the **IP address**, port **1812** and **secret** of the ISE policy service nodes.

Step 6 Disable **RADIUS testing**.

Step 7 Enable **RADIUS accounting**.

Step 8 In the **RADIUS accounting** field, enter the **IP address**, port **1813** and **secret** of the ISE policy service nodes.

Step 9 In the **RADIUS attribute specifying group policy name** field, select **Airespace-ACL-Name**.

Step 10 Ensure that **Assign group policies by device type** is disabled.

Step 11 Select **Bridge mode** for Client IP Assignment.

Step 12 Set the VLAN tagging option to **Don't use VLAN tagging**.

Note: Optionally, you may configure Per-User VLAN tagging in addition to the Group Policy assignment. ISE can tell the Cloud Management Platform which VLAN to assign to the user. This method would allow you to further differentiate user groups and assign different access policies during authentication.

Step 13 Click **Save Changes** to complete the configuration of the SSID. Refer to figure 4 for an example.

Dot1x SSID Access Control	
Network Access	
Association Requirements	**WPA-2 Enterprise with my RADIUS server.**
Splash Page	**None (direct access)**
RADIUS Servers	**IP address, port 1812 and secret of ISE policy service nodes**
RADIUS Testing	**RADIUS testing disabled**
RADIUS Accounting	**RADIUS accounting is enabled**
RADIUS Accounting Servers	**IP address, port 1813 and secret of ISE policy service nodes**
RADIUS attribute specifying group policy name	**Airespace-ACL-Name**
Assign group policies by device type	**Disabled: Do not assign group policies automatically**
Addressing and traffic	
Client IP assignment	**Bridged Mode: Make clients a part of the LAN**
VLAN tagging	**Don't use VLAN tagging**

Figure 4

This section shows an example of how to configure LWA using ISE as the RADIUS server. The captive portal webpage is served from the Cloud Management Platform and must be able to communicate with ISE across the Internet for credential validation. **The Meraki Security Appliance will need to be configured to allow RADIUS traffic on UDP ports 1812 and 1813 from the Cloud Management Platform to ISE**. Reference http://docs.meraki.com/ for

information on how to configured firewall rules on the Meraki Security Appliance. Guest credentials are created on ISE and sent to the guest user.

Procedure 3 Add ISE as a RADIUS Server for Guest SSID

Step 1 Under the **Configure** menu in the Meraki dashboard, select **Access control**.

Step 2 Select the SSID from the drop down menu that will be used by the Guest Identity Group.

Step 3 Ensure the **Open (no encryption)** radio button is selected for **Association Requirements**.

Step 4 Select **Single sign-on** for **Splash Page** and ensure **my RADIUS server** is selected from the drop down menu.

Step 5 Under **RADIUS for splash page**, enter the **publically reachable IP address**, port **1812** and **secret** of the ISE policy service node.

Step 6 Ensure that **Assign group policies by device type** is disabled.

Step 7 Select **Bridge mode** for Client IP Assignment.

Step 8 Set the VLAN tagging option to **Use VLAN tagging**.

Step 9 Under **VLAN ID**, select **Add VLAN**.

Step 10 Enter the **AP Tag** name for the **Guest VLAN ID**.

Note: The AP Tag must be configured on the access point for the configuration to take effect and the link between the switch and access point must be a VLAN trunk. In this scenario, ISE will not need to assign the VLAN ID, as each user attempting to authenticate to the Guest SSID will use the Guest VLAN. See Meraki Cloud Managed Wireless documentation for more information.

Step 11 For **RADIUS override**, select **Ignore VLAN attribute in RADIUS responses**.

Step 12 Click **Save Changes** to complete the configuration of the SSID. Refer to figure 5 for an example.

Guest SSID Access Control	
Network Access	
Association Requirements	**Open (no encryption)**
Splash Page	**Sign-on with my RADIUS server**
RADIUS for splash page	**IP address, port 1812 and secret of ISE policy service nodes**
Assign group policies by device type	**Disabled: Do not assign group policies automatically**
Addressing and traffic	
Client IP assignment	**Bridged Mode: Make clients a part of the LAN**
VLAN tagging	**Use VLAN tagging**
VLAN ID	**AP Tag and VLAN ID of guest VLAN on up stream switch**
RADIUS override	**Ignore VLAN attribute in RADIUS responses**

Figure 5

For this example, endpoints attempting to associate to the MAB SSID must be a member of the Workstation Endpoint Identity Group and will be placed in a separate VLAN. If an endpoint attempting to associate was not previously seen by ISE, access will be denied. It is recommended that device MAC address be imported into ISE prior to association.

Procedure 4 Add ISE as a RADIUS Server for MAB SSID

Step 1 Under the **Configure** menu in the Meraki dashboard, select **Access control**.

Step 2 Select the SSID from the drop down menu that will be used by the Workstation Identity Group.

Step 3 Ensure the **MAC-based access control (no encryption)** radio button is selected for **Association Requirements**.

Step 4 Select **None (direct access)** for **Splash Page**.

Step 5 In the **RADIUS servers** field, enter the **IP address**, port **1812** and **secret** of the ISE policy service nodes.

Step 6 Disable **RADIUS testing**.

Step 7 In the **RADIUS attribute specifying group policy name** field, select **Airespace-ACL-Name**.

Step 8 Ensure that **Assign group policies by device type** is disabled.

Step 9 Select **Bridge mode** for Client IP Assignment.

Step 10 Set the VLAN tagging option to **Use VLAN tagging**.

Step 11 Under **VLAN ID**, select **Add VLAN**.

Step 12 Enter the **AP Tag** name for the **Workstation VLAN ID**.

Step 13 For **RADIUS override**, select **Ignore VLAN attribute in RADIUS responses**.

Step 14 Click **Save Changes** to complete the configuration of the SSID. Refer to figure 5 for an example.

MAB SSID Access Control	
Network Access	
Association Requirements	**MAC-based access control (no encryption)**
Splash Page	**Sign-on with my RADIUS server**
RADIUS Servers	**IP address, port 1812 and secret of ISE policy service nodes**
RADIUS Testing	**RADIUS testing disabled**
RADIUS attribute specifying group policy name	**Airespace-ACL-Name**
Assign group policies by device type	**Disabled: Do not assign group policies automatically**
Addressing and traffic	
Client IP assignment	**Bridged Mode: Make clients a part of the LAN**
VLAN tagging	**Use VLAN tagging**
VLAN ID	**AP Tag and VLAN ID of Workstation (MAB) VLAN on up stream switch**
RADIUS override	**Ignore VLAN attribute in RADIUS responses**

Figure 6

Wired Network Configuration

This section outlines the configuration steps necessary to use ISE as a RADIUS server for use with Meraki switches. Meraki switches operate in a closed mode. In contrast to Meraki wireless networks, you do not have the ability to

apply Meraki Group Policy during authentication. Optionally, you may configure a guest VLAN. This is useful in the event of authentication failure or for wired guest access to the network.

Procedure 1 Add ISE as a RADIUS Server for Wired 802.1X

Step 1 Select the wired network for use with ISE from the **Network:** drop down menu.

Step 2 Under the **Configure** menu in the Meraki dashboard, select **Access policies**.

Step 3 Select **Add an access policy**.

Step 4 Give the new policy a **name**. (For example, ISE).

Step 5 In the **Host** field, enter the **IP address** of the **ISE node**.

Step 6 In the **Port** field, enter **1812**.

Step 7 In the **secret** field, enter the **shared secret**.

Step 8 Set **RADIUS testing** to **RADIUS testing disabled**.

Step 9 If desired, enter the **Guest VLAN** for use when users fail 802.1X authentication.

Step 10 Click **Save**.

Note: Once configured, your new Access Policy should look similar to Figure 7.

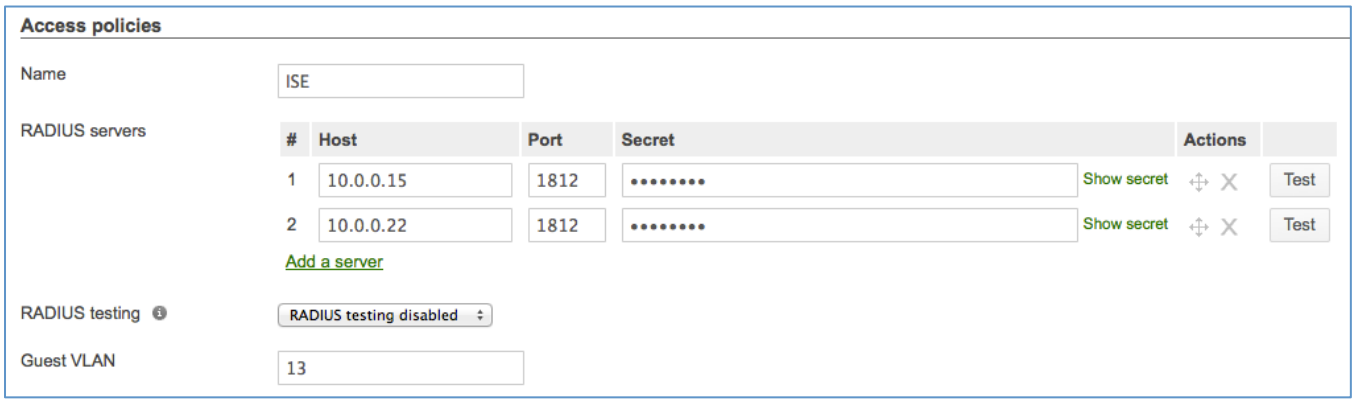

Figure 7

Procedure 2 Apply Access Policy to Switch Ports

Step 1 Select **Configure ➔ Switch ports**.

Step 2 Select the desired switch ports to apply the **Access policy**.

Step 3 In the **Access policy** drop down menu, select the name of the Access Policy (For example, **ISE**).

Step 4 Click **Update 1 port**.

Step 5 Repeat steps 1 through 4 for each port intended to use this Access Policy.

Note: Reference Figure 8 for a configuration example.

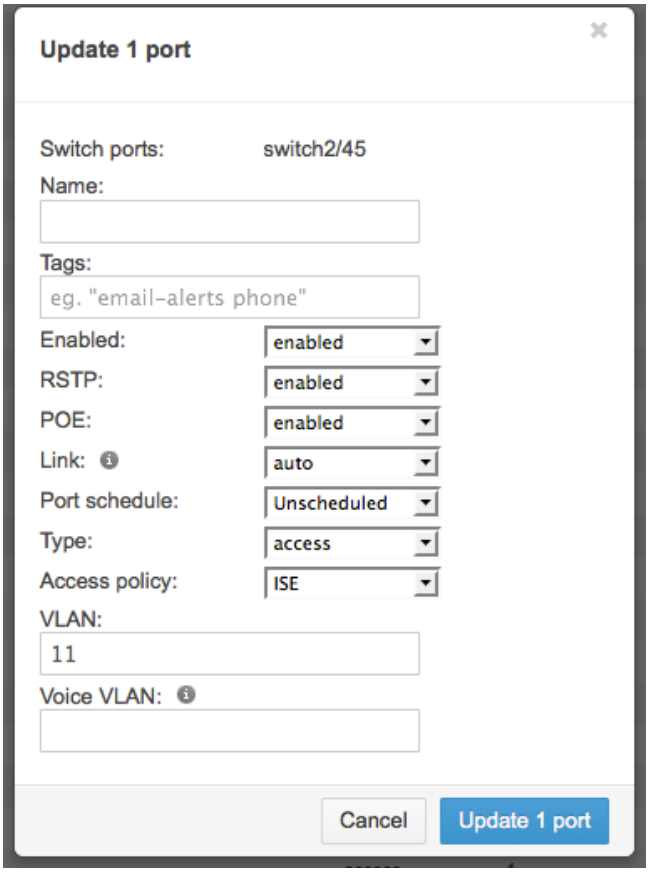

Figure 8

VPN Network Configuration

Procedure 3 Configure Client VPN Access

Step 6 Select the VPN network for use with ISE from the **Network:** drop down menu.

Step 7 Select **Configure ➔ Client VPN** in the Meraki dashboard.

Step 8 Set the **Client VPN Server** to **Enabled**.

Step 9 Enter a **subnet** that VPN Clients will use. (For example, 192.168.111.0/24)

Step 10 Select **Specify nameservers**… from the **DNS nameservers** drop down menu.

Step 11 Enter the **IP address(s)** of internal **DNS servers**.

Step 12 Specify a **secret** that users will need to configure a **L2TP over VPN** client.

Step 13 From the **Authentication** drop down menu, select **RADIUS**.

Step 14 Click **Add RADIUS server**.

Step 15 Enter the **IP address**, **Port** and **Shared Secret** for the ISE node.

Step 16 Click **Save**.

Note: Reference Figure 9 for a configuration example.

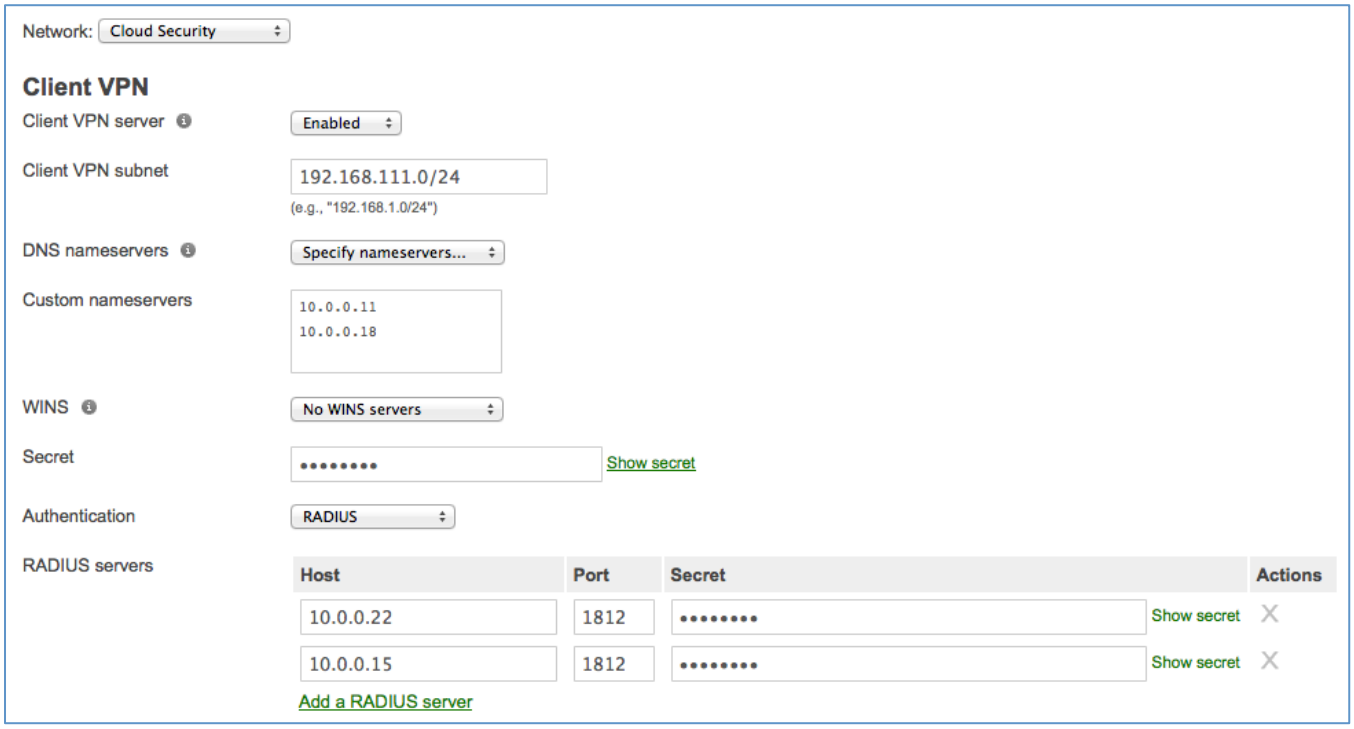

Figure 9

Basic ISE Configuration

In this section, we first configure Policy Sets. Next, the Meraki access points and Cloud RADIUS Clients will be added into the ISE deployment as network access devices. Then, configure an Authorization Profile for Employees, Contractors and Workstations. Configure allowed protocols for use in Authentication Policy. Finally, configure Authentication and Authorization Policy.

Enable Policy Sets

Procedure 1 Enable Policy Sets in ISE

Step 1 Navigate to **Administration ➔ Settings ➔ Policy Sets**.

Step 2 Click **Enabled**.

Step 3 Click **Save**.

Note: See Figure 9 for configuration example.

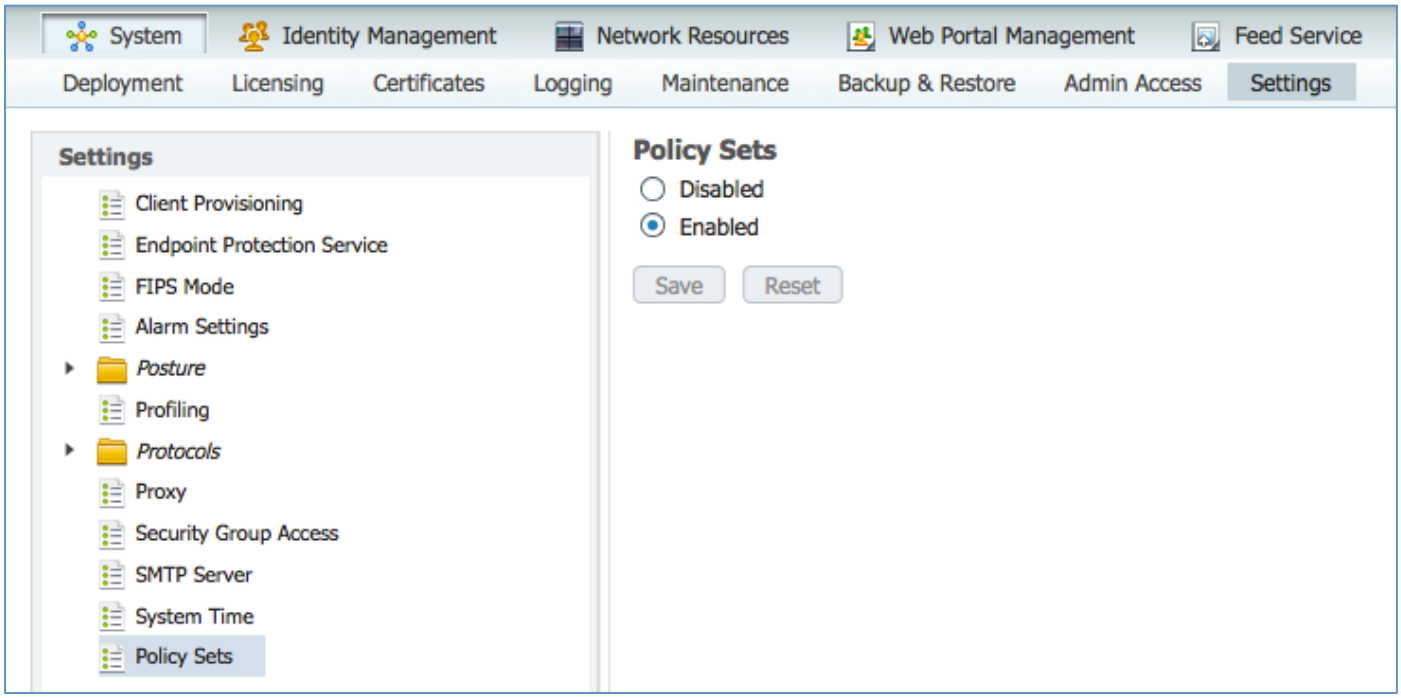

Figure 9

Network Access Devices

Procedure 1 Add Meraki Access Point as Network Access Device

Step 1 Navigate to **Administration ➔ Network Devices**.

Step 2 Click **Add** to create a new network device.

Step 3 Enter a **name** for the Cisco Meraki access point.

Step 4 Enter the **IP address** of the access point.

Step 5 Define the **Device Type** and **Location** of the access point.

Cisco Best Practice: Predefine **Device Type** and **Location** in the **Network Device Groups** menu. Putting all Meraki access points in a unique Device Type group will allow you to reference them in authentication and authorization policy later.

Step 6 Check the box for **Authentication Settings** and enter the **shared secret**.

Step 7 Click **Submit**.

Step 8 Repeat steps 1 through 7 for additional Meraki access points that will be used in the ISE deployment.

Note: You have the ability to bulk import network access devices. Simply click on "Import" and then "generate a template." Be sure to fill out all the required fields in the CSV template prior to uploading to ISE.

Procedure 2 Add Meraki Switch as Network Access Device

Step 1 Click **Add** to create a new network device.

Step 2 Enter a **name** for the Cisco Meraki switch.

Step 3 Enter the **IP address** of the switch.

Step 4 Define the **Device Type** and **Location** of the access point.

Step 5 Check the box for **Authentication Settings** and enter the **shared secret**.

Step 6 Click **Submit**.

Procedure 3 Add Meraki Security Appliance as Network Access Device

Step 1 Click **Add** to create a new network device.

Step 2 Enter a **name** for the Cisco Meraki security appliance.

Step 3 Enter the **IP address** for the access point.

Step 4 Define the **Device Type** and **Location** of the access point.

Step 5 Check the box for **Authentication Settings** and enter the **shared secret**.

Step 6 Click **Submit**.

Note: To use Meraki LWA, you must add the Cloud Management Platform itself as a network access device (NAD). RADIUS requests from the Cloud Management Platform will come from one of four public IP addresses: **64.156.192.245, 64.156.192.68, 74.50.51.16, and 74.50.56.161**. Create a NAD entry in ISE for each public IP address.

Procedure 4 Add Meraki Cloud RADIUS Clients as Network Access Devices

Step 1 Navigate to **Administration ➔ Network Devices**.

Step 2 Click **Add** to create a new network device.

Step 3 Enter a **name** for the Meraki access point.

Step 4 Enter one of the **IP addresses** for the Cloud RADIUS client.

Step 5 Define the **Device Type** and **Location** of the access point.

Step 6 Check the box for **Authentication Settings** and enter the **shared secret**.

Step 7 Click **Submit**.

Step 8 Repeat steps 1 through 7 for the remaining 3 Cloud RADIUS Clients.

Authorization Profiles

This procedure outlines the process necessary to tie ISE Authorization Policy to Group Policy on the Cisco Meraki access point. We will create Authorizations Profiles for Employees, Contractors and Workstation for use in Authorization Policy. For Cisco Meraki networks that will not use Group Policy, we will use the per-built Authorization Profile PermitAccess in Authorization Policy.

Procedure 5 Configure Authorization Profiles for Network Users

Step 1 Navigate to **Policy ➔ Results ➔ Authorization ➔ Authorization Profiles**.

Step 2 Click **Add** to create a new Authorization Profile.

Step 3 Name the Authorization Profile **MerakiWirelessEmployee** and leave the access type set to **Access_Accept**.

Step 4 Under **Common Tasks**, Check the box for **Airespace ACL Name** and enter **Employee**.

Step 5 Click **Submit** to save the new Authorization Profile.

Step 6 Repeat steps 1 through 5 and name the profile **MerakiWirelessContractor** and use **Contractor** for the **Airespace ACL Name**.

Step 7 Repeat steps 1 through 5 and name the profile **MerakiWirelessWorkstation** and use **Workstation** for the **Airespace ACL Name.**

Note: The Airespace ACL Name is the name of the group policy configured on the Meraki cloud controller (Figure 3) for use with ISE Authorization Profile. The Meraki cloud controller can be configured to look for 1 of 3 compatible RADIUS messages from Cisco ISE: Filter-ID, Airespace-ACL-Name and Reply-Message. This example uses Airespace-ACL-Name.

Allowed Protocols

Procedure 6 Configure ISE Allowed Protocols

Step 1 Navigate to **Policy ➔ Results ➔ Authentication ➔ Allowed Protocols**.

Step 2 Click **Add**.

Step 3 Enter a **name** for the new allowed protocols list. (For example, Meraki)

Step 4 Check the box for **Allow PAP/ASCII**.

Step 5 Under **Allow PAP/ASCII**, check the box for **Detect PAP as Host Lookup**.

Step 6 Check the box for **Allow PEAP** and under Inner Methods check **Allow PEAP-MSCHAPv2**.

Step 7 Click **Submit**.

Note: This example uses PEAP-MSCHAPv2 as the protocol to 802.1X authentications. Be sure you understand the needs of clients on your network prior to enabling or disabling allowed protocols. Reference Figure 10 as an example configuration.

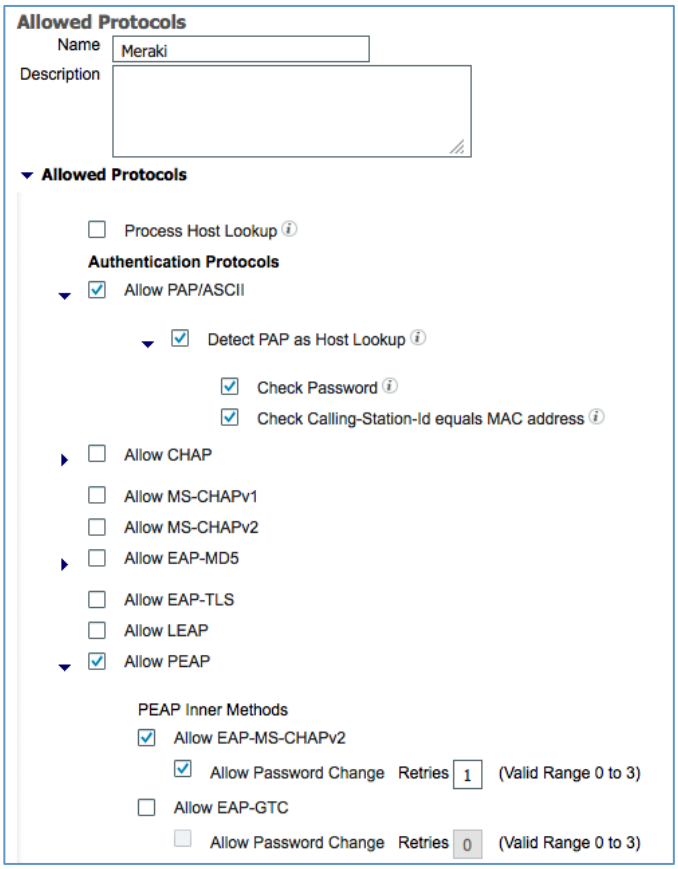

Figure 10

AAA Configuration

Meraki Policy Set

Procedure 1 Configure ISE Policy Set for Meraki Network Access Devices

Step 1 Navigate to **Policy ➔ Policy Sets**.

Step 2 Create a new Policy Set by clicking the green plus sign (**+**) then **Create Above**.

Step 3 Click **Edit** to customize the Policy Set rule.

Step 4 Enter and **Name** and **Description** (optional) for the Policy Set rule.

Step 5 Click the plus sign (**+**) in the conditions box and select **Create New Condition (Advanced Option)**.

Step 6 Navigate to Select **Attribute ➔ DEVICE ➔ Device Type**.

Step 7 Change the operator drop down from EQUALS to **CONTAINS**.

Step 8 Select the Device Type group defined earlier in this guide that contains all Meraki devices that will apply to the new Policy Set. Reference Figure 5 as an example.

Step 9 Click **Done** on the right hand side of the policy set rule.

Step 10 Click **Submit**.

Status	Name	Description	Conditions
	Meraki	AAA for Meraki Infrastructure.	DEVICE:Device Type CONTAINS Device Type#All Device Types#meraki

Figure 11

Note: You have the ability to reorder the policy set list by dragging them into order of preference. Reference Figure 11 as an example.

Wireless Authentication Rule

Since all wireless authentication types from the Cisco Meraki wireless network contain the NAS-Port-Type: Wireless – IEEE 802.11 RADIUS attribute, we will use it to define wireless authentications at a high level. Then configure authentication rules that describe 802.1X, MAB, and LWA.

Procedure 2 Configure Wireless Authentication Rule

Step 1 Create a new Authentication Policy rule by clicking the down arrow next to Edit and select **Insert New Rule Above**.

Step 2 Enter a **name** for the new rule. Example: **Wireless**.

Step 3 Click the plus sign (**+**) in the conditions field to access the drop down menu and select **Create New Condition (Advanced Option)**.

Step 4 Select the attribute **RADIUS ➔ NAS-Port-Type**.

Step 5 Leave the operator box set to **EQUALS**.

Step 6 In the last drop down box, select **Wireless - IEEE 802.11**.

Step 7 For Allowed Protocols, select **Meraki**.

Wireless 802.1X Authentication

Procedure 3 Configure Wireless 802.1X Authentication

Step 1 Select the Actions menu and click **Insert New Rule Above**.

Step 2 Give the sub-rule a **name** (Example: Dot1X).

Step 3 Click the small window icon to open the Conditions menu.

Step 4 Select **Create New Condition (Advanced Option)**.

Step 5 Select **Network Access ➔ EapAuthentication**.

Step 6 Leave the operator box set to **EQUALS**.

Step 7 In the last box select **EAP-MSCHAPv2**.

Step 8 In the Use field, select **ActiveDirectory** as the identity store.

Wireless MAB Authentication

Procedure 4 Configure Wireless MAB Authentication

Step 1 Select the Actions menu then **Insert New Rule Above**.

Step 2 Give the sub-rule a **name** (Example: MAB).

Step 3 Click the small window icon to open the **Conditions** menu.

Step 4 Select **Create New Condition (Advanced Option)**.

Step 5 Select **Network Access ➔ UseCase**.

Step 6 Leave the operator box set to **EQUALS**.

Step 7 In the last box select **Host Lookup**.

Step 8 In the Use field, select **Internal Endpoints** as the identity store.

Step 9 Set the "If user not found" field to **Continue**.

Wireless Local Web Authentication

Procedure 5 Configure Wireless LWA Authentication

Step 1 Select the Actions menu then **Insert New Rule Above**.

Step 2 Give the sub-rule a **name** (Example: LWA).

Step 3 Click the small window icon to open the **Conditions** menu.

Step 4 Select **Create New Condition (Advanced Option)**.

Step 5 Select **RADIUS ➔ Service-Type**.

Step 6 Leave the operator box set to **EQUALS**.

Step 7 In the last box select **Login**.

Step 8 In the "Use:" field, select **Internal Users** as the identity store.

Step 9 Click **Save**.

Cisco Best Practice: Once configured, your Authentication Policy will look similar to Figure 12. If these rules will be used in a production environment, be sure to set the Default rule to use DenyAccess as the identity store. In addition, you can configure an Identity Source Sequence for use with authenticating Active Directory users as well as guest users via LWA. Simply change the LWA rule to use the name of the Identity Source Sequence instead of Active Directory. See the ISE user guide for more information on Identity Source Sequences.

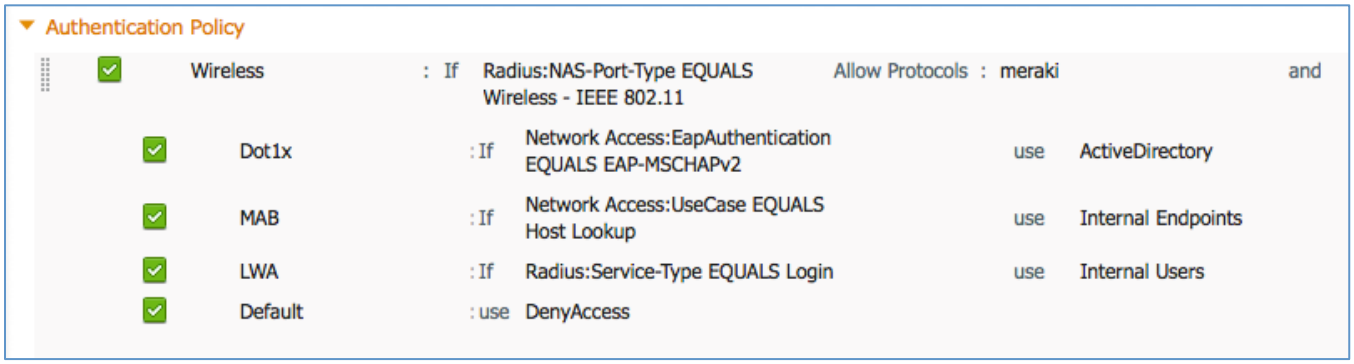

Figure 12

Wired 802.1X Authentication Rule

Procedure 6 Configure Wired Authentication Rule

Step 1 Create a new Authentication Policy rule by clicking the down arrow next to Edit and select **Insert New Rule Above**.

Step 2 Enter a **name** for the new rule. Example: **Wired Dot1x**.

Step 3 Click the plus sign (**+**) in the conditions field to access the drop down menu and select **Create New Condition (Advanced Option)**.

Step 4 Select the attribute **RADIUS ➔ NAS-Port-Type**.

Step 5 Leave the operator box set to **EQUALS**.

Step 6 In the last drop down box, select **Ethernet**.

Step 7 For Allowed Protocols, select the profile previously configured (Example: meraki).

Step 8 Click the plus sign (+) in the **Use** field and select **ActiveDirectory**.

Step 9 Click **Done** and save then **Save**.

Note: Reference Figure 13 for an example Wired Authentication Rule.

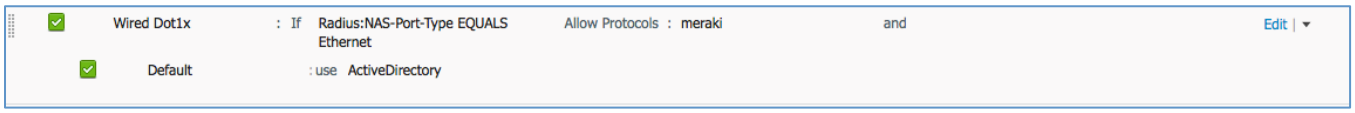

Figure 13

RA VPN Authentication

Procedure 7 Configure VPN Authentication Rule

Step 1 Create a new Authentication Policy rule by clicking the down arrow next to Edit and select **Insert New Rule Above**.

Step 2 Enter a **name** for the new rule. Example: **RA VPN**.

Step 3 Click the plus sign (**+**) in the conditions field to access the drop down menu and select **Create New Condition (Advanced Option)**.

Step 4 Select the attribute **RADIUS ➔ NAS-Port-Type**.

Step 5 Leave the operator box set to **EQUALS**.

Step 6 In the last drop down box, select **Framed**.

Step 7 Add a new **Attribute/Value** by selecting the gear icon.

Step 8 Select attribute **RADIUS ➔ Framed-Protocol**.

Step 9 Change the EQUALS operator to **EQUALS**.

Step 10 In the last drop down box, select **PPP.**

Step 11 For Allowed Protocols, select the profile previously configured (Example: meraki).

Step 12 Click the plus sign (+) in the **Use** field and select **ActiveDirectory**.

Step 13 Click **Done** and save then **Save**.

Note: Reference Figure 14 for an example VPN Authentication Rule.

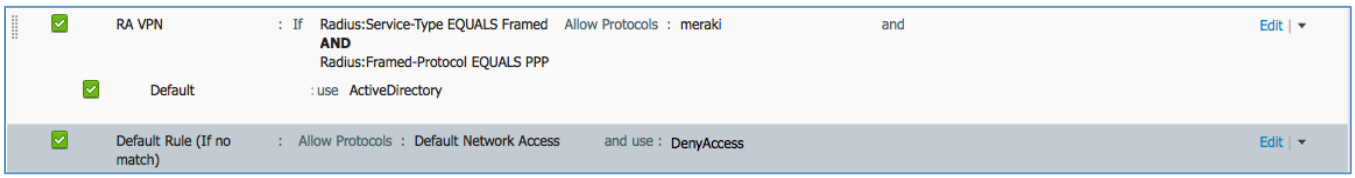

Figure 14

At this point, the Authentication Policy for Meraki devices is complete. The policy is sectioned into three parts: Wireless, Wired and RA VPN. The wireless section has subsections that describe the authentication types for 802.1X, MAB and LWA. The Wired an RA VPN subsections use a default rule that outlines with Identity Store to use during authentication. Reference Figure 15 as an example policy.

Name	Conditions (If)	Allowed Protocols	Identity Store (use)
Wireless	Radius:NAS-Port-Type EQUALS Wireless – IEEE 802.11	Meraki	
Dot1x	Network Access:EapAuthentication EQUALS EAP-MSCHAPv2		ActiveDirectory
MAB	Network Access:UseCase EQUALS Host Lookup		Internal Endpoints
LWA	Radius:Service-Type EQUALS Login		Internal Users
Default			DenyAccess
Wireless	Radius:NAS-Port-Type EQUALS Ethernet	Meraki	
Default			ActiveDiretory
RA VPN	Radius:NAS-Port-Type EQUALS Framed **AND** Radius:Framed-Protocol EQUALS PPP	Meraki	
Default			ActiveDiretory
Default (If no match)		Default Network Access and use: DenyAccess	

Figure 15

Wireless 802.1X Authorization

Procedure 1 Configure Wireless 802.1X Authorization Rule

Step 1 Navigated to **Policy ➔ Policy Sets**.

Step 2 Click the down arrow in the default authorization rule and select **Insert new rule above**.

Note: ISE Authorization rules are matched from top to bottom with the first matched rule being selected.

Step 3 Enter a name for the new Authorization Rule. Example: **Wireless Dot1x**.

Step 4 Leave the Identity Group field to **Any** then click the plus sign in the **Condition(s)** field.

Step 5 Select **Create New Condition (Advanced Option)**.

Step 6 Select attribute **Radius ➔ NAS-Port-Type ➔ Wireless-IEEE 802.11**.

Step 7 Add a new **Attribute/Value** by selecting the gear icon.

Step 8 Select attribute **Network Access ➔ EapAuthentication**.

Step 9 Change the EQUALS operator to **EQUALS**.

Step 10 In the last drop down box, select **EAP-MSCHAPv2**.

Step 11 Add a new **Attribute/Value** by selecting the **gear icon**.

Step 12 Select **attribute ➔ Active Directory ➔ ExternalGroups** and select **Employees**.

Step 13 Click the plus sign (**+**) in the field for Permissions.

Step 14 Click **Select an item ➔ Standard ➔ MerakiWirelessEmployees**.

Step 15 Click **Save**.

Step 16 Repeat steps 1 through 15 and select **Contractors** for the AD group and **MerakiWirelessContractors** as the Authorization Profile.

Wireless MAB Authorization

Procedure 2 Configure Wireless MAB Authorization Rule

Step 1 Click the down arrow in the default authorization rule and select **Insert new rule above**.

Step 2 Enter a name for the new Authorization Rule. Example: **Wireless Dot1x**.

Step 3 In the Identity Field, click the plus sign (+) and select **Endpoint Identity Groups ➔ Profiled ➔ Workstation**.

Step 4 Select **Create New Condition (Advanced Option)**.

Step 5 Select attribute **Radius ➔ NAS-Port-Type ➔ Wireless-IEEE 802.11**.

Step 6 Add a new **Attribute/Value** by selecting the gear icon.

Step 7 Select **Network Access ➔ UseCase**.

Step 8 Leave the operator box set to **EQUALS**.

Step 9 In the last box select **Host Lookup**.

Step 10 Click the plus sign (**+**) in the field for Permissions.

Step 11 Click **Select an item ➔ Standard ➔ MerakiWirelessWorkstation**.

Step 12 Click **Save**.

Note: Currently, Meraki wireless networking equipment does not support RADIUS CoA. This prevents ISE from granting access then assigning the appropriate Authorization Profile based upon profiling information. As a result, the MAC address of approved devices will need to be manually imported into ISE's Workstation Endpoint Identity Group.

Wireless LWA Authorization

Procedure 3 Configure Wireless LWA Authorization Rule

Step 1 Click the down arrow in the default authorization rule and select **Insert new rule above**.

Step 2 Enter a name for the new Authorization Rule. Example: **Wireless Dot1x**.

Step 3 In the Identity Field, click the plus sign (+) and select **User Identity Groups ➔ Guest**.

Step 4 Click the plus sign (+) again and select **User Identity Groups ➔ ActivatedGuest**.

Step 5 Select **Create New Condition (Advanced Option)**.

Step 6 Select attribute **Radius ➔ NAS-Port-Type ➔ Wireless-IEEE 802.11**.

Step 7 Add a new **Attribute/Value** by selecting the gear icon.

Step 8 Select **RADIUS ➔ Service-Type**.

Step 9 Leave the operator box set to **EQUALS**.

Step 10 In the last box select **Login**.

Step 11 Click the plus sign (**+**) in the field for Permissions.

Step 12 Click **Select an item ➔ Standard ➔ MerakiWirelessGuest**.

Step 13 Click **Save**.

Wired Authorization Policy

Procedure 1 Configure ISE Authorization Policy

Step 1 Click the down arrow in the default authorization rule and select **Insert new rule above**.

Note: ISE Authorization rules are matched from top to bottom with the first matched rule being selected.

Step 2 Enter a name for the new Authorization Rule. Example: **Wired Dot1x**.

Step 3 Leave the Identity Group field to **Any** then click the plus sign in the **Condition(s)** field.

Step 4 Select **Create New Condition (Advanced Option)**.

Step 5 Select attribute **Radius ➔ NAS-Port-Type ➔ Ethernet**.

Step 6 Add a new **Attribute/Value** by selecting the **gear icon**.

Step 7 Select **attribute ➔ Active Directory ➔ ExternalGroups** and select the **Employees**.

Step 8 Click the plus sign (**+**) in the field for Permissions.

Step 9 Click **Select an item ➔ Standard ➔ PermitAccess**.

Step 10 Click **Save**.

RA VPN Authorization

Procedure 1 Configure Wireless 802.1X Authorization Rule

Step 1 Navigated to **Policy ➔ Policy Sets**.

Step 2 Click the down arrow in the default authorization rule and select **Insert new rule above**.

Step 3 Enter a name for the new Authorization Rule. Example: **RA VPN**.

Step 4 Leave the Identity Group field to **Any** then click the plus sign in the **Condition(s)** field.

Step 5 Select **Create New Condition (Advanced Option)**.

Step 6 Select attribute **Radius ➔ NAS-Port-Type ➔ Framed**.

Step 7 Add a new **Attribute/Value** by selecting the gear icon.

Step 8 Select attribute **Radius ➔ Framed-Protocol**.

Step 9 Change the EQUALS operator to **EQUALS**.

Step 10 In the last drop down box, select **PPP**.

Step 11 Add a new **Attribute/Value** by selecting the **gear icon**.

Step 12 Select **attribute ➔ Active Directory ➔ ExternalGroups** and select **Employees**.

Step 13 Click the plus sign (**+**) in the field for Permissions.

Step 14 Click **Select an item ➔ Standard ➔ MerakiWirelessEmployees**.

Step 15 Click **Save**.

Note: Unlike Meraki wireless networks, VPN users cannot be assigned a group policy during authentication at the time of this writing. However, you can allow VPN access based upon the user's Identity Store membership. Once configured, your new Authorization Policy should be similar to the figure 16.

Rule Name	Identity Group	Conditions	Permissions
Wireless Dot1x Employee	Any	Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11 AND Network Access:EapAuthentication EQUALS EAP-MSCHAPv2 AND ActiveDirectory:ExternalGroups EQUALS ise.local/Users/Employees)	MerakiWirelessEmployees
Wireless Dot1x Contractor	Any	Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11 AND Network Access:EapAuthentication EQUALS EAP-MSCHAPv2 AND ActiveDirectory:ExternalGroups EQUALS ise.local/Users/Contractors)	MerakiWirelessContractor
Wireless MAB	Workstation	Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11 AND Network Access:UseCase EQUALS Host Lookup	MerakiWirelessWorkstation
Wireless LWA	**Guest** OR **ActivedGuest**	Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11 AND RADIUS:Service-Type EQUALS Login	PermitAccess
Wired Dot1x	Any	Radius:NAS-Port-Type EQUALS Ethernet AND ActiveDirectory:ExternalGroups EQUALS ise.local/Users/Domain Users)	PermitAccess
RA VPN	Any	Radius:NAS-Port-Type EQUALS Framed AND Radius:Framed-Protocol EQUALS PPP AND ActiveDirectory:ExternalGroups EQUALS ise.local/Users/Employees)	PermitAccess

Figure 16

Profiling Considerations

Wireless Network Profiling

RADIUS and DHCP profiling using Cisco Meraki wireless networking equipment is compatible with ISE but with limitations. While Cisco Meraki access points can dynamically profile wireless devices during authentication, that information cannot be shared with ISE for use with Authorization Policy. Cisco Meraki access points do not have the ability to forward DHCP requests. As such, a Catalyst 3560X was used during this configuration example for the ability to forward DHCP requests. RADIUS profiling with Cisco Meraki access points is supported via the calling-station-id attribute.

Wired Network Profiling

Cisco Meraki switches lack the ability to forward DHCP requests or run a DHCP server. In a network consisting of only Cisco Meraki equipment, only RADIUS profiling is possible with ISE via the calling-station-id attribute. The only device capable of running a DHCP server is the MX Security Appliance. However, like the Cisco Meraki access point, it does not have the ability forward DHCP requests.

References

Cisco TrustSec System

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides

Cisco Identity Services Engine User Guides:

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Meraki Cloud Managed Wireless Documentation:

https://docs.meraki.com/display/MR/Wireless+LAN

Configuring Meraki Wireless Group Policies:

https://docs.meraki.com/display/MR/Group+Policies.

Configuring Meraki RADIUS settings:

https://docs.meraki.com/display/MR/Externally+Hosted+RADIUS+Server