Integrate Cisco Meraki Systems Manager

Configure Cisco Meraki Systems Manager

Cisco Meraki Systems Manager supports a variety of platforms, enabling the diverse device ecosystems that are commonplace today. Systems Manager offers centralized, cloud-based tools for endpoint management with far-reaching scalability for growing organizations. Integrate Cisco Meraki Systems Manager as an MDM server in Cisco ISE to leverage the endpoint information that is collected by Cisco Meraki Systems Manager for compliance checks and endpoint policy management.

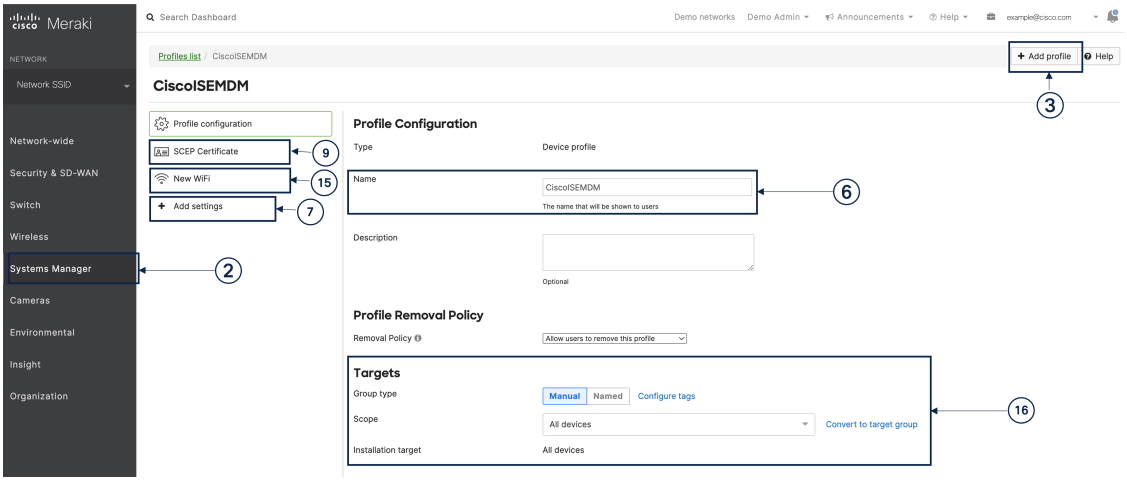
For more information about Cisco Meraki Systems Manager, see the datasheet.

Cisco Meraki Systems Manager now supports MDM API version 3 and can provide Cisco ISE with a unique device identifier for connected endpoints. If you already have an active Cisco Meraki Systems Manager integration in your Cisco ISE, carry out Steps 8 to 15 for the Cisco ISE-related device profile in your Cisco Meraki Systems Manager.

Configure Cisco Meraki Systems Manager as an MDM/UEM Server

The images in this section display the Cisco Meraki Systems Manager GUI fields that you must work with during this task. The numbers in the images correspond to the step numbers in the task.

Figure 1: Steps To Configure Cisco Merki Systems Manager



Before you begin

In Cisco ISE, create and export a System Certificate that is configured for Admin usage. You will use this certificate in Step 12 of the following task.

For instructions on how to create and export a system certificate, see the topic "System Certificates" in Chapter "Basic Setup" in the *Cisco ISE Administrator Guide* for your release.

Step 1 Log in to your Cisco Meraki Systems Manager portal.

Step 2 From the main menu, go to **Systems Manager** > **Manage** > **Settings**.

Step 3 Click **+ Add Profile**.

Step 4 In the Add New Profile dialog box that is displayed, click the **Device profile (Default)** radio button.

Step 5 Click **Continue**.

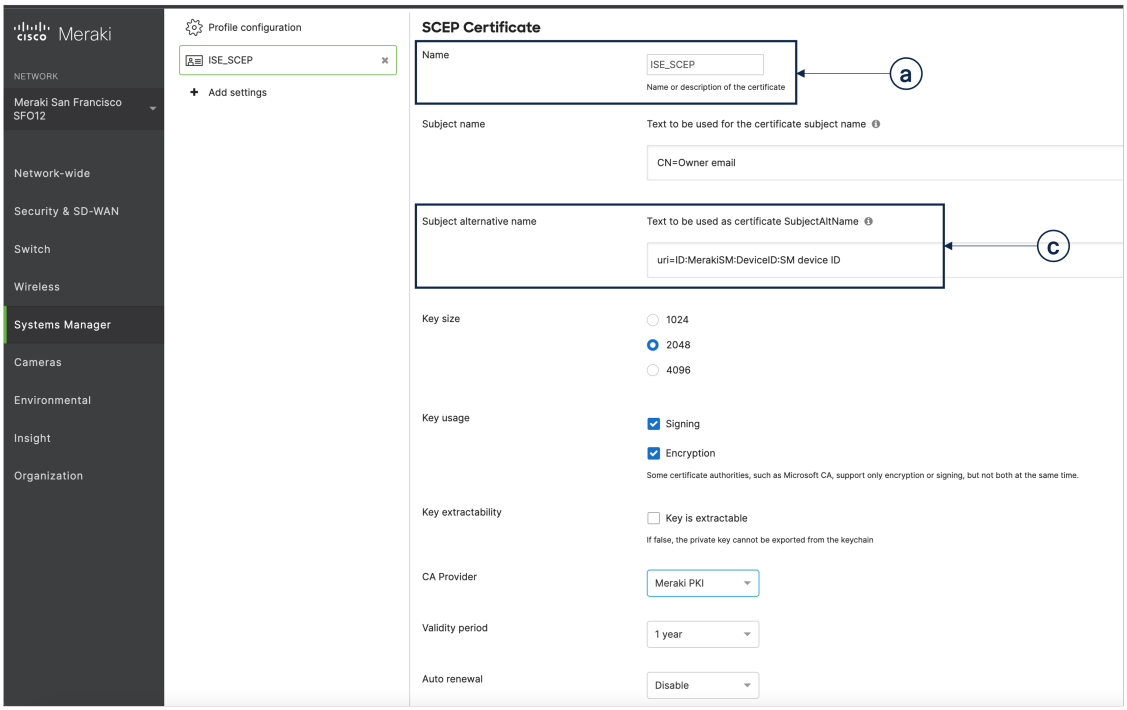
Step 6 In the **Name** and **Description** fields, enter the required values.

Step 7 Click **+Add settings**.

Step 8 In the **Add New Settings Payload** window that is displayed, click **SCEP Certificate.**

Step 9 In the **SCEP Certificate** window that is displayed:

Figure 2: The SCEP Certificate Configuration Window in Cisco Meraki Systems Manager



a) In the **Name** field, enter a name for the SCEP certificate. For example, **ISE_SCEP**.
b) In the **Subject name** field, enter the common name value for the certificate.
c) In the **Subject alternative name** field, enter **uri=ID:MerakiSM:DeviceID:$SM Device ID**.

   When you enter **$**, a drop-down list of variables is displayed. Choose SM Device ID from the list.

d) In the **Key Size** area, click the **2048** radio button.
e) In the **Key Usage** area, check the **Signing** and **Encryption** check boxes.
f) In the **CA Provider** area, choose a CA provider from the drop-down list.
g) Click **Save**.

Step 10 Click **+Add settings**.

Step 11 In the **Add New Settings Payload** window that is displayed, click **Certificate**

Step 12 In the **Certificate** window that is displayed:

a) In the **Name** field, enter a name for the certifiate.
b) From the **CertStore** drop-down list, choose **System**.
c) In the **Certificate** field, click **Choose File** and upload the Cisco ISE system certificate that you downloaded as a prerequisite step for this task.
d) Click **Save**.

Step 13 Click **+Add settings**.

Step 14 In the **Add New Settings Payload** window that is displayed, click **WiFi Settings**.

Step 15 In the **WiFi Settings** window that is displayed:

a) In the **SSID** field, enter the name of the Wi-Fi network to join.
b) From the **Security** drop-down list, choose one of the Wi-Fi Protected Access (WPA) options.

c) In the **Enterprise Settings** area that is displayed when you choose an enterprise option from the Security drop-down list:

1. In the **Protocol** tab, check the check box of any certificate-based protocol, such as TLS.
2. In the **Authentication** tab, in the **Identity Certificate** area, from the drop-down list, choose the SCEP certificate that you created for the Cisco ISE use case (in Step 10).
3. In the **Trust** tab, in the **Trusted Certificates** area, check the check box next to the Cisco ISE certificate that you uploaded in Step 12.
4. Click **Save**.

Step 16 In the **Profile Configuration** tab, in the **Targets** area, add a tag for the ISE use case. For information on how to create and manage tags in Meraki Systems Manager, see Manage Tags. The application of tags ensures that the ISE profile with its certificate and Wi-Fi settings is applied to the relevant devices.

Step 17 In the **You have unsaved changes** dialog box, click **Save**.

Step 18 From the left menu pane, choose **Organization > Configure> MDM**

Step 19 From the ISE Settings area:

a) Take note of the username and password details that must be input in Cisco ISE.

b) To download the SCEP certificate that you must use in Cisco ISE, click the **Download** button.

What to do next

Now, connect Cisco Meraki Systems manager as an MDM server in Cisco ISE. For information on how to carry out this task, see "Configure Mobile Device Management Servers in Cisco ISE" in the Chapter "Secure Access" in the *Cisco ISE Administrator Guide* for your release.