Monitoring Cisco Meraki (API)

Beta Version

Cisco: Meraki [API] PowerPack version 106, rev. 2

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Cisco Meraki access points, switches, phones, and cameras in SL1 using the *Cisco: Meraki [API]* PowerPack and the Meraki API.

The following sections provide an overview of Cisco Meraki and the *Cisco: Meraki [API]* PowerPack:

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is Cisco Meraki?

Cisco Meraki provides a set of networking devices and appliances that you can manage from the cloud. Cisco Meraki's centralized cloud architecture enables you to securely monitor users, applications, and devices in your environment.

What Does the Cisco: Meraki [API] PowerPack Monitor?

To monitor Cisco Meraki devices using SL1 and the Meraki API, you must install the *Cisco: Meraki [API]* PowerPack. This PowerPack enables you to discover and collect data about Cisco Meraki appliances.

The *Cisco: Meraki [API]* PowerPack includes:

- Dynamic Applications to discover, model, and monitor performance metrics and collect configuration data for Cisco Meraki devices
- Device Classes for each of the Cisco Meraki devices that SL1 monitors
- Event Policies and corresponding alerts that are triggered when Cisco Meraki devices meet certain status criteria
- Example credentials that you can use as template to create Basic/Snippet or SOAP/XML credentials for connecting to the Cisco Meraki API
- Run Book Action and Automation policies that gather the SNMP credential information needed for discovery and create a Meraki Cloud Controller virtual device during discovery

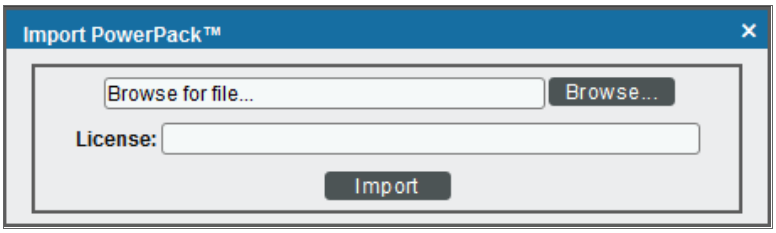
Installing the Cisco: Meraki [API] PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Cisco: Meraki [API]* PowerPack.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

> **NOTE:** If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuration and Discovery

Overview

The following sections describe how to configure and discover Cisco Meraki devices for monitoring by SL1 using the *Cisco: Meraki [API]* PowerPack and the Meraki API:

Generating a Cisco Meraki API Key

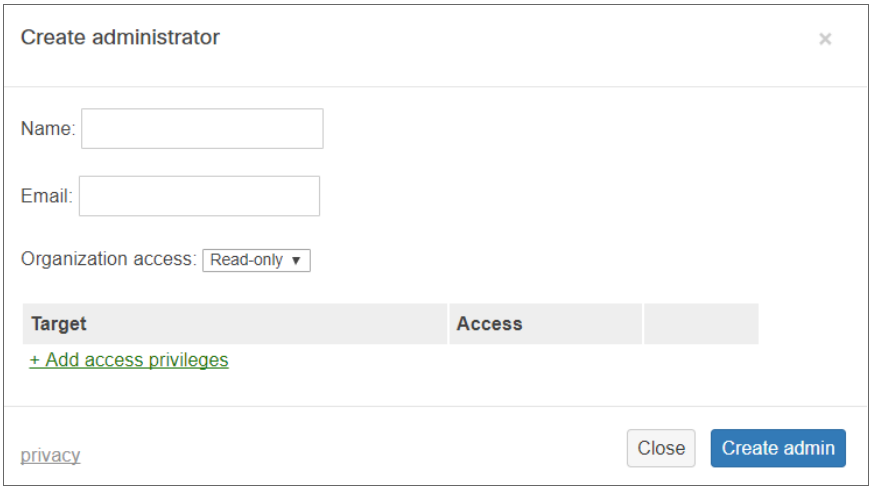
To configure Cisco Meraki for monitoring using the Meraki API, you must first generate an API key for a read-only Meraki user. You will then enter this user's API key in the ***Basic/Snippet credential*** you create in SL1 to monitor Meraki.

NOTE: If the read-only user has access to multiple organizations, then SL1 can discover all of those organizations with a single discovery session. In this scenario, each organization is created as a separate Cloud Controller in SL1.

However, if you want each Meraki organization to have its own corresponding ScienceLogic organization in SL1, ScienceLogic recommends creating a unique read-only user account and API key for each organization in Meraki. You can then create separate credentials in SL1 for each Meraki organization using those unique API keys, and then use those credentials to run separate discovery sessions for each organization.

To create a read-only user:

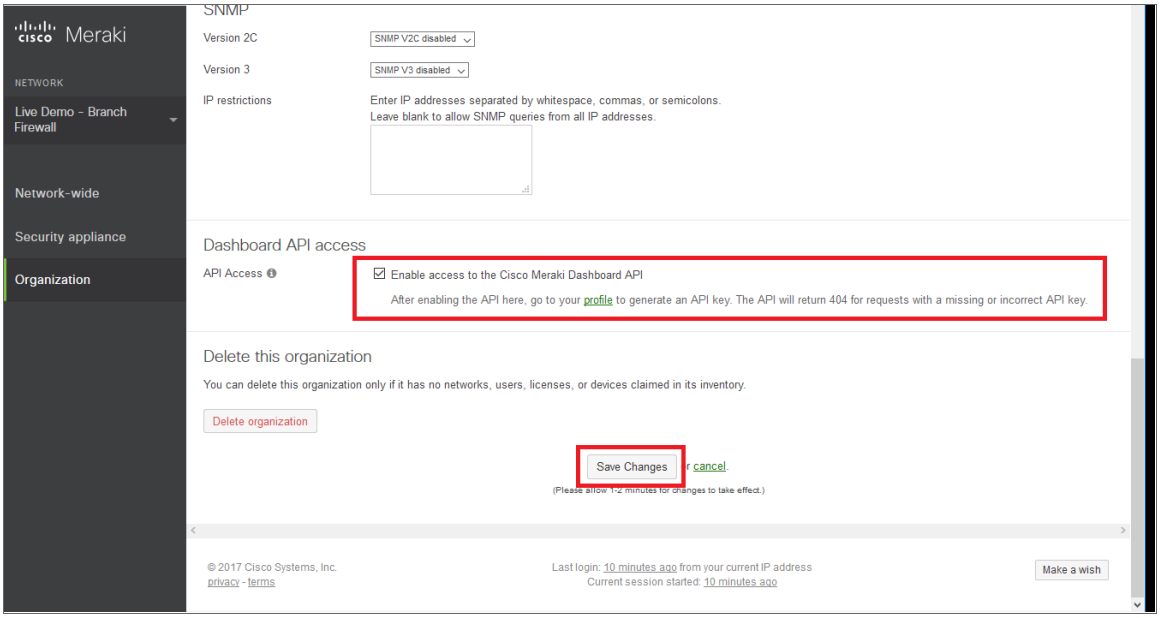
1. Log in to the Cisco Meraki web interface.
2. Go to **Organization > Administrators**, and then click the **[Add admin]** button.
3. On the **Create administrator** page, complete the following fields:



   - ***Name***. Type the user's name.
   - ***Email***. Type the user's email address.
   - ***Organization access***. Select *Read-only*.
4. Click **[Create admin]**. Cisco Meraki sends an email to the email address provided, describing how the user can complete the registration process. The user must complete those steps before generating the API key.

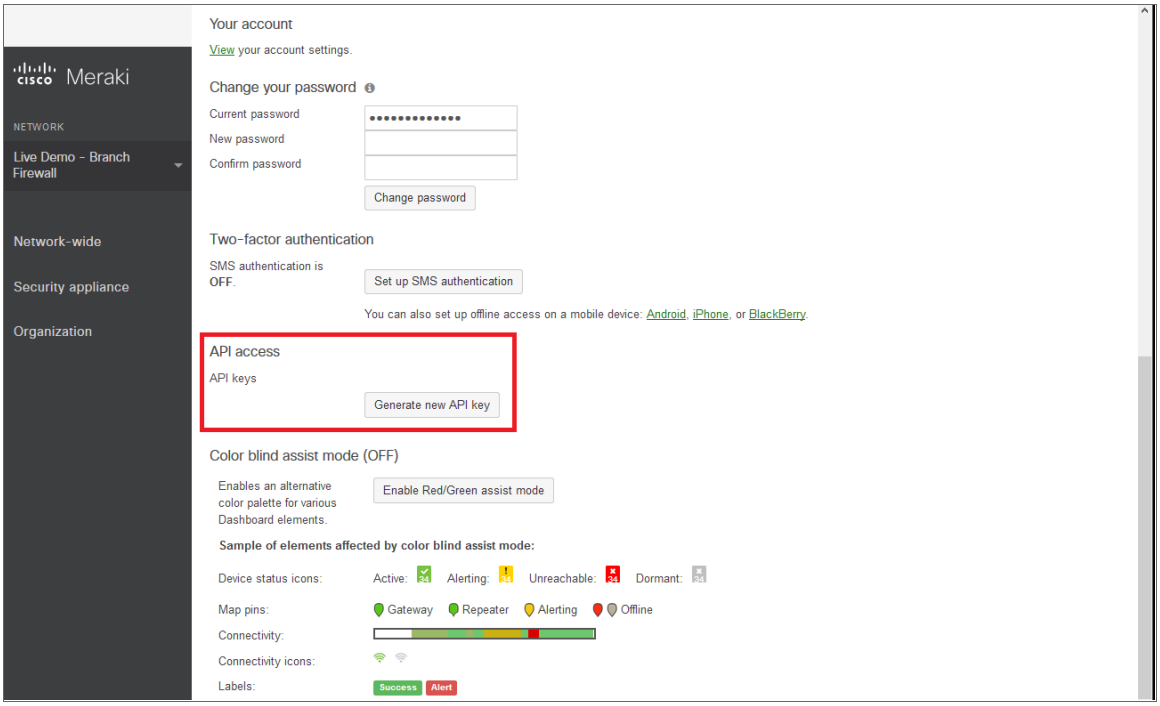
To generate a Cisco Meraki API key for that read-only user:

1. Log in to the Cisco Meraki web interface as the read-only user.
2. Go to **Organization > Settings**:



3. In the **Dashboard API access** section, select the **Enable access to the Cisco Meraki Dashboard API** checkbox.
4. Click the **Save Changes** button.
5. Click the **profile** link in the **Dashboard API access** section.

6. In your user profile, navigate to the **API access** section and click the **Generate new API key** button.



7. In the **API access** section, the API key appears. Copy and save the key value.

NOTE: API keys are visible only to the user that created them.

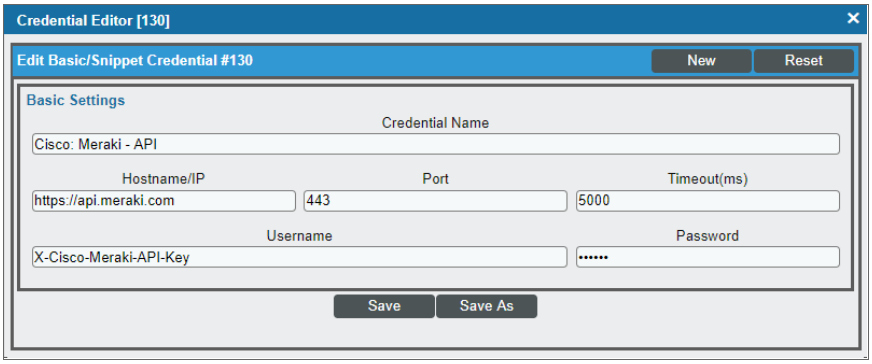
Creating a Basic/Snippet Credential

To configure SL1 to monitor Cisco Meraki systems using the Meraki API, you must create a Basic/Snippet credential. This credential allows the Dynamic Applications in the *Cisco: Meraki [API]* PowerPack to connect with the Cisco Meraki API. An example Basic/Snippet credential that you can edit for your own use is included in the PowerPack.

To create a Basic/Snippet credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Locate the **Cisco: Meraki - API** credential, and then click its wrench icon (). The **Edit Basic/Snippet Credential** modal page appears:



3. Complete the following fields:
    - ***Credential Name***. Type a new name for the credential.
    - ***Hostname/IP***. Keep the default value.

NOTE: You **must** use the default value in the ***Hostname/IP*** field.

    - ***Port***. Keep the default value.
    - ***Timeout(ms)***. Keep the default value.
    - ***Username***. Keep the default value.
    - ***Password***. Type the *Meraki API key.*
4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

Creating an SNMP V3 Credential

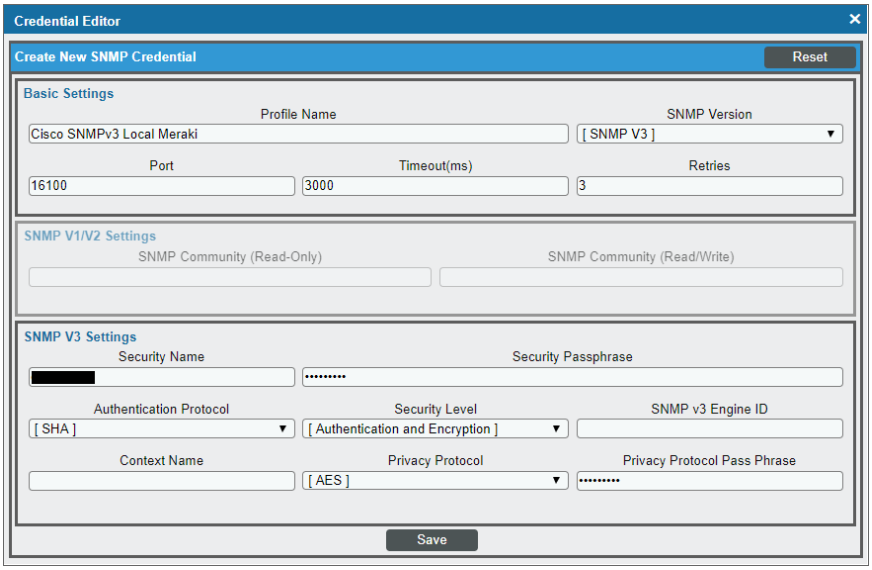
The Dynamic Applications in the *Cisco: Meraki [API]* PowerPack use SNMP to collect some data about Meraki component devices that is not available through the Meraki API. If your Meraki devices are configured for SNMP V3, then you must create an SNMP V3 credential that enables the PowerPack to connect with the devices through a series of Run Book Actions and Automations.

NOTE: If your Meraki system is configured for SNMP V2, you do not need to create an SNMP credential in SL1.

To create an SNMP V3 credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Click the **[Actions]** button, and then select *Create SNMP Credential*. The **Create New SNMP Credential** modal page appears:



3. Complete the following fields:
   - ***Profile Name***. Type a name for the credential.
   - ***SNMP Version***. Select *SNMP V3*.
   - ***Port***. Type "16100" for the port the platform will use to communicate with the device.
   - ***Timeout***. Type the amount of time, in milliseconds, after which the platform will stop trying to communicate with the device.
   - ***Retries***. Type the number of times the platform will try to authenticate and communicate with the device.
   - ***Security Name***. Type the Meraki device's SNMP V3 username.
   - ***Security Passphrase***. Type the Meraki device's SNMP V3 password.
   - ***Authentication Protocol***. *Select SHA*.
   - ***Security Level***. Select *Authentication and Encryption*.
   - ***SNMP v3 Engine ID***. Leave this field blank.
   - ***Context Name***. Leave this field blank.
   - ***Privacy Protocol***. Select *AES*.
   - ***Privacy Protocol Pass Phrase***. Type the Meraki device's AES privacy key.
4. Click **[Save]**.

Disabling Automatic SNMP V3 Credential Updates

If your Meraki devices are not configured for SNMP V3, you can disable the behavior in the *Cisco: Meraki [API]* PowerPack that searches for an SNMP V3 credential to use and triggers an event and Run Book Actions and Automations that automatically update the credential if one is found.

> **NOTE:** Disabling automatic SNMP V3 credential updates does not affect users whose Meraki devices are configured for SNMP V2.

To disable the automatic SNMP V3 credential update event:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Locate the "Cisco: Meraki Network Discovery [API]" Dynamic Application and click its wrench icon ().
3. Click the **[Snippets]** tab, and then click the wrench icon () for the "Network Discovery" snippet.
4. Edit the "Network Discovery" snippet to change `snmp_update=True` to `snmp_update=False`.
5. Click **[Save]**.

> **CAUTION:** If your Meraki devices are configured for SNMP V3 but you have the `snmp_update=False` value in the "Network Discovery" snippet, SL1 will not be able to collect the SNMP data for the "Cisco: Meraki Interface Performance [API]" and "Cisco: Meraki Device Configuration [API]" Dynamic Applications. If you want to collect this data, you will need to change the value back to `snmp_update=True` to enable SL1 to update the SNMP V3 credential and collect SNMP data from the Meraki devices.

Creating a SOAP/XML Credential

If you access Meraki systems through a third-party proxy server, you can create a SOAP/XML credential to enable the Dynamic Applications in the *Cisco: Meraki [API]* PowerPack to connect with the Cisco Meraki API via the proxy server.

Similarly, if you want to discover only some selected devices, you can create a SOAP/XML credential that specifies tag values that the Dynamic Applications in the *Cisco: Meraki [API]* PowerPack can use to determine which devices should be discovered.

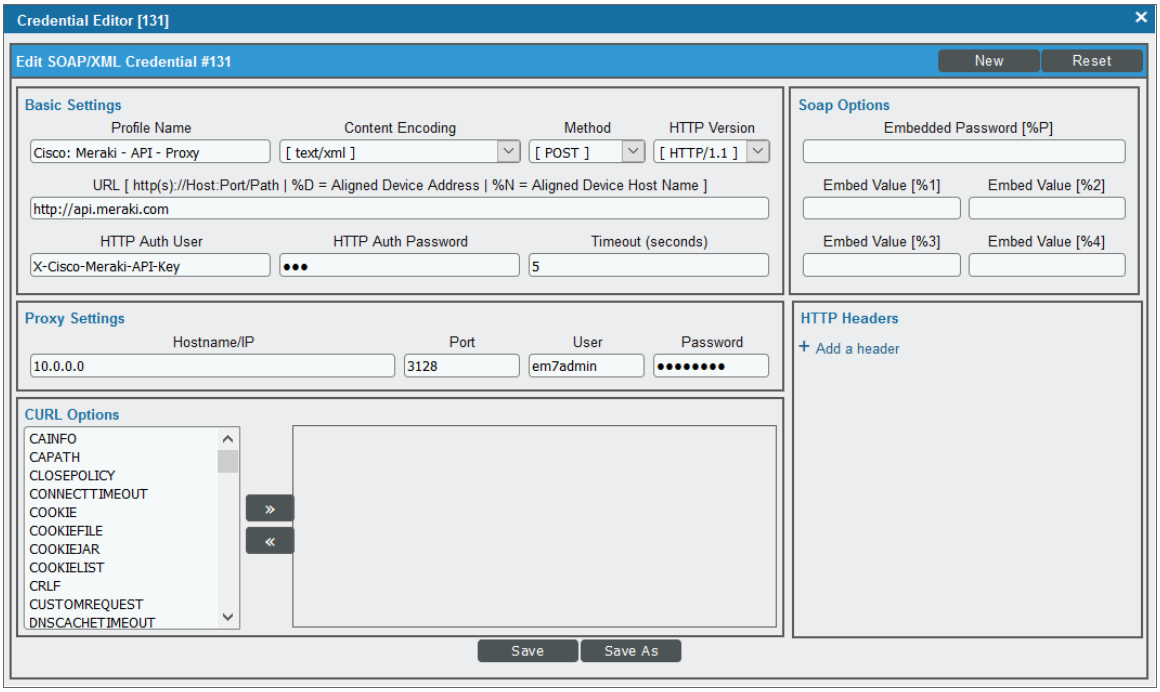
Two example SOAP/XML credentials that you can edit for your own use are included in the PowerPack:

- **Cisco: Meraki - API - Proxy**, for users who connect to Meraki through a third-party proxy server
- **Cisco: Meraki - API (Selective)**, for users who want to discover only some selected devices based on tag values

To define an SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Locate the **Cisco: Meraki - API - Proxy** or **Cisco: Meraki - API (Selective)** credential and click its wrench icon ( ). The **Credential Editor** modal page appears:



3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for your Meraki credential.
- ***HTTP Auth Password***. Type the *Meraki API key*.

> NOTE: You can use the default values for the remaining ***Basic Settings*** fields. You **must** use the default value in the ***URL*** field.

Proxy Settings

> NOTE: You must complete the ***Proxy Settings*** fields only if you connect to the Meraki API through a third-party proxy server. If you do not use a proxy to connect to Meraki, then you can leave these fields blank.

- ***Hostname/IP***. Type the server's hostname or IP address.
- ***Port***. Type the port on the proxy server to which you will connect.
- ***User***. Type the username used to access the proxy server.

- ***Password***. Type the password used to access the proxy server.

HTTP Headers

> **NOTE:** You can add and complete the ***HTTP Headers*** fields if you want to discover only some selected devices based on tag values. If you want to discover all Meraki devices, then you can leave these fields blank.

- ***Add a header***. Click **[Add a header]** once if you want to include tag values for SL1 to match when it discovers Meraki devices, or click **[Add a header]** twice if you want to include tag values and specify that tag-matching should be case-insensitive. In the blank fields that appear, do one or both of the following:
  - Type "tags:" in the first field, followed by one or more tag values. You can include multiple tag values in a string, using comma separators and no spaces. For example: "tags:value1,value2,value3".
  - Type "regex:IGNORECASE" in the second field if you want SL1 to match the tag values regardless of case.

> **NOTE:** If you are using a tag to discover a device and want to discover that device's network, the device and it's network must have the same tag applied.

> **NOTE:** Tag values can include wildcard characters.

> **NOTE:** After initial discovery, you can add more tag values and run discovery again to discover additional component devices. However, if you remove tag values and then run discovery again, the component devices that had been discovered based on the removed tag values will be updated to an unavailable state.

4. Click the **[Save As]** button, and then click **[OK]**.

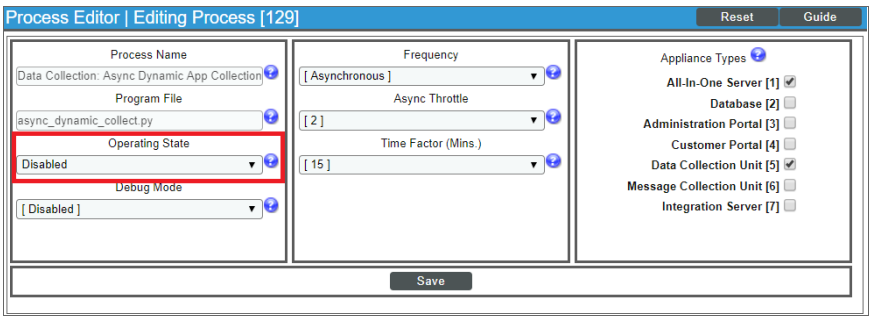
Disabling Asynchronous Dynamic Application Collection

If the Meraki system you want to monitor consists of more than 200 devices, you must disable the "Data Collection: Async Dynamic App Collection" process before discovering your Meraki system.

> **NOTE:** Disabling asynchronous Dynamic Application collection increases the amount of time it takes the ScienceLogic platform to discover all of the component devices in your Meraki system.

To disable asynchronous Dynamic Application collection:

1. Go to the **Process Manager** page (System > Settings > Admin Processes, or System > Settings > Processes in the SL1 classic user interface).
2. Use the ***Process Name*** filter field to search for the "Data Collection: Async Dynamic App Collection" process, and then click its wrench icon ( ). The **Process Editor** page appears.



3. In the ***Operating State*** field, select *Disabled*.
4. Click **[Save]**.

Re-enabling Asynchronous Dynamic Application Collection

If you no longer want to monitor Meraki devices in SL1 and you want to return the system to its original state with asynchronous Dynamic Application collection re-enabled, you must first delete all Meraki devices from the platform. You must then clear the Database Server or Data Collector of any asynchronous processes that are already queued. Failing to do these steps can result in the platform ceasing all data collection until those asynchronous processes are executed.

To re-enable asynchronous Dynamic Application collection:

1. Navigate to the Database Server by typing "<IP address>:8008" into your browser address bar.
2. Log in to the Database Server. The phpMyAdmin browser appears.
3. Select the database from the drop-down ***Database*** field, and then select the **master_logs** database.
4. In the **master_logs** database, select the **spool_process** table on the left menu, and then click the **[SQL]** tab.
5. Run the following query to clear out the processes on the database:

```
DELETE FROM 'spool_process' WHERE 'proc' = 129 AND 'state' != 0;
```

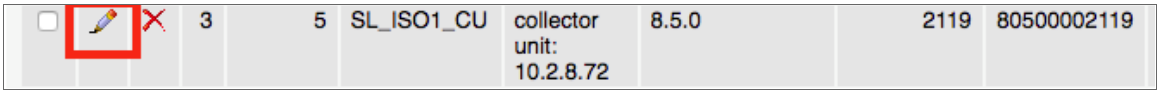
6. Click **[OK]** at the prompt. Many rows should have been deleted from the table.

If you are using a distributed ScienceLogic system, continue with step 7. Otherwise, go to step 14.

7. In the left menu of the phpMyAdmin browser, select the Data Collector appliance where Meraki devices were discovered.

   If the IP address of the Data Collector appears in the upper left-hand corner of the phpMyAdmin browser, go to step 12. Otherwise, if you receive a MySQL error message that your access is denied, continue with step 8.

8. In the Database Server, navigate to the **Master** database and then select the **system_settings_licenses** table.
9. Click **[Browse]** in the upper left-hand side of the page and then identify the Data Collector appliance.
10. Click the **edit** button for the Data Collector:



11. Locate the **db_user** and **db_pass** fields. In those fields, type the same credentials as the Database Server.
12. Click **[Go]**. Wait a few seconds before trying to access the Data Collector in the phpMyAdmin browser. When you do so, the IP address of the Data Collector should appear in the upper left-hand corner of the phpMyAdmin browser.
13. Repeat steps 3-6 on the Data Collector. If successful, many rows should have been deleted from the **spool_process** table.
14. In SL1, go to the **Process Manager** page (System > Settings > Admin Processes, or System > Settings > Processes in the SL1 classic user interface).
15. Use the ***Process Name*** filter field to search for the "Data Collection: Async Dynamic App Collection" process, and then click its wrench icon (). The **Process Editor** page appears.
16. In the ***Operating State*** field, select *Enabled*, and then click **[Save]**.

Discovering Cisco Meraki Component Devices

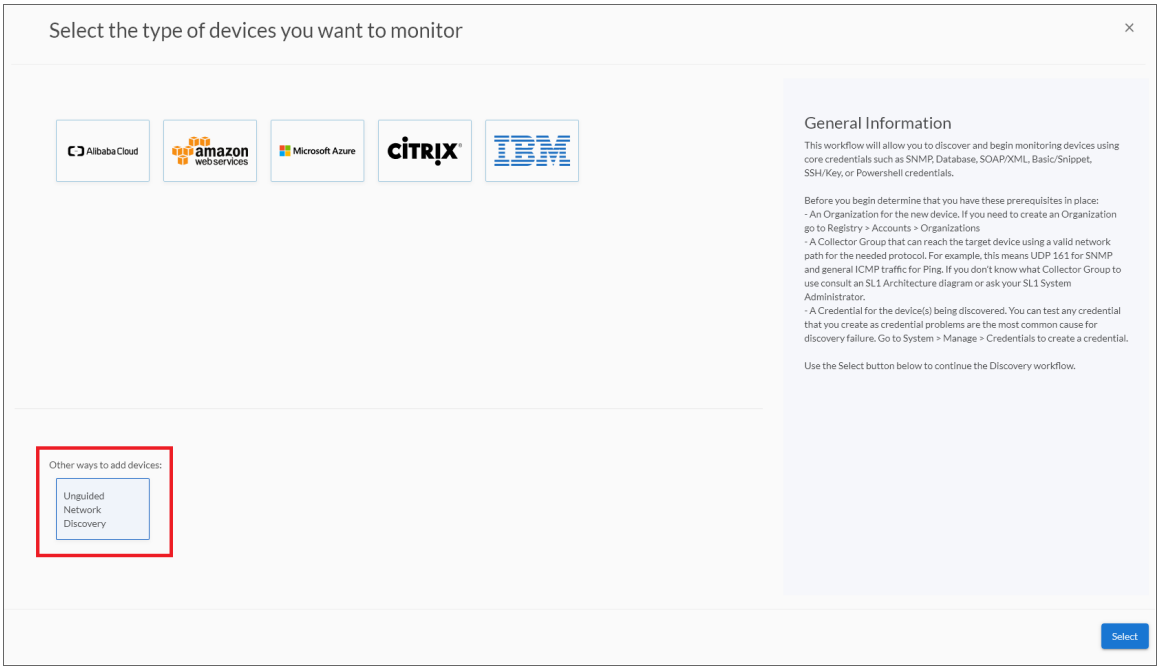
To model and monitor your Cisco Meraki devices, you must run a discovery session to discover your Meraki environment.

When the discovery session first completes, the Meraki system is initially discovered as a pingable physical device. The Run Book Action and Automation policies in the *Cisco: Meraki [API]* PowerPack then create a Meraki Cloud Controller virtual device that acts as the root device for your Meraki system. The Dynamic Applications included in the PowerPack then automatically align to the Cloud Controller virtual device to discover, model, and monitor the remaining Meraki devices.

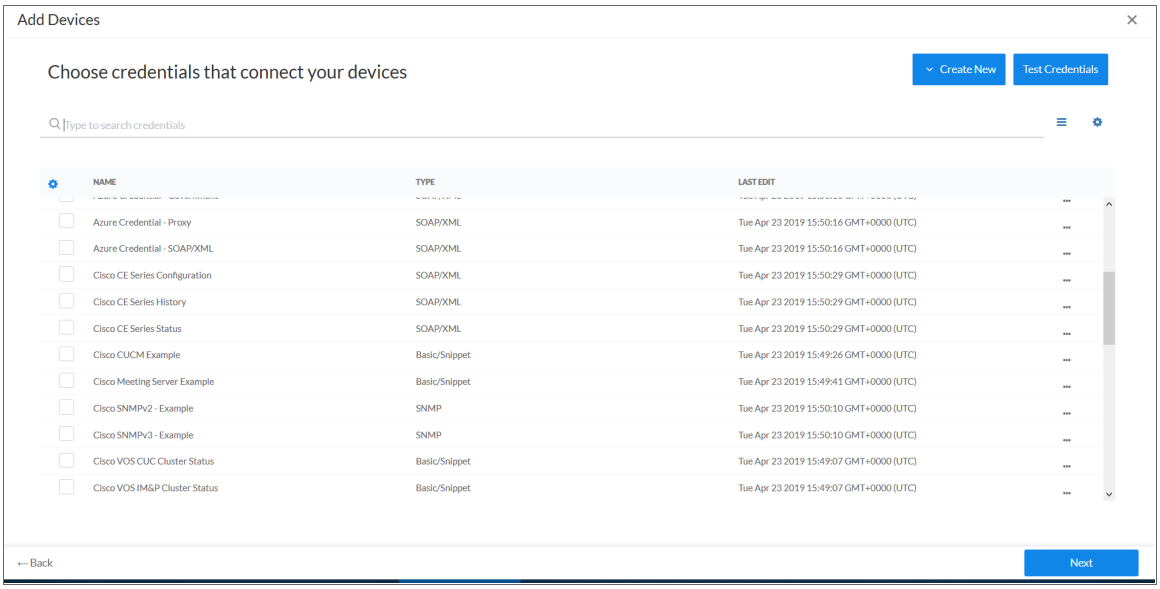
NOTE: If you have a pre-existing device component with an identical name to a Meraki Organization, the "Cisco: Meraki Cloud Controller Discovery" Dynamic Application will show you a false positive message, indicating that the device component was created, but it will fail to create one. This is because the Dynamic Application checks for the existence of the component name and if it finds a matching one, a new component is not created.

To discover the Meraki devices that you want to monitor:

1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



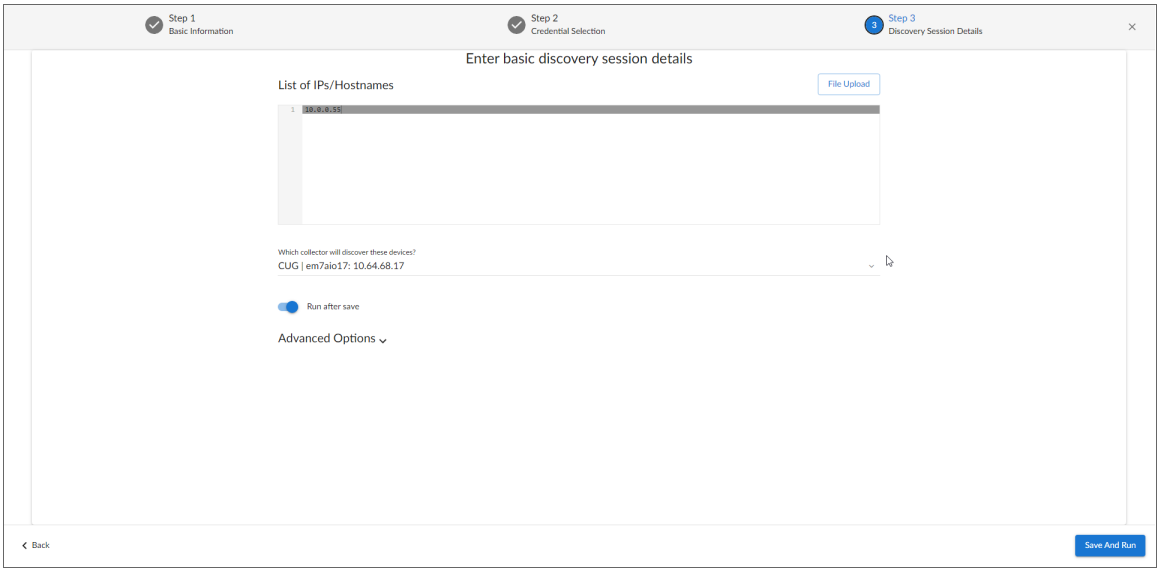
2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears.
4. Complete the following fields:
   - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
   - ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices
5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:



6. On the **Credentials** page, locate and select the ***Basic/Snippet credential*** you created for the Cisco Meraki devices.

NOTE: Do not select a credential in the ***SNMP Credentials*** field, even if you created an SNMP V3 credential for your Meraki devices. The Run Book Action and Automation policies included in the *Cisco: Meraki [API]* PowerPack automatically gather and use the necessary SNMP credential information during discovery.

7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



8. Complete the following fields:

- ***List of IPs/Hostnames***. Type the IP address or hostname for the Cisco Meraki Meraki system that you want to monitor.
- ***Which collector will monitor these devices?***. Required. Select an existing collector to monitor the discovered devices.
- ***Run after save***. Select this option to run this discovery session as soon as you save the session.

  In the **Advanced options** section, click the down arrow icon ( ) to complete the following fields:

  - ***Discover Non-SNMP***. Enable this setting.
  - ***Model Devices***. Enable this setting.

9. Click **[Save and Run]** if you enabled the Run after save setting, or **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.
11. Repeat the above steps for every set of Cisco Meraki devices you want to monitor, using a different credential for each set of devices.

NOTE: ScienceLogic recommends that you delete the physical pingable Meraki device after the platform creates the Cloud Controller virtual device that serves as the Meraki system root device.

NOTE: You can edit the ***Device Name*** of the Meraki Cloud Controller virtual device from the **Device Investigator** page (**Devices** > select the device > click the **[Edit]** button) for that device. This enables you to change the root device's name so that it matches the organization name as the Meraki Controller defines it. The *Cisco: Meraki [API]* PowerPack cannot discover multiple organizations with the same name.

Discovering Cisco: Meraki Component Devices in the SL1 Classic User Interface

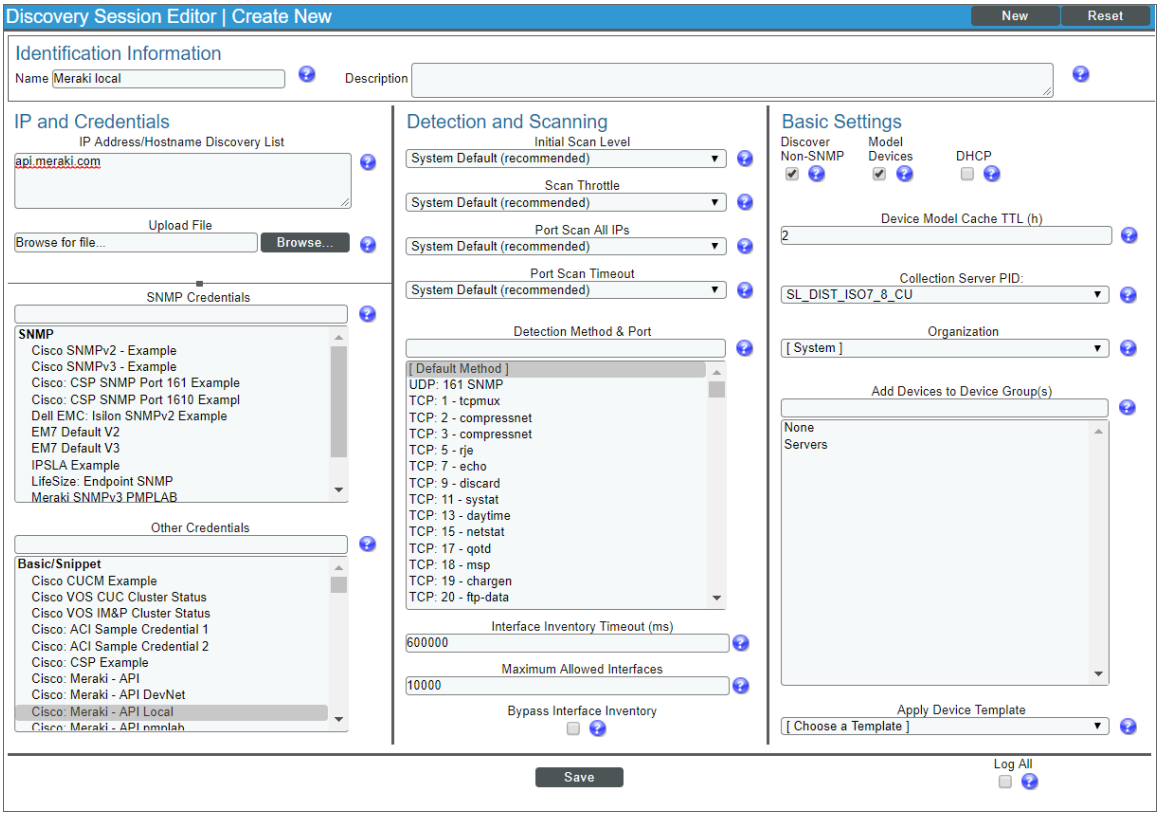
To model and monitor your Cisco Meraki devices, you must run a discovery session to discover your Meraki environment.

When the discovery session first completes, the Meraki system is initially discovered as a pingable physical device. The Run Book Action and Automation policies in the *Cisco: Meraki [API]* PowerPack then create a Meraki Cloud Controller virtual device that acts as the root device for your Meraki system. The Dynamic Applications included in the PowerPack then automatically align to the Cloud Controller virtual device to discover, model, and monitor the remaining Meraki devices.

NOTE: If you have a pre-existing device component with an identical name to a Meraki Organization, the "Cisco: Meraki Cloud Controller Discovery" Dynamic Application will show you a false positive message, indicating that the device component was created, but it will fail to create one. This is because the Dynamic Application checks for the existence of the component name and if it finds a matching one, a new component is not created.

To discover the Meraki devices that you want to monitor:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears.
3. On the **Discovery Session Editor** page, define values in the following fields:



- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type the IP address or hostname for the Cisco Meraki Meraki system that you want to monitor.
- ***Other Credentials***. Select the Basic/Snippet credential you created for Meraki.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

NOTE: Do not select a credential in the ***SNMP Credentials*** field, even if you created an SNMP V3 credential for your Meraki devices. The Run Book Action and Automation policies included in the *Cisco: Meraki [API]* PowerPack automatically gather and use the necessary SNMP credential information during discovery.

4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click **[Save]**, and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon ( ) to run the discovery session.
7. After the virtual device is created and the Cisco Meraki devices are discovered, click the device icon ( ) to view the **Device Properties** page for each device.
8. Repeat steps 2-7 for every set of Cisco Meraki devices you want to monitor, using a different credential for each set of devices.

NOTE: ScienceLogic recommends that you delete the physical pingable Meraki device after the platform creates the Cloud Controller virtual device that serves as the Meraki system root device.

NOTE: You can edit the ***Device Name*** of the Meraki Cloud Controller virtual device from the **Device Properties** page (Registry > Devices > wrench icon). This enables you to change the root device's name so that it matches the organization name as the Meraki Controller defines it. The *Cisco: Meraki [API]* PowerPack cannot discover multiple organizations with the same name.

Viewing Cisco Meraki Component Devices

In addition to the **Devices** page, you can view your Cisco Meraki devices in the following places in the user interface:

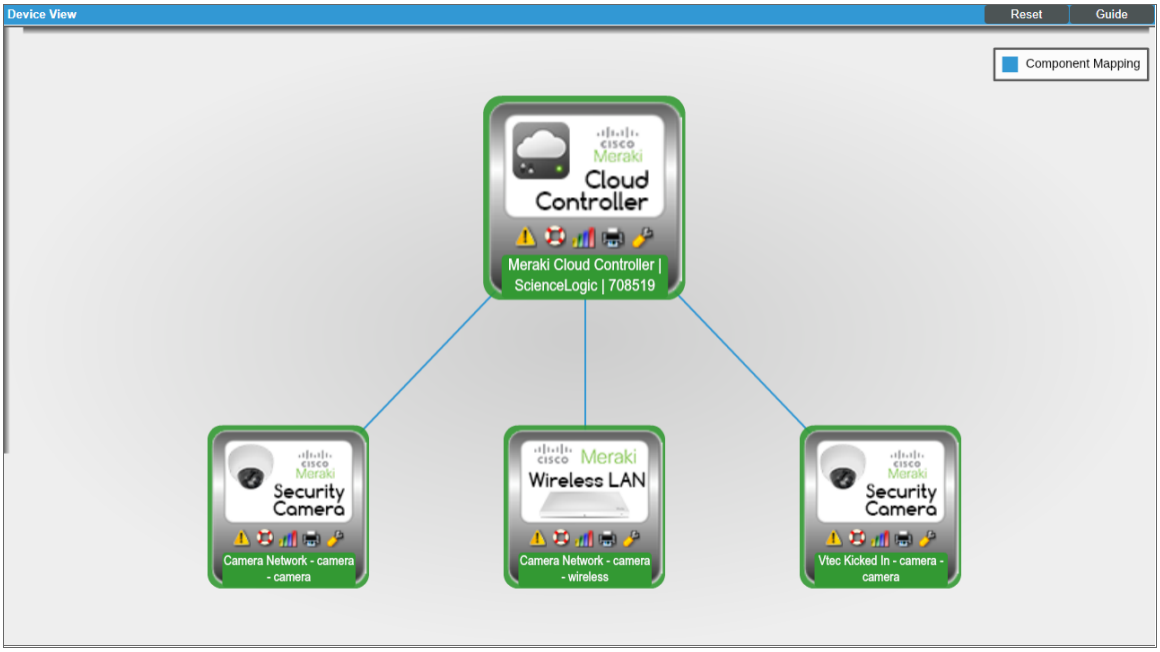
- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device.
- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1. The **Device Components** page displays all root devices and component devices in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a Cisco Meraki device, find the device and click its plus icon (+).

- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for a Cisco Meraki device, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.

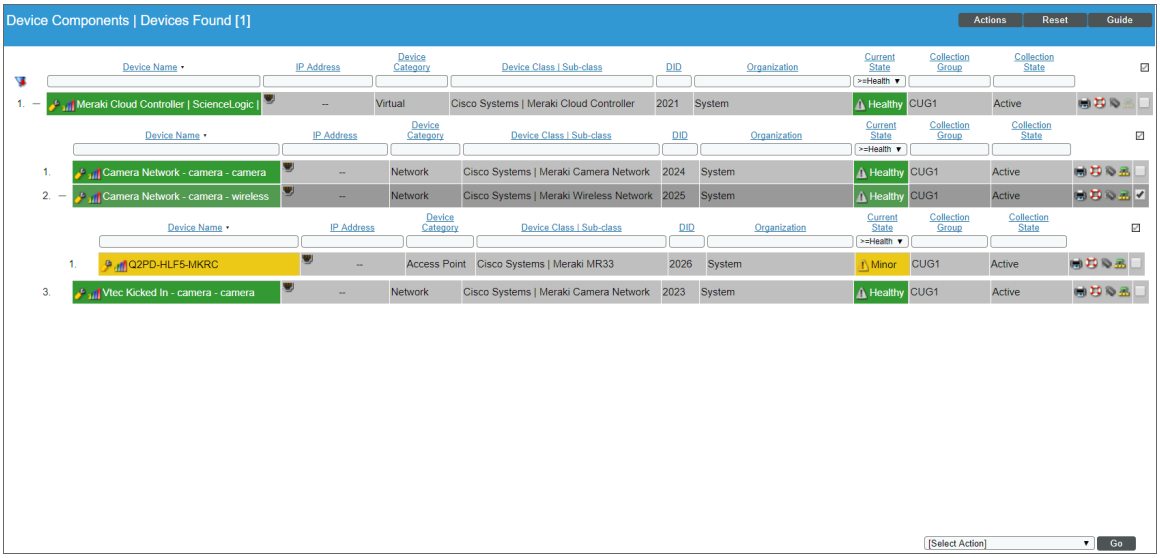
Viewing Cisco Meraki Component Devices in the SL1 Classic User Interface

In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view the Cisco Meraki devices in the following places in the user interface:

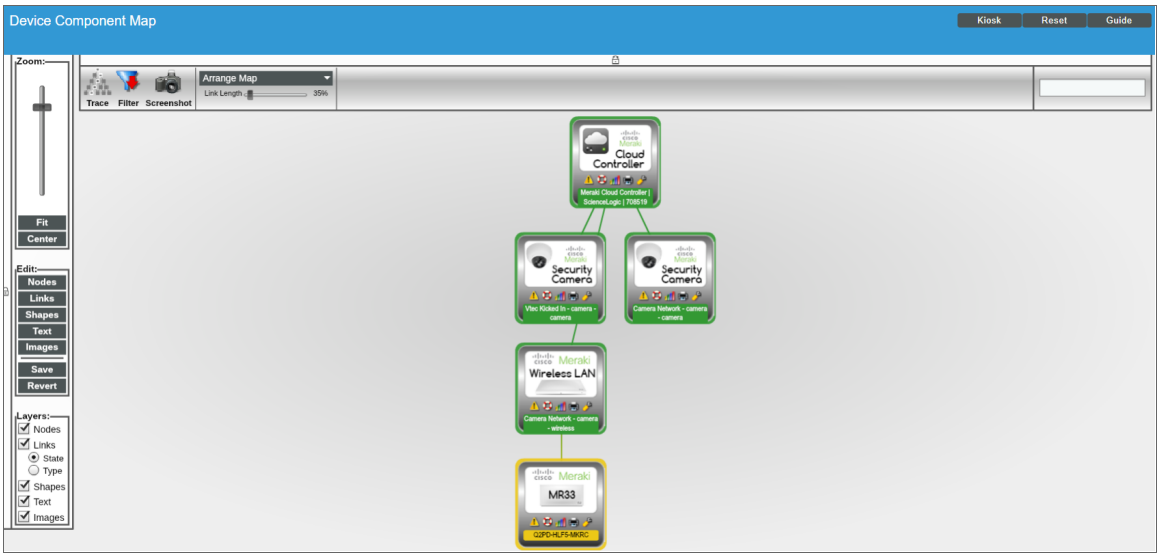
- The **Device View** modal page (click the bar-graph icon [] for a device, then click the **Topology** tab) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by SL1 in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with Cisco Meraki, find the Cisco Meraki root device and click its plus icon (+):



- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for Cisco Meraki devices, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



Creating Events from Cisco Meraki Emails

The *Cisco: Meraki [API]* PowerPack includes Event Policies that can generate events in SL1 based on emails that Cisco Meraki sends to SL1.

For SL1 to process events from inbound emails, you must configure your Meraki devices to send email to SL1 using certain formatting rules.

You must then enable SL1 to generate events from those inbound Meraki emails.

If configured properly, when SL1 domain receives an email with body text that matches a Meraki network component device name and a subject that matches the regular expression (RegEx) pattern of one of the PowerPack's Event Policies, SL1 will generate an event aligned to that network component device.

NOTE: Events from email are always aligned to network devices, even when the email includes references to one or more sub-component devices below the network device.

CAUTION: The email Event Policies included in the *Cisco: Meraki [API]* PowerPack each have an expiry delay setting that specifies the amount of time after which an active event is automatically cleared from SL1 if the event has not reoccurred. However, SL1 clearing an event for reaching its expiry delay setting does not mean that the initial condition that caused the event has been resolved.

Formatting Inbound Emails

Inbound emails must meet the following requirements to be processed as events by SL1:

- The email must be sent to the following address:

  ```
  notify@SL1-domain-name
  ```

  Where "SL1-domain-name" is one of the fully qualified domain names of the Database Server or All-In-One Appliance that is entered in the ***Authorized Email Domains*** field in the **Email Settings** (System > Settings > Email) page.

- The "from" address used by the external device must be "alerts-noreply@meraki.com" for non-maintenance events, "support-noreply@meraki.com" for maintenance events, or otherwise match an address defined in the ***Originator Address*** field in an email redirection policy on the **Emailer Redirection** page Events > Inbound Email, or Registry > Events > Inbound Email in the SL1 classic user interface).
- The email subject line must begin with "Alert for" or "Scheduled maintenance for" and match the regular expression (RegEx) pattern of one of the Event Policies included in the *Cisco: Meraki [API]* PowerPack.

- The email body must include the name of a network device monitored by the SL1 system.

  The following RegEx patterns are used:

  - For scheduled maintenance emails:

```
(Scheduled maintenance for)\s((network\s|\d\snetworks\sin\sorganization\s)"([a-zA-Z0-9_\-\.]+).*")
```

  - For all other emails:

```
(Alert for)\s*([a-zA-Z0-9_\-\.]+)\s*
```

NOTE: There must be a space between the RegEx pattern and the IP address, hostname, or device ID.

NOTE: The Event Policies included in the *Cisco: Meraki [API]* PowerPack ***do not*** include RegEx patterns "out of the box". Users can add or modify Event Policy RegEx patterns to best suit their needs.

NOTE: Emails that do not match the RegEx pattern of any Meraki Event Policy will generate a message in the system log. Emails that do not match the name of any component device in SL1 will not generate any events or messages.

NOTE: You can specify how an Event from Email policy will match a RegEx to a device name in the **Behavior Settings** page (System > Settings > Behavior). For more information, see the ***Configuring Inbound Email*** manual.

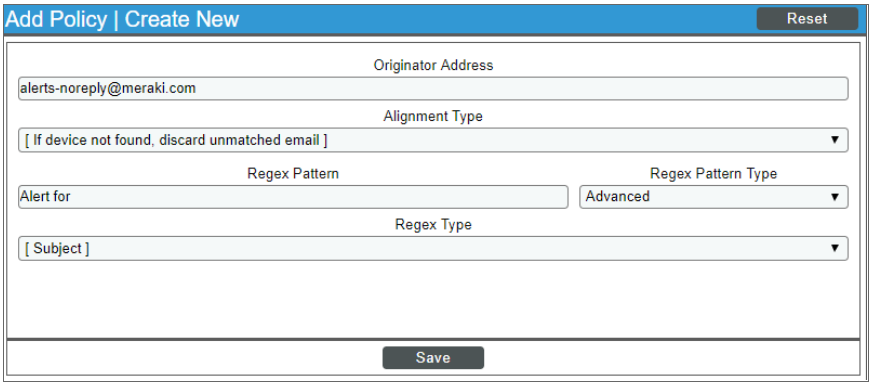
Enabling Inbound Email Alerts

After you have ensured that inbound Meraki emails are formatted correctly, you must enable SL1 to generate events from the inbound Meraki emails.

To do so:

1. Go to the **Emailer Redirection** page (Events > Inbound Email, or Registry > Events > Inbound Email in the SL1 classic user interface), and then click the **[Create]** button. The **Add Policy** modal page appears.

2. Complete the following fields:



- ***Originator Address***. Type "alerts-noreply@meraki.com".
- ***Alignment Type***. Select *If device not found, discard unmatched email*.
- ***Regex Pattern***. Type "Alert for" or "Scheduled maintenance for network".
- ***Regex Pattern Type***. Select *Advanced*.
- ***Regex Type***. Select *Subject*.

3. Click **[Save]**.

> **NOTE:** For more information about generating events from inbound emails, see the ***Configuring Inbound Email*** manual.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010