



Monitoring Cisco Meraki (API)

Beta Version

Cisco: Meraki [API] PowerPack version 103

Table of Contents

Introduction	3
What is Cisco Meraki?	3
What Does the Cisco: Meraki [API] PowerPack Monitor?	4
Installing the Cisco: Meraki [API] PowerPack	4
Configuring Cisco Meraki for Monitoring	6
Generating a Cisco Meraki API Key	6
Creating a Basic/Snippet Credential	9
Creating an SNMP V3 Credential	10
Creating a SOAP/XML Credential	11
Disabling Asynchronous Dynamic Application Collection	13
Re-enabling Asynchronous Dynamic Application Collection	14
Discovering Cisco Meraki Component Devices	15
Viewing Cisco Meraki Component Devices	17
Creating Events from Cisco Meraki Emails	19
Formatting Inbound Emails	19
Enabling Inbound Email Alerts	20

Chapter 1

Introduction

Overview

This manual describes how to monitor Cisco Meraki access points, switches, phones, and cameras in the ScienceLogic platform 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*:

<i>What is Cisco Meraki?</i>	3
<i>What Does the Cisco: Meraki [API] PowerPack Monitor?</i>	4
<i>Installing the Cisco: Meraki [API] PowerPack</i>	4

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 the ScienceLogic platform 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 the ScienceLogic platform 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

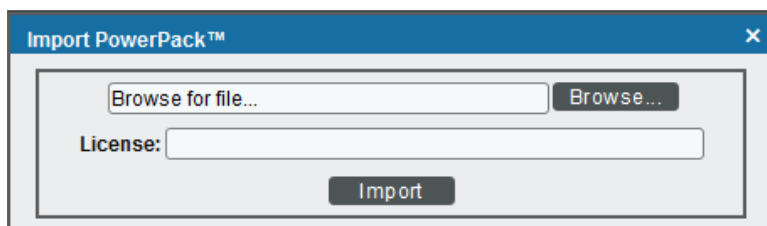
Installing the Cisco: Meraki [API] PowerPack

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 in 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 Customer Portal](#).
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 page appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal page 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 page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Configuring Cisco Meraki for Monitoring

Overview

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

<i>Generating a Cisco Meraki API Key</i>	6
<i>Creating a Basic/Snippet Credential</i>	9
<i>Creating an SNMP V3 Credential</i>	10
<i>Creating a SOAP/XML Credential</i>	11
<i>Disabling Asynchronous Dynamic Application Collection</i>	13
<i>Re-enabling Asynchronous Dynamic Application Collection</i>	14
<i>Discovering Cisco Meraki Component Devices</i>	15
<i>Viewing Cisco Meraki Component Devices</i>	17
<i>Creating Events from Cisco Meraki Emails</i>	19
<i>Formatting Inbound Emails</i>	19
<i>Enabling Inbound Email Alerts</i>	20

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 the ScienceLogic platform to monitor Meraki.

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

However, if you want each Meraki organization to have its own corresponding ScienceLogic organization in the platform, ScienceLogic recommends creating a unique read-only user account and API key for each organization in Meraki. You can then create separate credentials in the platform 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:

The screenshot shows a modal window titled "Create administrator" with a close button (x) in the top right corner. The form contains the following elements:

- Name:** A text input field.
- Email:** A text input field.
- Organization access:** A dropdown menu currently showing "Read-only".
- Table:** A table with two columns: "Target" and "Access". Below the table is a green link: "+ Add access privileges".
- Footer:** A "privacy" link on the left, and "Close" and "Create admin" buttons on the right.

- **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.

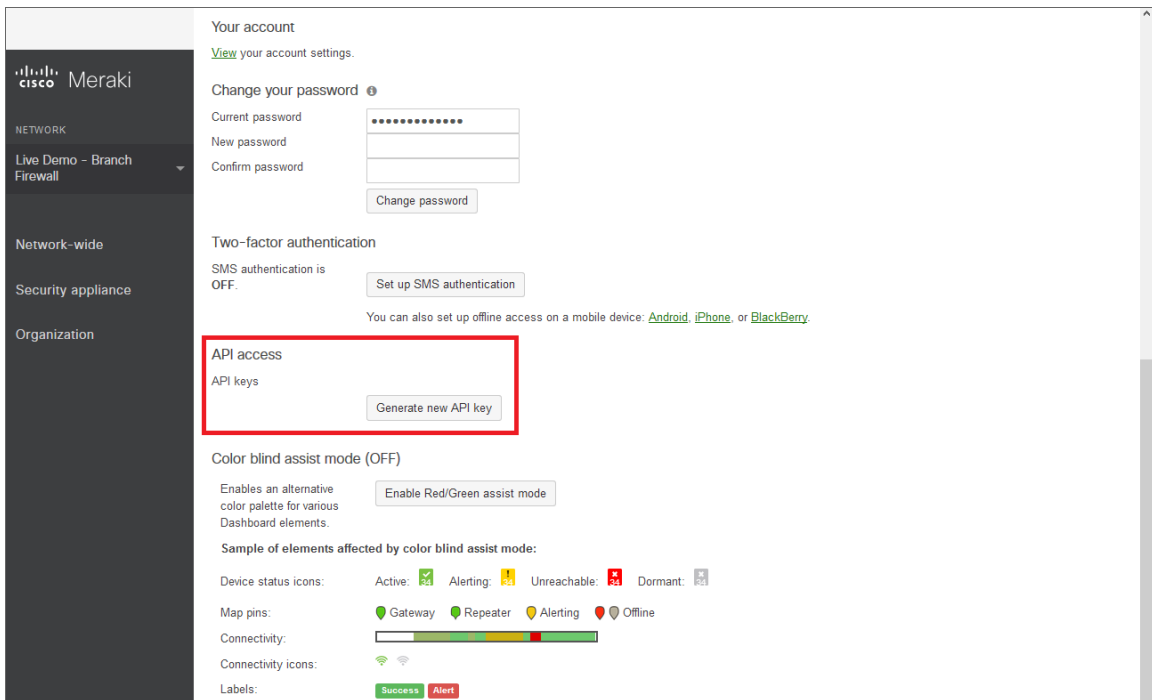
To generate a Cisco Meraki API key for that read-only user:

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.

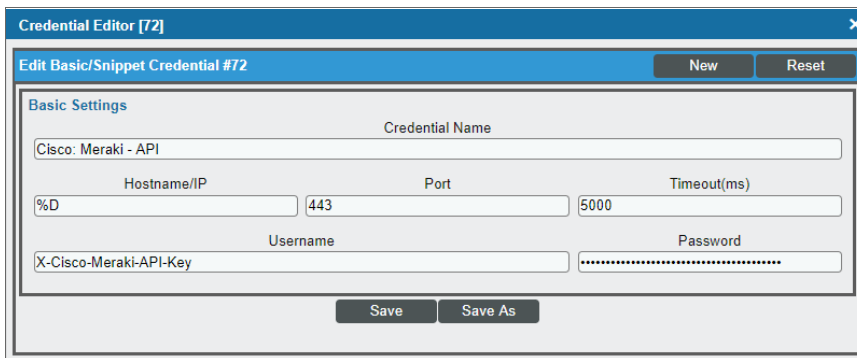
NOTE: API keys are visible only to the user that created them.

Creating a Basic/Snippet Credential

To configure the ScienceLogic platform 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:



The screenshot shows a modal window titled "Credential Editor [72]" with a sub-header "Edit Basic/Snippet Credential #72". It contains a form with the following fields and values:

Basic Settings			
Credential Name			
Cisco: Meraki - API			
Hostname/IP	Port	Timeout(ms)	
%D	443	5000	
Username		Password	
X-Cisco-Meraki-API-Key		

Buttons: New, Reset, Save, Save As

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

2

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:

The screenshot shows a 'Credential Editor' window with a 'Create New SNMP Credential' modal. The modal is divided into three sections: 'Basic Settings', 'SNMP V1/V2 Settings', and 'SNMP V3 Settings'. The 'Basic Settings' section includes fields for Profile Name (Cisco SNMPv3 Local Meraki), SNMP Version (SNMP V3), Port (16100), Timeout(ms) (3000), and Retries (3). The 'SNMP V1/V2 Settings' section includes fields for SNMP Community (Read-Only) and SNMP Community (Read/Write). The 'SNMP V3 Settings' section includes fields for Security Name, Security Passphrase, Authentication Protocol (SHA), Security Level (Authentication and Encryption), SNMP v3 Engine ID, Context Name, Privacy Protocol (AES), and Privacy Protocol Pass Phrase. A 'Save' button is at the bottom.

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]**.

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.

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 the ScienceLogic platform 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. If you want to include multiple tag values, include them in the same field, separating each value with a comma. You should not include spaces between "tags" and the values, nor between the values themselves. For example: "tags:value1,value2,value3".
 - Type "regex:IGNORECASE" in the second field if you want the platform to match the tag values regardless of case.

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 > Processes).

- 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.

The screenshot shows the 'Process Editor | Editing Process [129]' window. It has a 'Reset' and 'Guide' button in the top right. The main area is divided into three columns. The first column contains 'Process Name' (Data Collection: Async Dynamic App Collection), 'Program File' (async_dynamic_collect.py), 'Operating State' (Disabled, highlighted with a red box), and 'Debug Mode' ([Disabled]). The second column contains 'Frequency' ([Asynchronous]), 'Async Throttle' ([2]), and 'Time Factor (Mins.)' ([15]). The third column contains 'Appliance Types' with a list of checkboxes: All-In-One Server [1] (checked), Database [2] (unchecked), Administration Portal [3] (unchecked), Customer Portal [4] (unchecked), Data Collection Unit [5] (checked), Message Collection Unit [6] (checked), and Integration Server [7] (unchecked). A 'Save' button is at the bottom center.

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

Re-enabling Asynchronous Dynamic Application Collection

If you no longer want to monitor Meraki devices in the ScienceLogic platform 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:

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

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



- 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.

- 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:

<input type="checkbox"/>			3	5	SL_ISO1_CU	collector unit: 10.2.8.72	8.5.0	2119	80500002119
--------------------------	-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	---	---	------------	------------------------------	-------	------	-------------

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 the ScienceLogic platform, go to the **Process Manager** page (System > Settings > Processes).
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.

To discover the Meraki devices that you want to monitor:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears.

- On the **Discovery Session Editor** page, define values in the following fields:


The screenshot shows the 'Discovery Session Editor | Editing Session [1]' interface. It is divided into four main sections:


- Identification Information:** Includes fields for 'Name' (set to 'Meraki local') and 'Description'.
- IP and Credentials:** Contains 'IP Address/Hostname Discovery List' (set to 'snmp.meraki.com'), 'SNMP Credentials' (with a list including 'Cisco SNMPv2 - Example' and 'Cisco SNMPv3 Local Meraki'), and 'Other Credentials' (with a list including 'Cisco: Meraki - API local').
- Detection and Scanning:** Includes 'Initial Scan Level', 'Scan Throttle', 'Port Scan All IPs', and 'Port Scan Timeout' (all set to 'System Default (recommended)'). It also features a 'Detection Method & Port' list with options like 'UDP: 161 SNMP' and 'TCP: 1 - tcpmux'. Other fields include 'Interface Inventory Timeout (ms)' (600000), 'Maximum Allowed Interfaces' (10000), and a 'Bypass Interface Inventory' checkbox.
- Basic Settings:** Includes checkboxes for 'Discover Non-SNMP' and 'Model Devices' (both checked), and 'DHCP' (unchecked). It also has fields for 'Device Model Cache TTL (h)' (2), 'Collection Server PID: 3', 'Organization' (set to '[System]'), and an 'Add Devices to Device Group(s)' list (currently empty).

At the bottom, there are 'Save' and 'Save As' buttons, and a 'Log All' checkbox.

- **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.

- 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.
- Click **[Save]**, and then close the **Discovery Session Editor** window.
- 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.

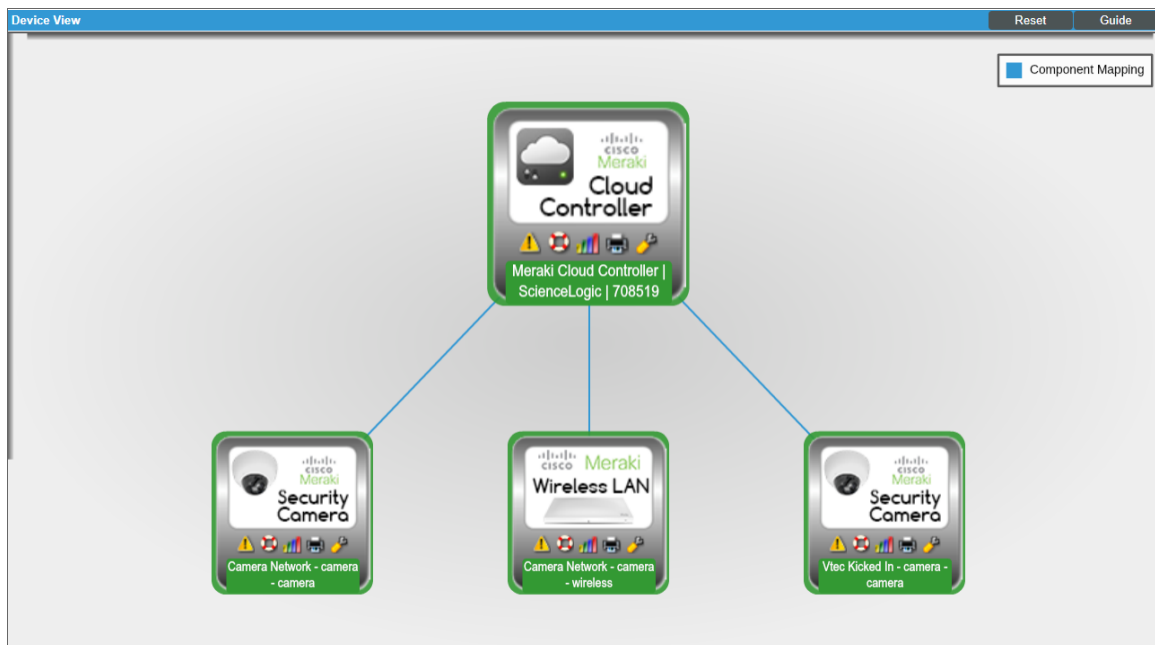
NOTE: ScienceLogic recommends that you delete the physical pingable Meraki device after the platform creates the Cloud Controller virtual device that serves as the Meraki system root device.

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 **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:

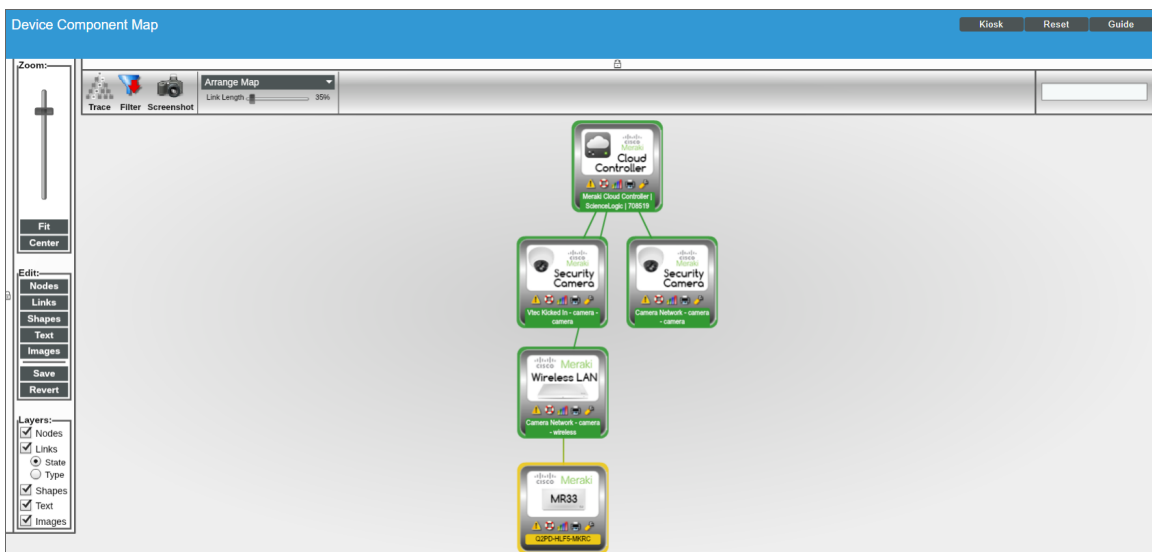


- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by the ScienceLogic platform in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices.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

Device Components | Devices Found [1]

Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Current State	Collection Group	Collection State
Meraki Cloud Controller ScienceLogic	--	Virtual	Cisco Systems Meraki Cloud Controller	2021	System	Healthy	CUG1	Active
Camera Network - camera - camera	--	Network	Cisco Systems Meraki Camera Network	2024	System	Healthy	CUG1	Active
Camera Network - camera - wireless	--	Network	Cisco Systems Meraki Wireless Network	2025	System	Healthy	CUG1	Active
Q2PD-HLFS-MKRC	--	Access Point	Cisco Systems Meraki MR33	2026	System	Minor	CUG1	Active
Vtc-Kicked In - camera - camera	--	Network	Cisco Systems Meraki Camera Network	2023	System	Healthy	CUG1	Active

- The **Component Map** page (Views > 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. The ScienceLogic platform 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 the ScienceLogic platform based on emails that Cisco Meraki sends to the platform.

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

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

If configured properly, when the ScienceLogic platform 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, the platform 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 the ScienceLogic platform if the event has not reoccurred. However, the platform 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 the platform:

- The email must be sent to the following address:

`notify@domain-name-of-ScienceLogic-platform`

Where "domain-name-of-ScienceLogic-platform" 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", or otherwise match an address defined in the **Originator Address** field in an email redirection policy on the **Mailer Redirection** page (Registry > Events > Inbound Email).
- The email subject line must begin with "Alert for" or "Scheduled maintenance for network" 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 ScienceLogic system.

The following RegEx patterns are used:

- For scheduled maintenance emails:

```
(Scheduled maintenance for network)\s*"([a-zA-Z0-9_-\.\.])"\s*
```

- 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 the ScienceLogic platform 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 the platform to generate events from the inbound Meraki emails.

To do so:

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

2. Complete the following fields:

The screenshot shows a configuration form titled "Add Policy | Create New" with a "Reset" button in the top right corner. The form contains the following fields:

- Originator Address:** A text input field containing "alerts-noreply@meraki.com".
- Alignment Type:** A dropdown menu with the selected option "[If device not found, discard unmatched email]".
- Regex Pattern:** A text input field containing "Alert for".
- Regex Pattern Type:** A dropdown menu with the selected option "Advanced".
- Regex Type:** A dropdown menu with the selected option "[Subject]".

A "Save" button is located at the bottom center of the form.

- **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.

© 2003 - 2018, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

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