



HOW-TO GUIDE

# N-central Cisco Meraki Integration



*Last updated:  
November 20,  
2020*

# Table of Contents

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
<b>2</b>	<b>WHAT'S INCLUDED</b>	<b>1</b>
<b>3</b>	<b>GETTING ORGANIZATION ID, NETWORK ID, DEVICE SERIAL NUMBERS</b>	<b>2</b>
<b>4</b>	<b>CREATING THE CUSTOM PROPERTIES</b>	<b>3</b>
<b>5</b>	<b>IMPORTING THE SERVICE TEMPLATE INTO N-CENTRAL</b>	<b>4</b>
<b>6</b>	<b>CONFIGURING ALERTING/TICKETING</b>	<b>6</b>
	Importing the Filter	
	Creating the Rule	
	Creating the Notification Template	
<b>7</b>	<b>ADDING A MERAKI DEVICE INTO N-CENTRAL</b>	<b>8</b>
<b>8</b>	<b>VERIFYING MONITORING IS AUTOMATICALLY APPLIED</b>	<b>8</b>
<b>9</b>	<b>APPENDIX: CUSTOM SERVICE DETAILS</b>	<b>9</b>

# Introduction

This document will guide you through configuring N-central to monitor your customer's Cisco® Meraki environments. Once you've completed all the steps in this document, your N-central® server will be optimally configured for Meraki, to help you minimize the steps to onboard new Meraki environments, and standardize how monitoring and alerting is deployed within your N-central environment.

This document is intended for a technical audience familiar with administering both N-central and Cisco Meraki devices. Your N-central server must be running at least N-central version 2020.1, and the monitoring device should be running at least PowerShell Version 5.1.

## What's Included

This package includes the following items:

- **A filter that finds Meraki devices.** This filter can be imported into your N-central server and will be used to automatically assign monitoring to your customer's Meraki cloud environments.
- **11 Custom Services.** The Services including the word "Device" focus on device-level monitoring, and services including the word "Organization" focus on organization-level monitoring:
  - Meraki - Device Cumulative Bandwidth
  - Meraki - Device Performance Score
  - Meraki - Network Appliance Uplink Status
  - Meraki - Network Devices Connectivity Status
  - Meraki - Organization Appliance Uplink Status
  - Meraki - Organization Devices Connectivity Status
  - Meraki - Organization License Details
  - Meraki - Organization Security Events
  - Meraki - Switch Port Status
  - Meraki - Switch Status (Bandwidth and Connectivity)
  - Meraki - WAP Wi-Fi Networks Detail
- **One Service Template**

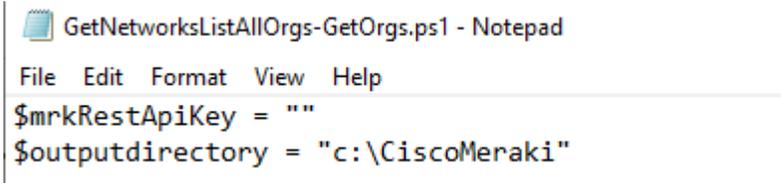
# Getting Organization ID, Network ID, and Device Serial Numbers

The Cisco Meraki web UI publishes the device serial number, and it can be obtained by going to the Meraki UI and looking at a device. The serial number will look like this “AAAA-AAAA-AAAA”

The UI does not publish the Organization ID or the Network ID, so we have created a PowerShell Script attached to this which will return all organizations and all networks in an output text file.

To use it:

1. Edit the script called “GetNetworksListAllOrgs-GetOrgs.ps1”
2. Enter the res API key between the quotation marks on line 1.



```
GetNetworksListAllOrgs-GetOrgs.ps1 - Notepad
File Edit Format View Help
$mrkRestApiKey = ""
$outputdirectory = "c:\CiscoMeraki"
```

3. On line 2, the output directory is set to c:\CiscoMeraki. Either create it on your computer or change the folder path on line 2 to a path that exists. This is where the text file will be created.
4. Then save the file
5. Finally run the script on your computer. The easiest option is to open the file in PowerShell ISE and run the file.
6. This will output several text files on the output folder set on step 3. Open them to see the network IDS. The network id will look like this: “L\_11111111111”

Those numbers must be used in the custom properties in subsequent steps.

# Creating Custom Properties

The Meraki Custom Services need several values to be populated, as they are unique to your customer's Meraki environments. SolarWinds recommends creating the following Custom Properties:

NAME	PROPERTY LEVEL	DATA TYPE	DEFAULT VALUE
<b>Meraki - Device Serial Number</b>	Device	Text	No default value
<b>Meraki - API Key</b>	Organization	Password	No default value
<b>Meraki - Organization ID</b>	Organization	Text	No default value
<b>Meraki - Device Network ID</b>	Device	Text	No default value

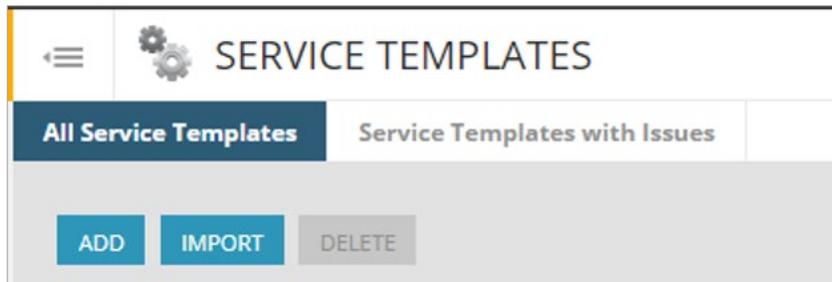
You can create Custom Properties by completing the following steps:

1. Log in to the N-central UI.
2. At the SO or System level, navigate to the **Administration -> Custom Properties** screen.
3. To create the **Meraki - Device Serial Number** custom property, click the **Add -> By Devices -> Text Type** option, and fill in the required fields.
4. To create the two organization-level custom properties, click the **Add -> By Customer** option, and choose either **Text** or **Password**, as required.
5. Finally, go to each Customer/Site, and configure the **Meraki API Key and Meraki Organization ID** custom properties with the values appropriate for those customers.

# Importing the Service Template into N-central

This package includes the XML files for each Custom Service and a Service Template ZIP file that can be used to upload all the Custom Services in one step. If you don't want to use the included Service Template, you can upload the custom services individually, via the **Administration -> Service Management -> Custom Services** screen. Importing the Service Template ZIP file is the most efficient

1. Log in to the N-central UI
2. At the SO or System level, navigate to the **Configuration -> Monitoring -> Service Templates** screen



3. 1. Click the **Import** button
4. 2. Click the **Browse...** button, and select "Cisco Meraki Service Template.zip" file



5. Click the **Import Service Template** button
6. The Custom Services require their Input Parameters to be mapped to the Custom Properties you created earlier, and you'll be prompted to configure those settings. Each Custom Service that needs to be configured will have a red "!" icon beside its name:

Before this Service Template can be saved, you must address the issues with the highlighted services below.

Error	Name	Service	Action	Automatically add new instances
<input type="checkbox"/>	<span style="color: red;">!</span> Meraki - Device Cumulative Bandwidth	Meraki - Device Cumulative Bandwidth - 24 Hrs	✎ Add or Modify	<input type="checkbox"/> OFF
<input type="checkbox"/>	<span style="color: red;">!</span> Meraki - Device Cumulative Bandwidth 2	Meraki - Device Cumulative Bandwidth - 15 Mins	✎ Add or Modify	<input type="checkbox"/> OFF
<input type="checkbox"/>	<span style="color: red;">!</span> Meraki - Device Cumulative Bandwidth 3	Meraki - Device Cumulative Bandwidth - 1 Hr	✎ Add or Modify	<input type="checkbox"/> OFF
<input type="checkbox"/>	<span style="color: red;">!</span> Meraki - Device Cumulative Bandwidth 4	Meraki - Device Cumulative Bandwidth - 1 Week	✎ Add or Modify	<input type="checkbox"/> OFF
<input type="checkbox"/>	<span style="color: red;">!</span> Meraki - Device Performance Score	Meraki - Device Performance Score	✎ Add or Modify	<input type="checkbox"/> OFF
<input type="checkbox"/>	<span style="color: red;">!</span> Meraki - Network Appliance Uplink Status	Meraki - Network Appliance Uplink Status	✎ Add or Modify	<input type="checkbox"/> OFF
<input type="checkbox"/>	<span style="color: red;">!</span> Meraki - Network Devices Connectivity Status	Meraki - Network Devices Connectivity Status	✎ Add or Modify	<input type="checkbox"/> OFF



- To configure each Custom Service, click on the name of the Custom Service and then fill in the Input Parameters:

**INPUT PARAMETERS** ?

Input Parameter	Select or Enter Value
Meraki Device Serial	<input type="radio"/> <input style="width: 100%;" type="text" value="aaaa-aaaa-aaaa"/> <input checked="" type="radio"/> Meraki - DeviceSerial <span style="float: right;">▼</span>
Meraki API Key	<input type="radio"/> <input style="width: 100%;" type="text" value="(unchanged)"/> <input type="checkbox"/> Show Password <input checked="" type="radio"/> Meraki - APIKey <span style="float: right;">▼</span>

- Click the **Save** button once you've configured the Input Parameters and repeat those steps for the remaining Custom Services
- Once the Custom Services are configured, click the **Save** button to finish importing the Service Template

(OPTIONAL)

**CONFIGURING THE CUSTOM SERVICES FOR USE OUTSIDE OF A SERVICE TEMPLATE**

If you plan to use the Meraki Custom Services outside of the Service Template, you'll need to edit each one so it references the appropriate Custom Property. This will save you and your technicians from having to manually and repeatedly configure these settings each time you deploy the Custom Service.

- Log in to the N-central UI
- At the SO or System level, navigate to the **Administration -> Service Management -> Custom Services** screen
- Locate the first Meraki Custom Service, click on its name, and configure the Input Parameters so they reference the appropriate Custom Properties
- Click the **Save** button
- Repeat steps 3 and 4 for each of the remaining Meraki Custom Services

# Configuring Alerting/Ticketing

In order for N-central to alert you when there's an issue detected in one of your customer's Meraki environments, you must configure the appropriate Filter, Notification Profile, and Rule.

## IMPORTING THE FILTER

1. Log in to the N-central UI
2. At the SO level, navigate to the **Configuration -> Filters** screen
3. Click the **Import** button and import the Filter ZIP file included in the Meraki monitoring bundle

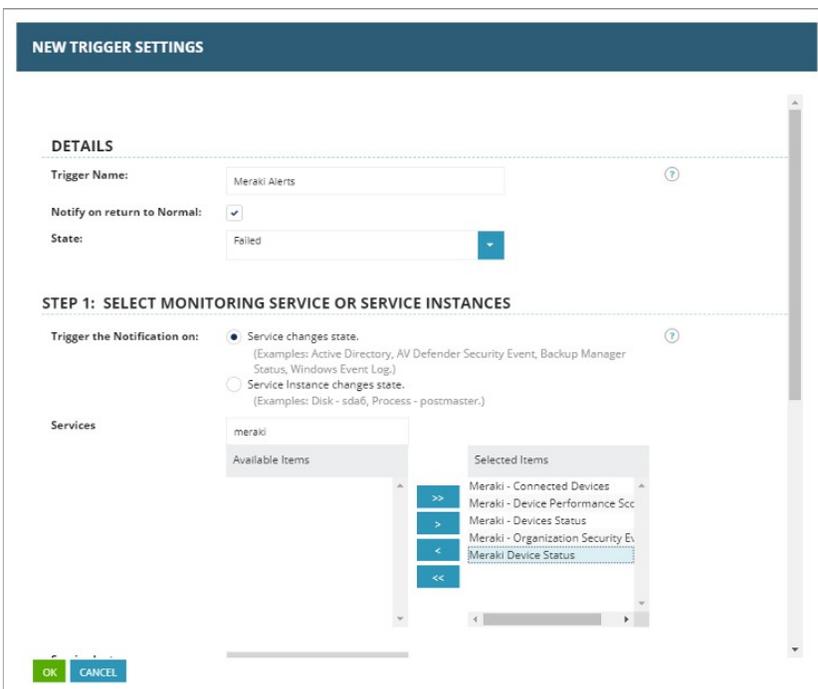
## CREATING THE RULE

4. At the SO level, navigate to the **Configuration -> Monitoring -> Rules** screen
5. Click the Add button
6. Configure the Rule as follows:
  - **Name:** Meraki Devices
  - **Description:** Applies monitoring to Meraki devices
  - On the **Devices to Target** tab, select the **Meraki Devices** filter
  - On the **Monitoring Options** tab, move the **Meraki service template** to the **Selected Service Templates** widget
  - On the **Grant Customers & Sites Access** tab, choose to propagate the Rule to the appropriate Customers and Sites
  - Click the **Save** button

## CREATING THE NOTIFICATION TEMPLATE

1. At the SO level, navigate to the **Configuration -> Monitoring -> Notifications** screen
2. Click the **Add Notification** button
3. Specify "Meraki Notifications" as the Name of the Notification Profile, and keep the default **Single Device, Single Service** Notifications profile type
4. Configure the Primary Notification section as appropriate for your environment

5. Click **Save and Continue**
6. On the Trigger Details tab, click the **Add** button
7. Configure the Notification Trigger with the following properties:
  - **Trigger Name:** Meraki Alerts
  - **Notify on Return to Normal:** Yes
  - **State:** Failed
  - **Services:** Filter to find all the Meraki Custom Services, and move them to the Select Items widget



- In **Step 2: Apply the Notification Trigger to the Selected Devices** section, move the Rule you created earlier to the Selected Items widget
- Click the **OK** button

# Adding a Meraki Device Into N-central

Create a device per Customer/Site to represent your customer's Meraki environment.  
Add the Meraki Custom Services to this device.

## CREATING THE RULE

1. At the Customer or Site level, navigate to the **Actions -> Add/Import Devices** screen
2. Click the **More Options** bar, and then click the **Add Device** button, under the **Manually Create a Device that Represents an External Website or IP Address** section



3. Configure the device as follows:
  - **Given Name:** Meraki Environment
  - **Device Class:** Switch/Router
  - **Network Address:** Specify the URL of your customer's Meraki cloud environment
  - **License Mode:** Professional Mode
4. Click the **Save** button

## Verifying Monitoring Is Automatically Applied

The final step is to verify the Meraki Custom Services were successfully applied to the Meraki device you created, confirm there are no remaining configuration steps, and confirm the Custom Services are reporting accurate data.

1. At the Customer or Site level, navigate to the **Views -> All Devices** View screen
2. Click into the Meraki device
3. Navigate to the **Monitoring** tab
4. Verify the Meraki services are present
5. Verify each Meraki service is reporting back valid/accurate data for your customer's Meraki environment

## Appendix: Custom Service Details

### MERAKI – DEVICE CUMULATIVE BANDWIDTH

This service is used to capture several bandwidth and client-related metrics for a specific Meraki device. It can be applied multiple times to a device with different timeframes. The default template applies it 4 different times with 15 minutes, 1hr, 24hrs, and 1 week.

#### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1a23a5a 135a135a1833a189a 3518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Device Serial</b>	String	AAAA-AAAA-AAAA	This is the unique device serial as found in the portal.
<b>How Many Hours to Look Back</b>	Number	24	This is the desired timeframe to get data. The service will go back up to 1 week.

#### Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Total Devices Connected in the Selected Timeframe</b>	Number	This is the number of devices connected to that Meraki device in the selected time.
<b>Total Bandwidth (GB) for the Selected Timeframe</b>	Number	This is the total combined (sent + received) traffic for the selected time. This is useful to see if a specific device is getting higher usage than usual, or if a device is overused.
<b>Total Received Bandwidth (GB) for the Selected Timeframe</b>	Number	This is the total incoming traffic for the device for the selected time.
<b>Total Sent Bandwidth (GB) for the Selected Timeframe</b>	Number	This is the total outgoing traffic for the device for the selected time.
<b>Top 5 Connected Devices by Total Bandwidth for the Selected Timeframe</b>	String	This returns the 5 devices that used the most GB during the selected time. It returns the device name, IP, and total bandwidth in GB.

*Continued:*

<b>APIErrors</b>	String	This returns any errors provided by the API calls.
------------------	--------	--

## MERAKI – DEVICE PERFORMANCE SCORE

This service is used to capture the performance score as reported by Cisco. The score will be a 0 to 100 value, with 100 indicating the device is fully utilized and at capacity.

### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1a23 a5a135a135a1833 a189a3518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Network ID</b>	String	L_111111111	This is the unique Network ID which typically looks like the format in the example. This should match the device serial. If the device is in a different network than what is entered here, the service will fail.
<b>Device Serial</b>	String	AAAA-AAAA-AAAA	This is the unique device serial as found in the portal.

### Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Performance Score</b>	Number	This is a 0 – 100 numeric value.
<b>Api Errors</b>	String	This returns any errors provided by the API calls.

## MERAKI – NETWORK APPLIANCE UPLINK STATUS

This service looks at a specific Meraki network and returns information about all the devices with uplink and checks if they are working properly (WAN/Cellular WAN).

### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1a23 a5a135a135a1833 a189a3518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Organization ID</b>	String	12345	This is the unique Meraki Organization ID.
<b>Meraki Network ID</b>	String	L_111111111	This is the unique Network ID, which typically looks like the format in the example.
<b>Allow Not Connected as a Valid Status</b>	String	True	This is a True/False field. Entering 'True' will be considered "NotConnected" as a normal state. Entering 'False' will cause a Fail status.

### Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Number of Devices Found with Uplinks in the Organization</b>	Number	This is the total number of Meraki devices with uplinks.
<b>Total Number of Uplinks Found</b>	Number	This is the total number of uplinks found (some Meraki devices can have more than one).
<b>Total Number of Uplinks Found with Errors</b>	Number	This is the total number of uplinks with any errors.
<b>Details of Devices with Uplink Issues</b>	String	This is the details of the uplinks with reported errors. This will show the network ID, device serial, the date/time it last checked in, the network name, its status, and the internal/public IP addresses.
<b>Details of Devices with No Uplink Issues</b>	String	This will show the network ID, device serial, the date/time it last checked in, the network name, status, and the internal/public IP addresses.
<b>Api Errors</b>	String	This returns any errors provided by the API calls.

## MERAKI – NETWORK DEVICE CONNECTIVITY STATUS

This service returns the number of Meraki devices on a specific network, along with details of any offline devices.

### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1a23 a5a135a135a1833 a189a3518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Organization ID</b>	String	12345	This is the unique Meraki Organization ID.
<b>Meraki Network ID</b>	String	L_111111111	This is the unique Network ID, which typically looks like the format in the example.

### Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Total Devices Found in Network</b>	Number	This returns the total number of Meraki devices found on the specified network.
<b>Total Online Devices</b>	Number	This returns the total of responding/online devices.
<b>Total Offline Devices</b>	Number	This returns the total number of offline/non-responsive devices.
<b>Offline Devices Found</b>	String	This returns the details of the offline devices, including device name (if available), serial, and the date/time when it was last online.
<b>Online Devices Found</b>	String	This returns the details of the online devices, including device name (if available), serial, and the date/time when it was last online.
<b>Api Errors</b>	String	This returns any errors provided by the API calls.

## MERAKI – ORGANIZATION APPLIANCE UPLINK STATUS

This service looks at a whole organization and returns information about all the devices with uplink and checks if they are working properly (WAN/Cellular WAN).

Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1a23 a5a135a135a1833 a189a3518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Organization ID</b>	String	12345	This is the unique Meraki Organization ID.
<b>Allow Not Connected as a Valid Status</b>	String	True	This is a True/False field. Entering 'True' will be considered "Not Connected" as a normal state. Entering 'False' will cause a Fail status

Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Number of Devices Found with Uplinks in the Organization</b>	Number	This is the total number of Meraki devices with uplinks.
<b>Total Number of Uplinks Found</b>	Number	This is the total number of uplinks found (some Meraki devices can have more than one).
<b>Total Number of Uplinks Found with Errors</b>	Number	This is the total number uplinks with any errors.
<b>Details of Devices with Uplink Issues</b>	String	This is the details of the uplinks with reported errors. This will show the network ID, device serial, the date/time it last checked in, the network name, the status, and the internal/public IP addresses.
<b>ApiErrors</b>	String	This returns any errors provided by the API calls.

## MERAKI – ORGANIZATION DEVICE CONNECTIVITY STATUS

This service returns the number of Meraki devices on a specific organization, along with details of any offline devices.

### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1a23 a5a135a135a1833 a189a3518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Organization ID</b>	String	12345	This is the unique Meraki Organization ID.

### Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Total Devices Found in Network</b>	Number	This returns the total number of Meraki devices found on the specified network.
<b>Total Online Devices</b>	Number	This returns the total of responding/online devices.
<b>Total Offline Devices</b>	Number	This returns the total number of offline/non-responsive devices.
<b>Offline Devices Found</b>	String	This returns the details of the offline devices, including device name (if available), serial, and the date/time when it was last online.
<b>ApiErrors</b>	String	This returns any errors provided by the API calls.

## MERAKI – ORGANIZATION LICENSE DETAILS

This service returns details of the licenses for a specific organization.

### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1a23 a5a135a135a1833 a189a3518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Organization ID</b>	String	12345	This is the unique Meraki Organization ID.

### Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Licensing Status</b>	String	This returns the status ID of the license. Anything other than "OK" will return an error.
<b>License ExpirationDate</b>	String	This returns the expiry date of the license as shown on the organization.
<b>Days Left on License</b>	Number	This is the number of days left on the license based on the date.
<b>Licensed Devices Details</b>	String	This is the details of how many devices of each type are licensed in that organization.
<b>ApiErrors</b>	String	This returns any errors provided by the API calls.

## MERAKI – ORGANIZATION SECURITY EVENTS

This service returns events of varying severity for an organization, for a desired timeframe.

### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1a23 a5a135a135a1833 a189a3518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Organization ID</b>	String	12345	This is the unique Meraki Organization ID.
<b>Timespan (Minutes)</b>	Number	60	This is how far back it will look for events. It can be set up to 1 week.
<b>Minimum Priority</b>	Number	4	This is the priority of events to be looked for. It will look for the selected priority and any higher priority. For example, selecting 3 will look for events of priority 1,2,3. Selecting 2 will do 1,2 only, and so on.

### Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Number of Events Found</b>	Number	This will return a count of how many events were found based on the entered criteria.
<b>Most Recent Event Found</b>	String	This will be the most recent event and its details.
<b>Most Recent Event – Priority Level</b>	Number	This will be the priority of the most recent event (1,2,3,4).
<b>Most Recent 5 Events Found</b>	String	This will be the details of the most recent 5 events.
<b>ApiErrors</b>	String	This returns any errors provided by the API calls.

## MERAKI – SWITCH PORT STATUS

This service returns the status of a specific port on a Meraki Switch device, including connectivity, speed, traffic, etc.

### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1 a23a5a135a13 5a1833a189a3 518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Device Serial</b>	String	AAAA-AAAA- AAAA	This is the unique serial of the Cisco Meraki Switch.
<b>How Many Hours to Look Back</b>	Number	24	This is how far back it will look for events. It can be set up to 1 week.
<b>Port Number</b>	Number	2	This is the port number of the device.

### Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Is Port Enabled</b>	String	This returns true/false based on whether the port is enabled for use.
<b>Port Number</b>	Number	This returns the selected port number.
<b>Port Status</b>	String	This returns the status of the port, whether it is in error, connected, etc.
<b>Port Errors</b>	String	This returns any errors as reported by the switch.
<b>Port Warnings</b>	String	This returns any warnings as reported by the switch.
<b>Detected Port Speeds</b>	String	This returns the port speed (Gbps, 100meg, etc.).
<b>Duplex Enabled</b>	String	This returns whether full duplex is enabled.
<b>Detected Client Count on Port</b>	Number	This is the count of devices found on the selected port.
<b>Bandwidth Sent in kbps</b>	Number	This is the sent bandwidth in Kbps at the time of the service polling.
<b>Bandwidth Received in Kbps</b>	Number	This is the received bandwidth in Kbps at the time of the service polling.
<b>Bandwidth Combined in Kbps</b>	Number	This is the total bandwidth in Kbps at the time of the service polling.
<b>Total Sent Traffic for Selected Time Period in MB</b>	Number	This is the total sent traffic for that time in megabytes.

Continued:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Total Received Traffic for Selected Time Period in MB</b>	Number	This is the total received traffic for that time in megabytes.
<b>Total Combined Traffic for Selected Time Period in MB</b>	Number	This is the total combined traffic for that time in megabytes.
<b>API Errors</b>	String	This returns any errors provided by the API calls.

### MERAKI – SWITCH STATUS (BANDWIDTH AND CONNECTIVITY)

This service returns the status of all ports of a Meraki Switch, and combining band- width/traffic data to show overall usage.

#### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1 a23a5a135a13 5a1833a189a3 518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Device Serial</b>	String	AAAA-AAAA- AAAA	This is the unique serial of the Cisco Meraki Switch.
<b>How Many Hours to Look Back</b>	Number	24	This is how far back it will look for events. It can be set up to 1 week.

#### Output:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Total Ports on the Switch</b>	Number	This is the total number of ports detected on the switch.
<b>Total Enabled Ports</b>	Number	This is the total number of enabled ports.
<b>Total Disabled Ports</b>	Number	This is the number of disabled ports (total).
<b>Total Ports Connected and Active</b>	Number	This is the total number of ports actively connected to a device and working.
<b>Total Ports Disconnected</b>	Number	This is the total number of ports disconnected.
<b>Bandwidth Sent in Kbps</b>	Number	This is the sent bandwidth in Kbps at the time of the service polling.

Continued:

FIELD NAME	TYPE	NOTES/DETAILS
<b>Bandwidth Received in Kbps</b>	Number	This is the received bandwidth in Kbps at the time of the service polling.
<b>Bandwidth Combined in Kbps</b>	Number	This is the total bandwidth in Kbps at the time of the service polling.
<b>Total Sent Traffic for Selected Time Period in MB</b>	Number	This is the total sent traffic for that time period in megabytes.
<b>Total Received Traffic for Selected Time Period in MB</b>	Number	This is the total received traffic for that time in megabytes.
<b>Total Combined Traffic for Selected Time Period in MB</b>	Number	This is the total combined traffic for that time in megabytes.
<b>Port Details and Status</b>	String	This returns every port along with whether they are enabled, connected, and its total traffic as of the time of polling in Kbps.
<b>API Errors</b>	String	This returns any errors provided by the API calls.

## MERAKI – WAP WI-FI NETWORK DETAILS

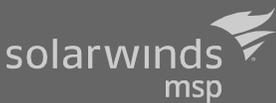
This returns the details of all the Wi-Fi networks on a specific WAP.

### Input Parameters:

FIELD NAME	TYPE	EXAMPLE	NOTES/DETAILS
<b>Meraki API Key</b>	Password	aa123a11a1a1a23 a5a135a135a1833 a189a3518a	This is the API key found in the Cisco Meraki Portal. In the Meraki portal, use a user account with the proper permissions and generate a unique API key to be used here. This should be linked to a custom organization property.
<b>Meraki Device Serial</b>	String	AAAA-AAAA-AAAA	This is the unique serial of the Cisco Meraki Switch.

**Output:**

FIELD NAME	TYPE	NOTES/DETAILS
<b>Number of Wi-Fi Networks</b>	Number	Total number of Wi-Fi Networks registered on that WAP.
<b>Enabled Wi-Fi Networks</b>	Number	Total number of Wi-Fi networks enabled for use.
<b>Disabled Wi-Fi Networks</b>	Number	Total number of Wi-Fi networks configured but disabled.
<b>Visible Wi-Fi Networks</b>	Number	Total number of Wi-Fi networks visible to any guest.
<b>Not Visible Wi-Fi Networks</b>	Number	Total number of Wi-Fi networks not visible.
<b>Broadcasting Wi-Fi Networks</b>	Number	Total number of Wi-Fi networks broadcasting their info.
<b>Not Broadcasting Wi-Fi Networks</b>	Number	Total number of Wi-Fi networks not broadcasting info.
<b>Wi-Fi Network Details</b>	String	This is the detail of all Wi-Fi networks. This returns the network name, band, channel, power, visibility and broadcasting status.
<b>API Errors</b>	String	This returns any errors provided by the API calls.



Learn more today at [solarwindsmsp.com](http://solarwindsmsp.com)

*SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT management software. Our products give organizations worldwide—regardless of type, size, or complexity—the power to monitor and manage their IT services, infrastructures, and applications; whether on-premises, in the cloud, or via hybrid models. We continuously engage with technology professionals—IT service and operations professionals, DevOps professionals, and managed services providers (MSPs)—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures and applications. Targeted for MSPs, the SolarWinds MSP product portfolio delivers broad, scalable IT service management solutions that integrate layered security, collective intelligence, and smart automation. Our products are designed to enable MSPs to provide highly effective outsourced IT services for their SMB end customers and more efficiently manage their own businesses.*

© 2020 SolarWinds MSP Canada ULC and SolarWinds MSP UK Ltd. All rights reserved.

The SolarWinds and SolarWinds MSP trademarks are the exclusive property of SolarWinds MSP Canada ULC, SolarWinds MSP UK Ltd. or its affiliates. All other trademarks mentioned herein are the trademarks of their respective companies.

This document is provided for informational purposes only. SolarWinds makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information.