Monitoring Cisco Meraki

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Meraki MX is an enterprise security & SD-WAN appliance designed for distributed deployments that require remote administration. It is ideal for network administrators who demand both ease of deployment and a state-of-the-art feature set.

Meraki MX appliances are equipped with SD-WAN capabilities that enable administrators to maximize network resiliency and bandwidth efficiency.

In large environments where Cisco Meraki is deployed, glitches in its performance can cause the untimely collapse the entire environment, which in turn might result in significant delays in the delivery of the dependent end-user services and prolonged service outages. To avoid such adversities, eG Enterprise helps network administrators to continuously monitor the Cisco Meraki.

Chapter 2: How does eG Enterprise Monitor Cisco Meraki?

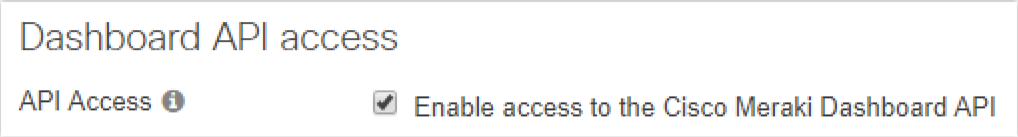
eG Enterprise employs an *agentless* approach to monitor the target Cisco Meraki. This approach requires that the eG agent be deployed on a remote Windows host in the target environment. To collect the metrics of interest from the target Cisco Meraki, this agent uses the *Dashboard API*.

The pre-requisites that need to be fulfilled to monitor the target Cisco Meraki are discussed in detail in the forthcoming section.

2.1 Pre-requisites for Monitoring Cisco Meraki

In high security environments where the eG agent should connect to the target Cisco Meraki and collect the required metrics, administrators of those environments may not wish to provide the credentials of the user possessing administrator privileges. Therefore, to monitor Cisco Meraki, eG Enterprise requires the administrator of the Cisco Meraki to create a new user with *read-only* privilege and determine the API key for that user. This API key should be provided while configuring the tests that will be executed to collect the required metrics. To determine the API Key, do the following:

1. Login to the Cisco Meraki Dashboard API as a user with *administrator* privileges.
2. Then, for the eG agent to collect the required metrics, the Dashboard API should be enabled. For this, navigate through the menu sequence: *Organization* -> *Settings* -> *Dashboard API Access*. In the *Dashboard API access* section as shown in Figure 2.1, select the check box before the **Enable access to the Cisco Meraki Dashboard API**.

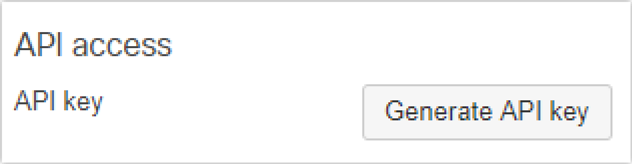


Dashboard API access

API Access ☑ Enable access to the Cisco Meraki Dashboard API

Figure 2.1: Enabling Dashboard API access

3. Once the API access is enabled, navigate to the **My Profile** page. Figure 2.2 will then appear. Here, click the **Generate API key** button available against the **API key** option in the **API access** section.



API access

API key

Figure 2.2: Generating the API Key

4. The API key is then generated and displayed.
5. This API key should be specified in the **API Key** text box while configuring the tests.

Once the aforesaid pre-requisites are fulfilled, add the Cisco Meraki component for monitoring using eG administrative interface. The steps for achieving this have been discussed in the **How to Monitor Cisco Meraki Using eG Enterprise?** chapter.

Chapter 3: How to Monitor Cisco Meraki Using eG Enterprise?

The broad steps for monitoring Cisco Meraki using eG Enterprise are as follows:

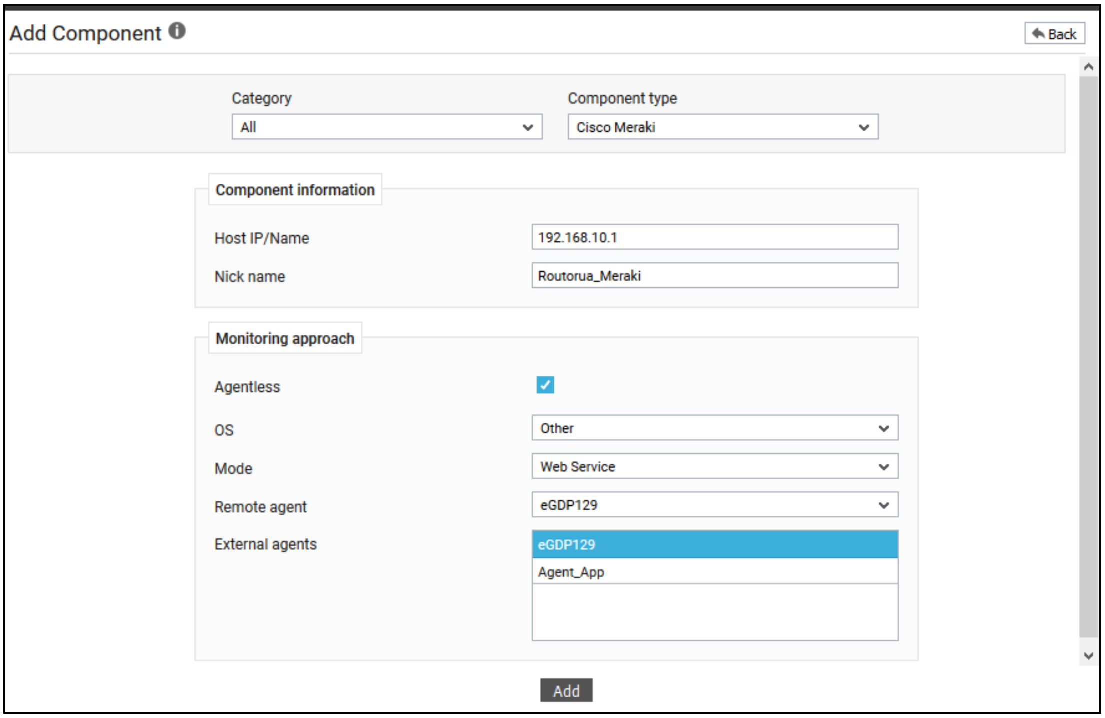
- Managing the Cisco Meraki
- Configuring the tests

These steps have been discussed in following sections.

3.1 Managing the Cisco Meraki

The eG Enterprise cannot automatically discover Cisco Meraki. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage Cisco Meraki, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *Cisco Meraki* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 3.1.



Add Component

Category	All
Component type	Cisco Meraki

Component information

Host IP/Name	192.168.10.1
Nick name	Routorua_Meraki

Monitoring approach

Agentless	☑
OS	Other
Mode	Web Service
Remote agent	eGDP129
External agents	eGDP129 Agent_App

Figure 3.1: Adding the Cisco Meraki

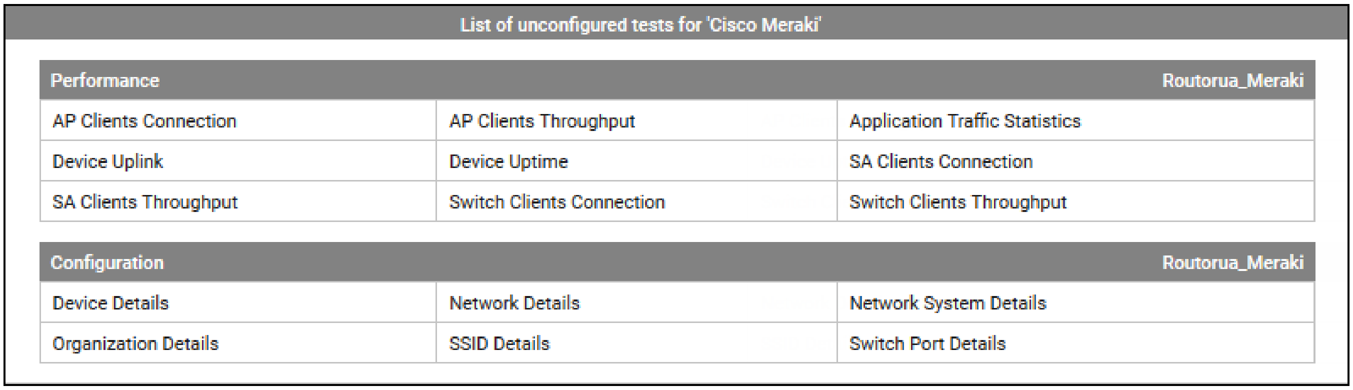
4. Specify the **Host IP** and the **Nick name** for the Cisco Meraki in Figure 3.1. By default, the Cisco Meraki component is monitored in an agentless manner. Therefore, the **Agentless** flag will be checked by default.

5. Next, choose **Other** as the **OS** and **Web Service** as the **Mode** for monitoring the Cisco Meraki component.

6. Finally, click the **Add** button to register the changes.

3.2 Configuring the tests

1. When you attempt to sign out of eG administrative interface, a list of unconfigured tests will appear as shown in Figure 3.2. This list reveals the unconfigured tests that require manual configuration.



List of unconfigured tests for 'Cisco Meraki'

Performance		Routorua_Meraki
AP Clients Connection	AP Clients Throughput	Application Traffic Statistics
Device Uplink	Device Uptime	SA Clients Connection
SA Clients Throughput	Switch Clients Connection	Switch Clients Throughput

Configuration		Routorua_Meraki
Device Details	Network Details	Network System Details
Organization Details	SSID Details	Switch Port Details

Figure 3.2: List of tests that need to be configured for the Cisco Meraki

2. To configure the tests, click on the test names in the list of unconfigured tests. To know more on how to configure the tests, refer to **Monitoring the Cisco Meraki** chapter.

3. Once all the tests are configured, signout of the eG administrative interface.

Chapter 4: Monitoring the Cisco Meraki

eG Enterprise provides a specialized monitoring model (see Figure 4.1) to monitor the target Cisco Meraki inside-out and sheds light on data transmitted /received through the switches, security appliances connected to it.

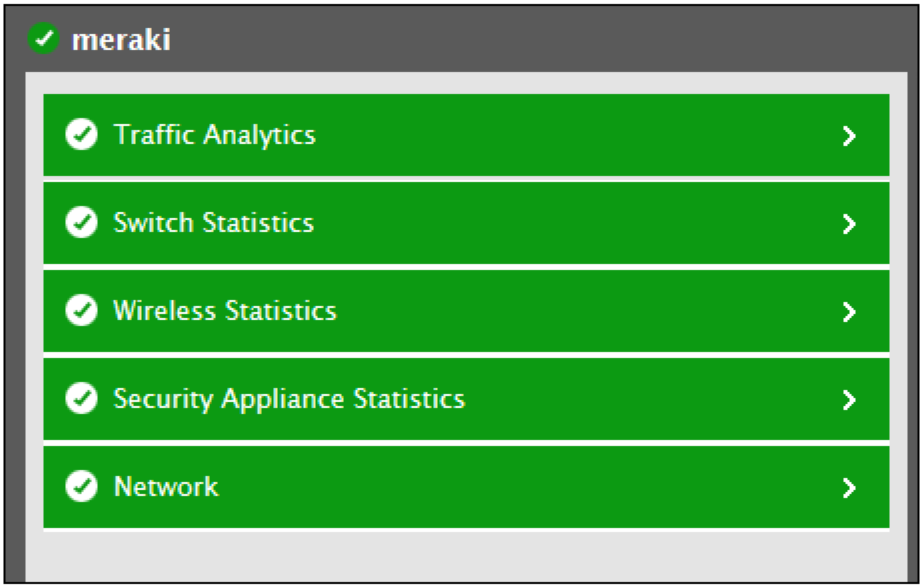


Figure 4.1: The layer model of the Cisco Meraki

Every layer of the layer model is mapped to a variety of tests that monitor critical performance parameters of the components associated with the target Cisco Meraki.

To pull out useful metrics from the Cisco Meraki, the eG agent needs to be deployed on a remote Windows host in the environment and connect to the Dashboard API of the target Cisco Meraki so that tests can be executed periodically. The metrics reported by these tests enable administrators to answer the following questions:

- How many clients are connected to the access point on the target Cisco Meraki?
- What amount of data was sent and received by each client connected to the access point on the target Cisco Meraki?
- How many clients are connected to the security appliance on the target Cisco Meraki?
- What amount of data was sent and received by each client connected to the security appliance?
- What is the status of the uplink interface?

- Was a static IP used for connecting to the uplink interface?
- How many clients are connected to the switch?
- What amount of data was sent and received by each client connected to the switch?

The sections that follow discusses each of the layers of Figure 4.1 in great detail.

4.1 The Security Appliance Statistics Layer

The tests associated with the **Security Appliance Statistics** layer and the measures reported by them provide in-depth insights into the data sent and received by each client associated with each security appliance and the total number of clients connected to each security appliance.

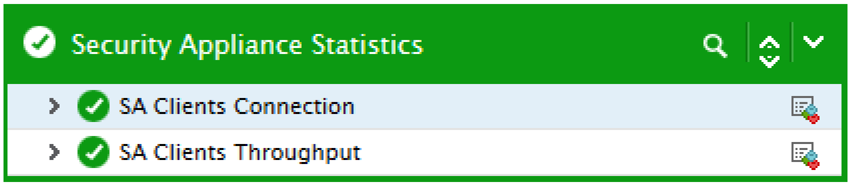


Figure 4.2: The tests mapped to the Security Appliance Statistics layer

4.1.1 SA Clients Connection Test

This test monitors the security appliances connected to the target Cisco Meraki and for each security appliance, reports the total number of clients connected. Using this test, administrators can figure out the security appliance that is utilized widely by the maximum number of clients.

Target of the test : A Cisco Meraki

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Network:Security Appliance* combination on the target Cisco Meraki being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Meraki to be monitored.
Port	The port at which the specified Host listens. By default, this will be *NULL*.
API Key	The eG agent collects the required metrics from the target Cisco Meraki by executing

Parameter	Description
	API commands using Dashboard API and pulls out critical metrics. In order to collect metrics, the eG agent should be provided with a valid API key. To know how to generate the API key, refer to Section **2.1**. Specify the generated API key in this text box.
SSL	By default, the target Cisco Meraki is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total clients	Indicates the total number of clients currently connected to this security appliance.	Number	The detailed diagnosis of this measure lists the name of the client, ID, MAC address and IP address.

4.1.2 SA Clients Throughput Test

For each client accessing the security appliance connected to the target Cisco Meraki, this test reports the amount of data sent and received. Using this test, administrators can identify the client sending/receiving the maximum amount of data.

Target of the test : A Cisco Meraki

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Network:Security Appliance:Client* connected to the target Cisco Meraki being monitored.

Configurable parameters for the test

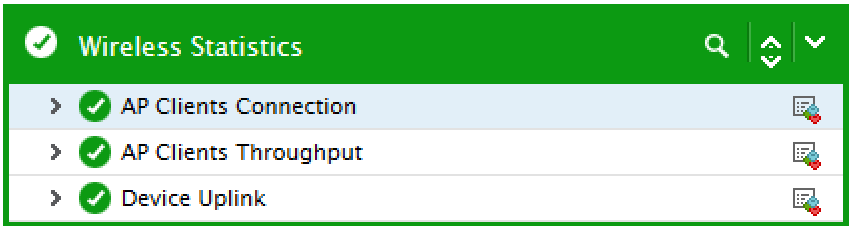
Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Meraki to be monitored.
Port	The port at which the specified Host listens. By default, this will be *NULL*.
API Key	The eG agent collects the required metrics from the target Cisco Meraki by executing API commands using Dashboard API and pulls out critical metrics. In order to collect metrics, the eG agent should be provided with a valid API key. To know how to generate the API key, refer to Section **2.1**. Specify the generated API key in this text box.
SSL	By default, the target Cisco Meraki is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Sent data	Indicates the rate at which data was sent from this client during the last measurement period.	KB/sec	Compare the value of this measure across the clients to figure out the client through which maximum amount of data was sent.
Received data	Indicates the rate at which data was received by this client during the last measurement period.	KB/sec	Compare the value of this measure across the clients to figure out the client that received the maximum amount of data.

4.2 The Wireless Statistics Layer

The tests associated with the **Wireless Statistics** layer and the measures reported by them provide in-depth insights into the data sent and received by each client associated with each access point and the total number of clients connected to each access point. In addition, the status of the uplink interface is also monitored round the clock and reported.


Wireless Statistics

- AP Clients Connection
- AP Clients Throughput
- Device Uplink

Figure 4.3: The tests mapped to the Wireless Statistics layer

4.2.1 AP Clients Connection Test

This test monitors the access points connected to the target Cisco Meraki and for each access point, reports the total number of clients connected. Using this test, administrators can figure out the access point that is busy catering to the maximum number of clients.

Target of the test : A Cisco Meraki

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Network:Access Point* combination on the target Cisco Meraki being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Meraki to be monitored.
Port	The port at which the specified Host listens. By default, this will be *NULL*.
API Key	The eG agent collects the required metrics from the target Cisco Meraki by executing API commands using Dashboard API and pulls out critical metrics. In order to collect metrics, the eG agent should be provided with a valid API key. To know how to generate the API key, refer to Section **2.1** . Specify the generated API key in this text box.
SSL	By default, the target Cisco Meraki is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server,

Parameter	Description
	choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total clients	Indicates the total number of clients currently connected to this access point.	Number	The detailed diagnosis of this measure lists the name of the client, ID, MAC address and IP address.

4.2.2 AP Clients Throughput Test

For each client accessing the access point of the target Cisco Meraki, this test reports the amount of data sent and received. Using this test, administrators can identify the client that is sending/receiving the maximum amount of data.

Target of the test : A Cisco Meraki

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Network:Access Point:Client* connected to the target Cisco Meraki being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Meraki to be monitored.
Port	The port at which the specified Host listens. By default, this will be *NULL*.

Parameter	Description
API Key	The eG agent collects the required metrics from the target Cisco Meraki by executing API commands using Dashboard API and pulls out critical metrics. In order to collect metrics, the eG agent should be provided with a valid API key. To know how to generate the API key, refer to Section **2.1** . Specify the generated API key in this text box.
SSL	By default, the target Cisco Meraki is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Sent data	Indicates the rate at which data was sent during the last measurement period to this client.	KB/sec	Compare the value of this measure across clients to identify the client that is sending the maximum amount of data.
Received data	Indicates the rate at which data was received by this client during the last measurement period.	KB/sec	Compare the value of this measure to identify the client that is receiving the maximum amount of data.

4.2.3 Device Uplink Test

This test auto-discovers the uplink interfaces of the target Cisco Meraki and for each uplink interface, reports the current status. This test further reports whether static IP was used for the uplink interface or not.

Target of the test : A Cisco Meraki

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Network:Access Point:Uplink interface* combination on the target Cisco Meraki being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Meraki to be monitored.
Port	The port at which the specified Host listens. By default, this will be *NULL*.
API Key	The eG agent collects the required metrics from the target Cisco Meraki by executing API commands using Dashboard API and pulls out critical metrics. In order to collect metrics, the eG agent should be provided with a valid API key. To know how to generate the API key, refer to Section **2.1** . Specify the generated API key in this text box.
SSL	By default, the target Cisco Meraki is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

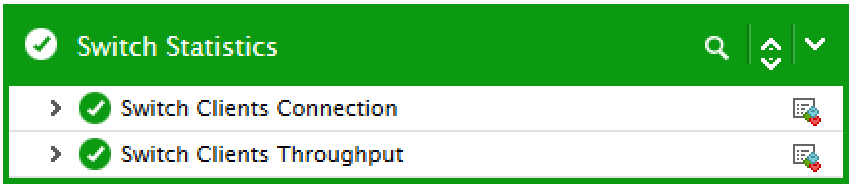
Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this uplink interface.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Down</td><td>0</td></tr>
<tr><td>Active</td><td>1</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><b>Note:</b>
By default, this measure reports the <b>Measure Values</b> listed in the table above to indicate the current status of this uplink interface. The graph of this measure however, is represented using the numeric equivalents only i.e., 0 or 1.</td></tr>
<tr><td>Is static IP used?</td><td>Indicates whether/not static IP was used for this uplink interface.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>No</td><td>0</td></tr><tr><td>Yes</td><td>1</td></tr></table><b>Note:</b>
By default, this measure reports the <b>Measure Values</b> listed in the table above to indicate whether/not static IP was used for this uplink interface. The graph of this measure however, is represented using the numeric equivalents only i.e., 0 or 1.</td></tr>
</table>

4.3 The Switch Statistics Layer

The tests associated with the **Switch Statistics** layer and the measures reported by them provide in-depth insights into the data sent and received by each client associated with each switch and the total number of clients connected to each switch.



Switch Statistics

Switch Clients Connection

Switch Clients Throughput

Figure 4.4: The tests mapped to the Switch Statistics layer

4.3.1 Switch Clients Connection Test

This test monitors the switches connected to the target Cisco Meraki and for each switch, reports the total number of clients connected. Using this test, administrators can figure out the switch that is busy catering to the maximum number of clients.

Target of the test : A Cisco Meraki

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Network:Switch* combination on the target Cisco Meraki being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Meraki to be monitored.
Port	The port at which the specified Host listens. By default, this will be *NULL*.
API Key	The eG agent collects the required metrics from the target Cisco Meraki by executing API commands using Dashboard API and pulls out critical metrics. In order to collect metrics, the eG agent should be provided with a valid API key. To know how to generate the API key, refer to Section **2.1**. Specify the generated API key in this text box.
SSL	By default, the target Cisco Meraki is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total clients	Indicates the total number of clients currently connected to this switch.	Number	The detailed diagnosis of this measure lists the name of the client, ID, MAC address, IP address and Switch port.

4.3.2 Switch Clients Throughput Test

For each client accessing the switch connected to the target Cisco Meraki, this test reports the amount of data sent and received. Using this test, administrators can identify the client that is sending/receiving the maximum amount of data.

Target of the test : A Cisco Meraki

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Network:Switch:Client* connected to the target Cisco Meraki being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Meraki to be monitored.
Port	The port at which the specified Host listens. By default, this will be *NULL*.
API Key	The eG agent collects the required metrics from the target Cisco Meraki by executing API commands using Dashboard API and pulls out critical metrics. In order to collect metrics, the eG agent should be provided with a valid API key. To know how to generate the API key, refer to Section **2.1**. Specify the generated API key in this text box.
SSL	By default, the target Cisco Meraki is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Sent data	Indicates the rate at which data was sent during the last measurement period to this client.	KB/sec	Compare the value of this measure across clients to identify the client that is sending the maximum amount of data.
Received data	Indicates the rate at which data was received by this client during the last measurement period.	KB/sec	Compare the value of this measure to identify the client that is receiving the maximum amount of data.

4.4 The Traffic Analytics Layer

Using the test associated with this layer, administrators can figure out the data sent and received by each application and the number of destinations and clients connected to each application can be monitored with ease. This way, administrators can easily identify the application and the destination that is constantly in use.

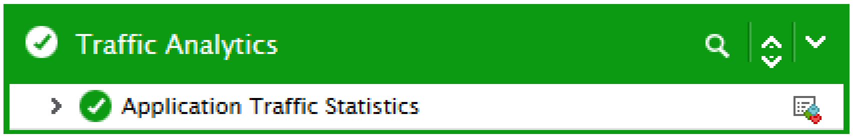


Figure 4.5: The tests mapped to the Traffic Analytics layer

4.4.1 Application Traffic Statistics Test

For each application over the network connected to the target Cisco Meraki, this test reports the amount of data sent and received. In addition, this test reveals the number of clients accessing each application and the number of destinations used by the clients . Using this test, administrators can figure out the destination that is mostly utilized by the application.

Target of the test : A Cisco Meraki

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Network:Application* connected to the target Cisco Meraki being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Meraki to be monitored.
Port	The port at which the specified Host listens. By default, this will be *NULL*.
API Key	The eG agent collects the required metrics from the target Cisco Meraki by executing API commands using Dashboard API and pulls out critical metrics. In order to collect metrics, the eG agent should be provided with a valid API key. To know how to generate the API key, refer to Section **2.1** . Specify the generated API key in this text box.
SSL	By default, the target Cisco Meraki is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default.
Report by Destination	By default, this flag is set to **No**. This implies that this test reports the statistics of each application, by default. However if administrators want to monitor the individual statistics of each destination corresponding to the application on the network of the target Cisco Meraki, then, this flag can be set to **Yes**.
Report by Total	This flag appears only when the Report by Destination flag is set to Yes. By default, this flag is set to **Yes**. If set to **Yes**, then the test will report measures for an additional Total descriptor summarizing the statistics of all the applications over the network of the target Cisco Meraki.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Sent data	Indicates the rate at which data was sent from this application during the last measurement period.	MB	Compare the value of this measure across the applications to figure out the application through which maximum amount of data was sent.
Received data	Indicates the rate at which data was received by this application during the last measurement period.	MB	Compare the value of this measure across the applications to figure out the application that received the maximum amount of data.
Total client(s)	Indicates the total number of clients currently accessing this application.	Number	Comparing the value of this measure across the applications would reveal the application that is being accessed the most/least by the clients.
Total destinations	Indicates the total number of destinations used by the client to access this application.	Number	**This measure will report metrics only when the Report by Destination flag is set to Yes.**

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.