Monitoring Alcatel Switch

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Alcatel OmniSwitch 6600 family switches are advanced 10/100 based stackable layer 3 workgroup switches that provide wire rate L2+ switching, L3 routing and advanced services with high availability for IP communications and mission-critical environments.

If this switch, which assures service operators of continuous network connectivity and secure transaction of business, starts malfunctioning suddenly, the connection to mission-critical services will be lost, thereby causing irreparable damage to reputation and revenue. It is therefore imperative that the operations of the Alcatel switch are monitored 24 x 7.

The eG Enterprise provides exclusive *Alcatel switch* monitoring model for monitoring the availability, data transmission and bandwidth usage of the switches.

Chapter 2: How to Monitor Alcatel Switch using eG Enterprise?

eG Enterprise monitors the Alcatel Switch using an eG external agent that is deployed on a remote host. This eG agent polls the SNMP MIB of the switch to gather the statistics related to the Alcatel Switch at configured intervals. Before attempting to monitor the Alcatel switch, ensure that the switch is SNMP-enabled.

2.1 Managing the Alcatel Switch

The eG Enterprise suite cannot automatically discover a Alcatel switch. This implies that you need to manually add the component for monitoring. To manage a Alcatel Switch component, 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 **COMPONENTS** page that appears next, select *Alcatel Switch* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

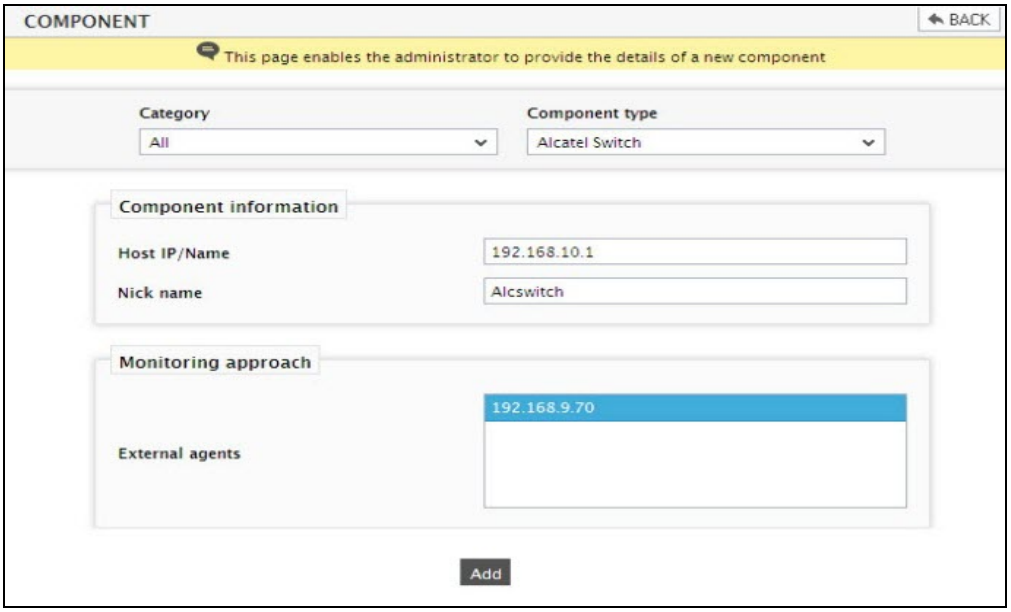

Figure 2.1: Adding an Alcatel Switch

4. Specify the **Host IP/Name** and **Nick name o**f the Alcatel Switch component to be monitored as shown in Figure 2.1. Then, click **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).

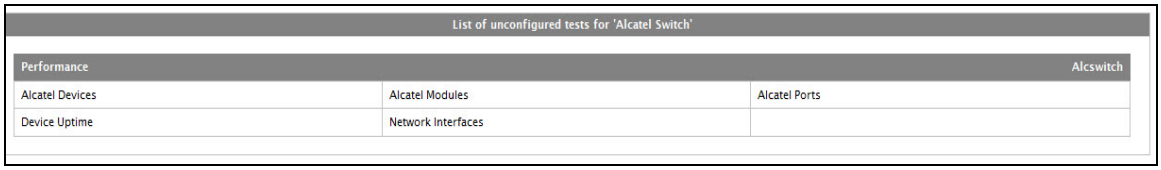

Figure 2.2: List of Unconfigured tests for the Alcatel Switch

6. Click on any test in the list of unconfigured tests. For instance, click on the **Alcatel Devices** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.

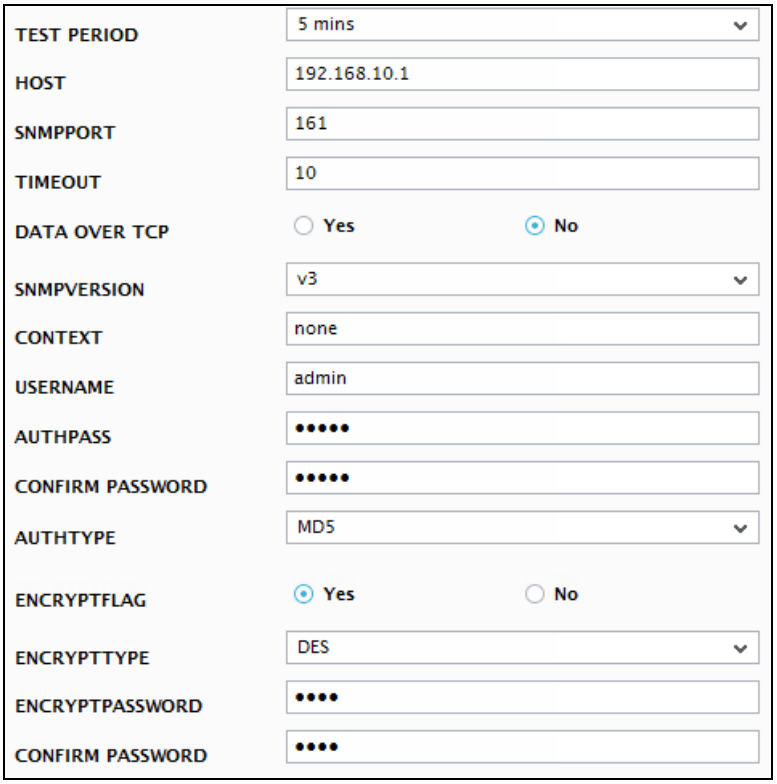

Figure 2.3: Configuring the Alcatel Devices test

To know how to configure the tests, refer to the **Monitoring the Alcatel Switch**.

7. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the Alcatel Switch

eG Enterprise provides a specialized *Alcatel Switch* model to keep track of the internal health and external availability of the Alcatel switch.

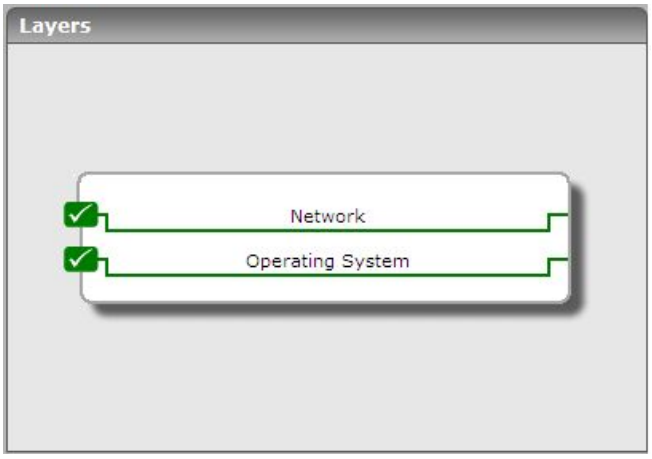

Figure 3.1: Layer model of the Alcatel Switch

This model connects to the SNMP MIB of the switch to collect a wide variety of metrics revealing the following:

- How is the I/O activity on the switch devices? Is it unusually high on any device?
- Do the switch devices use CPU and memory optimally, or is any device using these resources excessively?
- Have the chassis and the chassis management module (CMM) registered unusually high temperatures?
- Are the switch modules using the I/O, CPU, and memory resources available to it effectively? Is any module consuming resources excessively?
- Is any port on the switch unavailable currently?
- Is any port utilizing the CPU, I/O, or memory resources excessively?

The sections to come discuss the layers in the Figure 3.1 in great detail.

3.1 The Operating System Layer

Using the tests associated with this layer, administrators can assess how effectively the switch devices and modules utilize the CPU, memory, and I/O resources available to the switch.

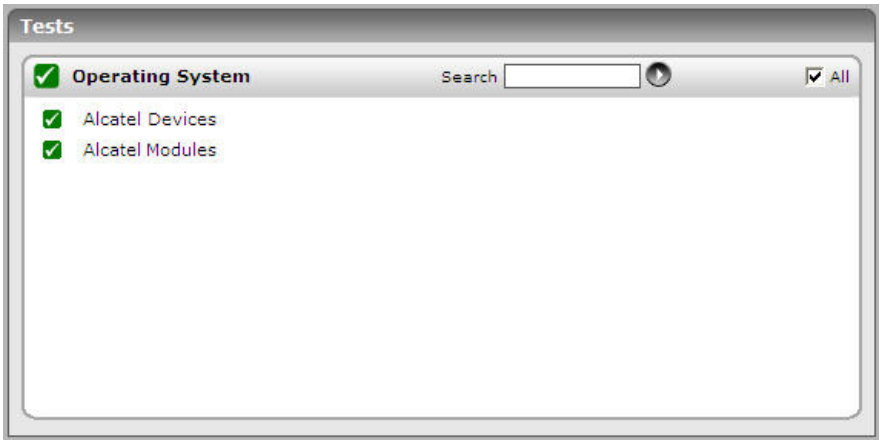

Figure 3.2: The tests associated with the Operating System layer

3.1.1 Alcatel Devices Test

This test reports critical statistics pertaining to the switch device.

Target of the test : An Alcatel Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for every switch monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB;
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen

Parameters	Description
	is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:

Parameters	Description
	• **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Device input utilization	Indicates the device-level input utlization.	Percent	
Device I/O utilization	Indicates the percentage of I/O used by the device.	Percent	A high value of this measure indicates high I/O activity on the device.
Device CPU utilization	Indicates the percentage of CPU used up by the device.	Percent	Ideally, this value should be low. A high value is indicative of excessive CPU usage by the device.
Device memory utilization	Indicates the percentage of memory utilized by the device.	Percent	Ideally, this value should be low. A high value is indicative of excessive memory usage by the device.
Chassis temperature	Indicates the current chassis temperature.	Deg	A consistent increase in the value of this measure could be a cause for concern.
CMM CPU temperature	Indicates the current temperature of the chassis management module (CMM) CPU.	Deg	A consistent increase in the value of this measure could be a cause for concern.

3.1.2 Alcatel Modules Test

This test reports the resource usage of each of the modules of the Alcatel switch.

Target of the test : An Alcatel Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for every module on the switch monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB;
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the

Parameters	Description
	Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Module input utilization	Indicates the input utilization by this module.	Percent	
Module I/O utilization	Indicates the percentage of I/O used by this module.	Percent	A high value of this measure indicates high I/O activity on the module. Comparing the value of this measure across modules will enable administrators accurately identify that module on which I/O usage is the maximum.
Module CPU utilization	Indicates the percentage of CPU used up by this module.	Percent	Ideally, this value should be low. A high value is indicative of excessive CPU usage by the module. Comparing the value of this measure across modules will enable administrators accurately identify that module on which CPU usage is unusually high.
Module memory utilization	Indicates the percentage of memory utilized by this module.	Percent	Ideally, this value should be low. A high value is indicative of excessive memory usage by the module. Comparing the value of this measure across modules will enable administrators accurately identify the module(s) which is consuming memory excessively.

3.2 The Network Layer

The tests mapped to this layer enable administrators to determine the following:

- Whether the switch is available or not
- The current status of the ports on the switch
- The resource usage of the switch ports
- The network traffic to and from the switch

- The bandwidth usage of the network interfaces supported by the switch
- The uptime of the switch

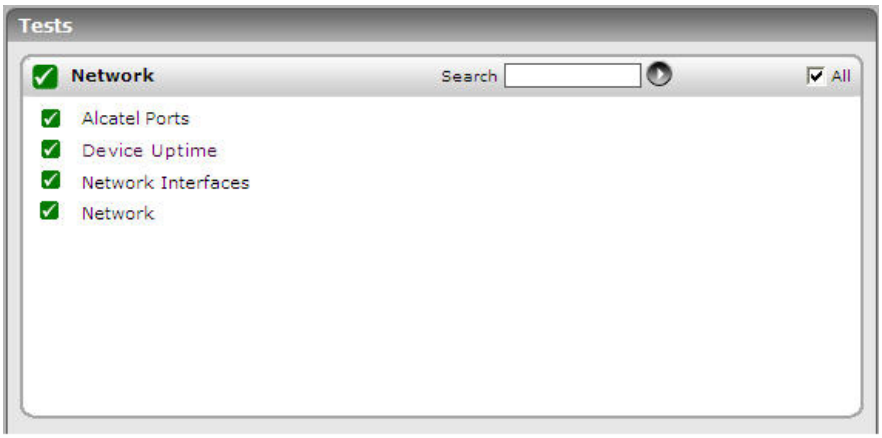

Figure 3.3: The tests associated with the Network layer

The **Network Interfaces** test, the **Network** test, and **Device Uptime** test are discussed in the *Monitoring Cisco Routers*, the section to come will discuss the **Alcatel Ports** test only.

3.2.1 Alcatel Ports Test

This test reports the status of the ports on the Alcatel switch and their resource usage.

Target of the test : An Alcatel Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for every port on the switch monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB;
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This

Parameters	Description
	parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following

Parameters	Description
	encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Is port up?	Indicates whether this port is up or down currently.		The values that this measure can report and their corresponing numeric values have been described in the table below Measure Value / Numeric Value Up – 100 Down – 0 **Note:** By default, this measure reports one of the **Measure Value**s listed in the table above to indicate the current state of a port. The graph of this measure however, represents the same using

Measurement	Description	Measurement Unit	Interpretation
			the numeric equivalents – 0 and 100.
Port input utilization	Indicates the input utilization by the port.	Percent	
Port I/O utilization	Indicates the percentage of I/O used up by this port.	Percent	Ideally, this value should be low. A high value is indicative of excessive I/O activity on the port. Comparing the value of this measure across ports will enable administrators accurately identify that port on which I/O activity peaks.

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.