Monitoring Juniper SA Device

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

CHAPTER 1: INTRODUCTION 1

CHAPTER 2: HOW TO MONITOR JUNIPER SA DEVICE USING EG ENTERPRISE? 2

2.1 Managing the Juniper SA Device 2

CHAPTER 3: MONITORING THE JUNIPER SA DEVICE 4

3.1 The Operating System Layer 4

3.1.1 Ive Host Test 5

3.2 The Network Layer 7

3.3 The Tcp Layer 8

3.3.1 TCP Statistics Test 8

3.4 The VPN Service Layer 12

3.4.1 Ive Service Test 12

ABOUT EG INNOVATIONS 16

Table of Figures

Figure 2.1: Adding a Juniper SA device 3

Figure 2.2: A list of unconfigured tests 3

Figure 3.1: The layer model of the Juniper SA VPN 4

Figure 3.2: The test associated with the HOST layer 4

Figure 3.3: The tests associated with the Network layer 8

Figure 3.4: The test associated with the Tcp layer 8

Figure 3.5: The test associated with the VPN Service layer 12

Chapter 1: Introduction

The Juniper Networks Secure Access (SA) VPN is designed for medium to large enterprises, and features performance, scalability, and redundancy for organizations with high volume secure access and authorization requirements. The hardware platform of the SA device is designed to scale to the largest enterprise deployments and optimize application delivery, with available options that include redundant hot swappable hard disks, power supplies and fans, as well as GBIC-based multiple Ethernet ports for the creation of separate physical networks and redundant or meshed configurations. The SA device also features an SSL acceleration chipset to speed CPU-intensive encrypt/decrypt processes, as well as built in compression for all traffic. The SA device is built on the Virtual Extranet (IVE) platform, and uses the Secure Socket Layer (SSL) available in all Web browsers as a means of secure transport.

Any abnormal activity on the Juniper SA device, if not detected on time and resolved, could cause unsavory consequences such as a dramatic increase in the unsafe/unauthorized traffic on your network. Therefore, continuous monitoring of the device becomes mandatory. The eG Enterprise Suite helps network administrators in continuous monitoring of the Juniper SA device.

This document briefs you about how to manage and monitor the Juniper SA device.

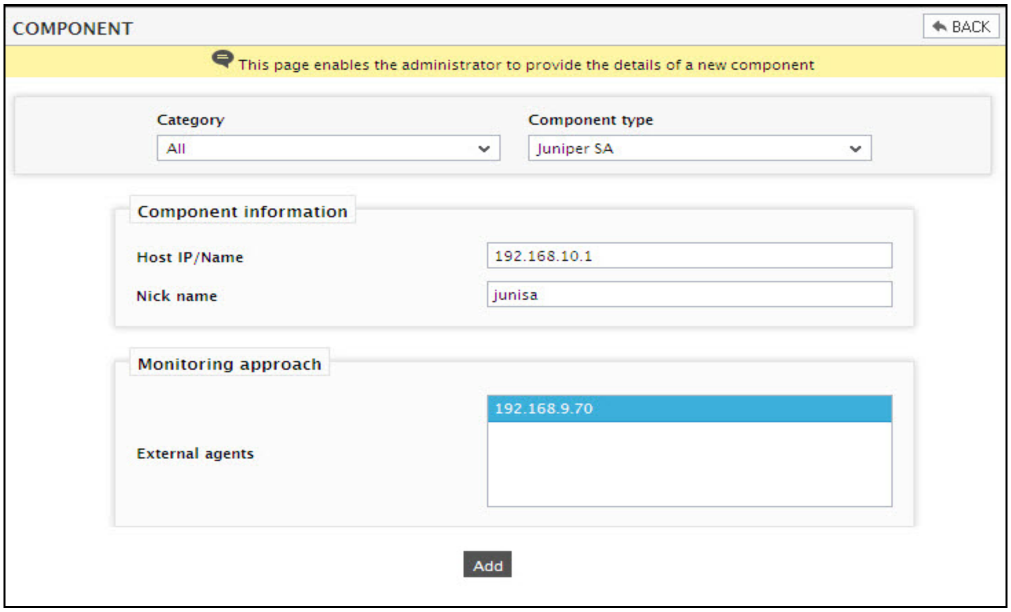
Chapter 2: How to Monitor Juniper SA Device Using eG Enterprise?

eG Enterprise adopts agentless approach to monitor the Juniper SA device. A single eG external agent is all that is required to monitor the Juniper SA device. This agent, when deployed on a remote host, executes tests that connect to the SNMP MIB of the Juniper SA device to be monitored, and collects statistics of interest from it. The key pre-requisite for monitoring the Juniper SA is to check whether the Juniper SA device is SNMP-enabled or not. Once this requirement is fulfilled, manage the Juniper SA device component using eG admin interface to start monitoring the Juniper SA device. The steps for managing the Juniper SA device are explained in the following section.

2.1 Managing the Juniper SA Device

To manage the Juniper SA device, do the following:

1. Log into the eG administrative interface.
2. Since the eG Enterprise suite cannot automatically discover a Juniper SA device, you need to manually add the component using the **COMPONENTS** page (Infrastructure-> Components -> Add/Modify) (see Figure 2.1). Remember that components manually added are managed automatically. Discovered components, however, are managed using the **COMPONENTS - MANAGE/UNMANAGE** page.



COMPONENT

This page enables the administrator to provide the details of a new component

Category: All

Component type: Juniper SA

Component information

Host IP/Name: 192.168.10.1

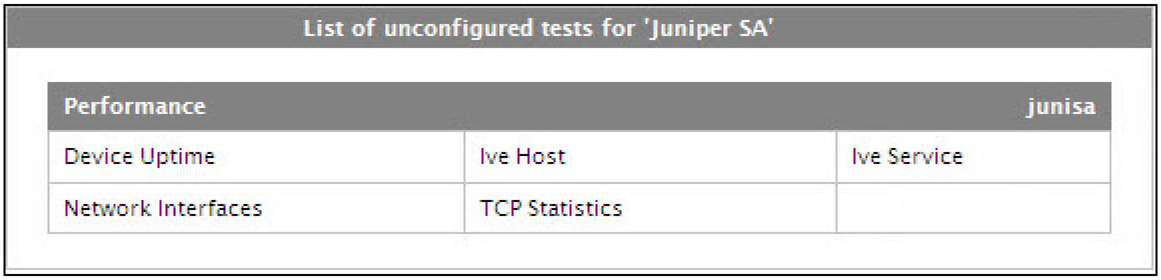
Nick name: junisa

Monitoring approach

External agents: 192.168.9.70

Figure 2.1: Adding a Juniper SA device

3. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).



List of unconfigured tests for 'Juniper SA'

Performance		junisa
Device Uptime	Ive Host	Ive Service
Network Interfaces	TCP Statistics	

Figure 2.2: A list of unconfigured tests

4. Click on the **Ive Service** test to configure it. To know how to configure the test, refer to Section **3.4.1**.
5. The next time you try to sign out of the admin interface, you will be prompted to configure the **Network Interfaces** test. To configure this test, click on the **Network Interfaces** test, refer to the *Monitoring Cisco Routers* document.
6. Finally, sign out of the eG administrative interface.

Chapter 3: Monitoring the Juniper SA Device

By executing a couple of simple tests on the SNMP MIB exposed by the Juniper SA device, the eG external agent performs 24 x 7 monitoring of the SA device, extracts critical performance data from the device, and reports the metrics so gathered to the eG manager. The eG manager in turn, maps these tests to the layers of the unique *Juniper SA* layer model (see Figure 3.1) that it prescribes for the Juniper SA device, and displays the performance data in the eG monitor console.

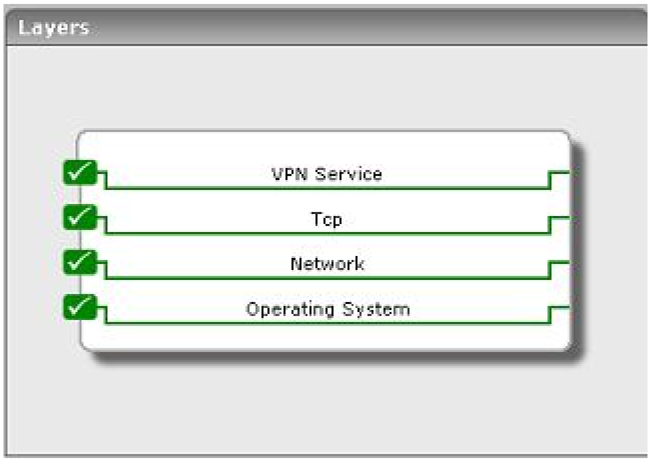


Figure 3.1: The layer model of the Juniper SA VPN

Each of the sub-sections to come will discuss every layer of the layer model, in more detail.

3.1 The Operating System Layer

Using the **IveHostTest** associated with it, the **HOST** layer returns host-level statistics such as the disk space usage, memory usage, etc., of the IVE system.

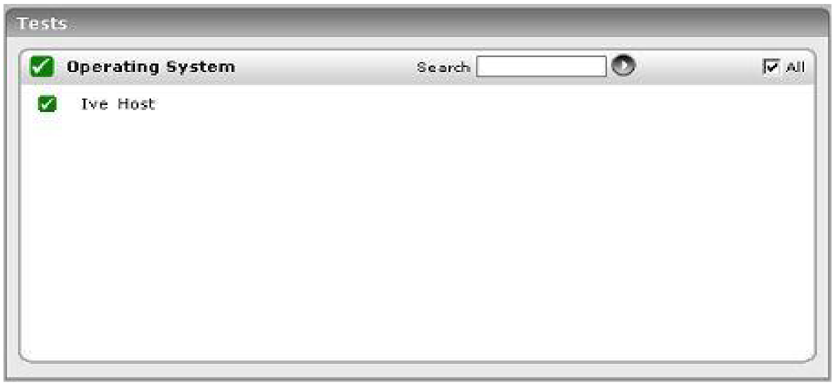


Figure 3.2: The test associated with the HOST layer

3.1.1 Ive Host Test

This test reports the host level statistics like disk space, CPU, memory and swap utilization of the Juniper SA device.

Target of the test : A Juniper SA device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Juniper SA device being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the monitored target.
Port	The port at which the device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
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

Parameter	Description
	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: • **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

Parameter	Description
	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
Disk space utilization	Indicates the percentage of disk space utilized on the IVE system.	Percent	A value close to 100% can indicate a potential problem situation where applications executing on the system may not be able to write data to the disk partition(s) with very high usage.
CPU utilization	Indicates the percentage of CPU utilized on the IVE system.	Percent	A high value could signify a CPU bottleneck. The CPU utilization may be high because a few processes are consuming a lot of CPU, or because there are too many processes contending for a limited resource.
Memory utilization	Indicates the percentage of memory utilized on the IVE system.	Percent	Ideally, this value should be low.
Swap utilization	Indicates the percentage of swap memory utilized on the IVE system.	Percent	An unusually high value for the swap usage can indicate a memory bottleneck.

3.2 The Network Layer

The tests associated with the **Network** layer reflect the status of network connectivity to and from the IVE system, the bandwidth usage of the interfaces supported by the system, and the uptime of the system.

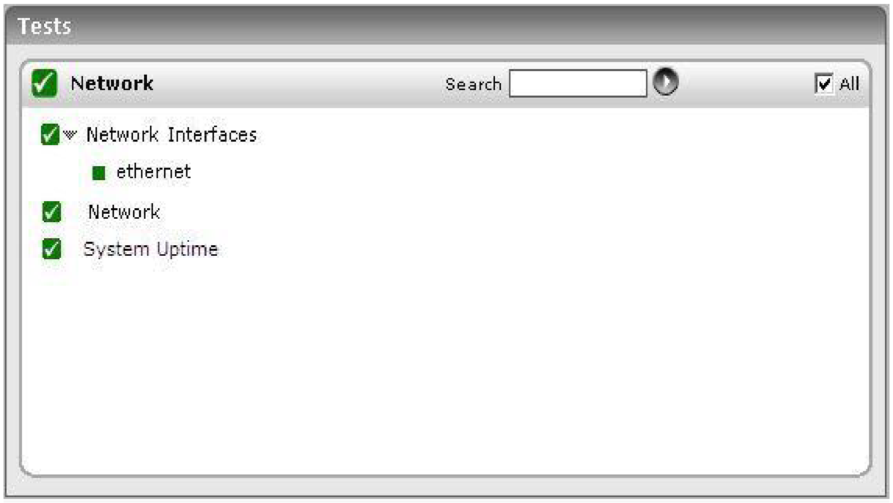


Figure 3.3: The tests associated with the Network layer

All the tests in Figure 3.3 have been dealt in the *Monitoring Cisco Routers* document.

3.3 The Tcp Layer

This test associated with the **Tcp** layer measures the incoming and outgoing TCP connections on the IVE system.

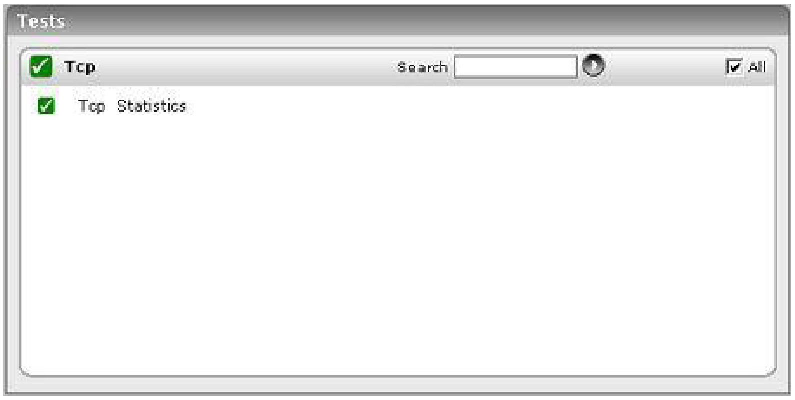


Figure 3.4: The test associated with the Tcp layer

3.3.1 TCP Statistics Test

This test reports TCP statistics pertaining to the IVE system.

Target of the test : A Juniper SA device

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the monitored target.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
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 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:

Parameters	Description
	- **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
Incoming connections	Indicates the connections per second received by the server.	Conns/Sec	A high value can indicate an increase in input load.
Outgoing connections	Indicates the connections per second initiated by the server	Conns/Sec	A high value can indicate that one or more applications executing on the host have started using a number of

Measurement	Description	Measurement Unit	Interpretation
			TCP connections to some other host (s).
Connection failures	Indicates the rate of half open TCP connections dropped from the listen queue.	Conns/Sec	This value should be 0 for most of the time. A prolonged non-zero value can indicate either that the server is under SYN attack or that there is a problem with the network link to the server that is resulting in connections being dropped without completion.
Current connections	Indicates the currently established connections.	Number	A sudden increase in the number of connections established on a host can indicate either an increase in load to one or more of the applications executing on the host, or that one or more of the applications are experiencing a problem (e.g., a slow down).
Segment rate in	The total number of segments received, including those received with errors. This count includes segments received on currently established connections.	Segments/Sec	
Segment rate out	Indicates the total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	Segments/Sec	
Retransmissions	Indicates the total number of segments retransmitted – that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	Segments/Sec	

3.4 The VPN Service Layer

The wide gamut of services provided by the Juniper SA device are closely monitored using the IveSvc test mapped to the this layer.

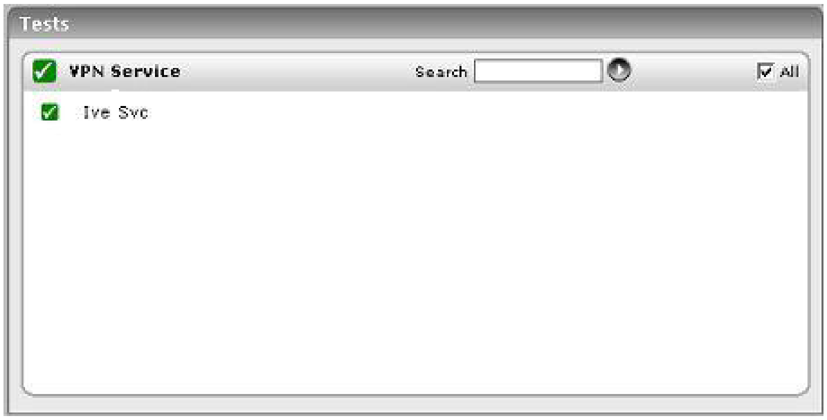


Figure 3.5: The test associated with the VPN Service layer

3.4.1 Ive Service Test

This test reports the statistics like user sign-ins and various hit ratios of the Juniper SA device.

Target of the test : A Juniper SA device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Juniper SA device being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the monitored target.
Port	The port at which the device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
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	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

Parameter	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
Log utilization	This measure indicates the log file growth in the IVE node.	Percent	
Signed in web users	Indicates the number of web users who have signed into the IVE system.	Number	
Signed in mail users	Indicates the number of mail users who have signed into the IVE system.	Number	
Concurrent users in the IVE node	Indicates the number of users who have simultaneously logged in for the IVE node.	Number	

Measurement	Description	Measurement Unit	Interpretation
Concurrent users in the cluster	Indicates the number of users logged in for the cluster.	Number	
Total hits	Indicates the total number of hits on the IVE system during the last measurement period.	Number	
File hits	Indicates the number of files on the IVE system that have been hit during the last measurement period.	Number	
Web hits	Indicates the number of web hits on the IVE system during the last measurement period.	Number	
Applet hits	Indicates the number of applet hits on the IVE node during the last measurement period,	Number	
Terminal hits	Indicates the terminal hits on the IVE system during the last measurement period.	Number	
Secure app mgr hits	Indicates the number of secure application manager (SAM) hits during the last measurement period.	Number	
Network connect hits	Indicates the number of network connects hits that have been hits during the last measurement period.	Number	
Meeting hits	Indicates the number of meeting hits during the last measurement period.	Number	

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.