Monitoring Cisco Pix Firewall

eG Innovations Product Documentation

www.eginnovations.com

eG Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Cisco PIX 500 Series Firewalls are purpose-built security appliances that deliver enterprise-class security services including stateful inspection firewalling, standards-based IPsec Virtual Private Networking (VPN), intrusion protection and much more.

In an environment where a Cisco PIX firewall is used, the continuous availability of the firewall device and its error-free functioning is very crucial to the safety of the data that is transacted within the environment. Continuous monitoring of the Cisco PIX firewall hence becomes imperative. Hence, the eG Enterprise suite of products includes customized monitoring capabilities for the Cisco PIX firewall.

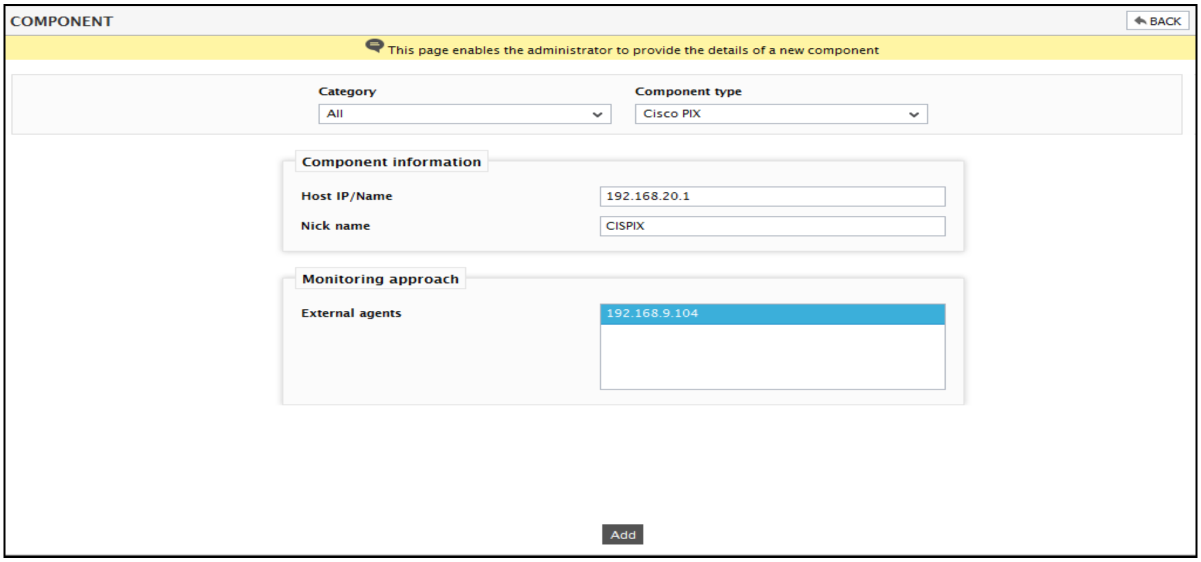
Chapter 2: How does eG Enterprise Monitor Cisco PIX Firewall?

A single eG external agent is all that is required to monitor a firewall. This agent, when deployed on a remote host, executes tests that connect to the SNMP MIB of the firewall device to be monitored, and collects statistics of interest from it. To enable the eG agent to communicate with the Cisco Pix firewall, make sure that the Cisco Pix firewall is SNMP-enbled.

2.1 Managing the Cisco PIX Firewall

To add a Cisco PIX firewall component for monitoring, do the following:

1. Log into the eG administrative interface.
2. If the Cisco PIX firewall is already discovered, then directly proceed towards managing it using the **COMPONENTS - MANAGE/UNMANAGE** page (Infrastructure -> Components -> Manage/Unmanage). If not, manually add the component by using the below steps.
3. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
4. In the **COMPONENT** page that appears next, select Cisco PIX as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.



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

Category	All
Component type	Cisco PIX

Component information

Host IP/Name	192.168.20.1
Nick name	CISPIX

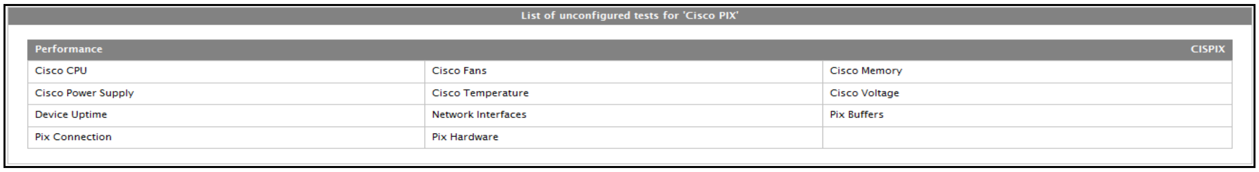
Monitoring approach

External agents	192.168.9.104

Figure 2.1: Adding a Cisco Pix firewall

5. Specify the **Host IP/Name** and the **Nick name** of the Cisco Pix firewall in Figure 2.1. Then, click the **Add** button to register the changes.

6. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

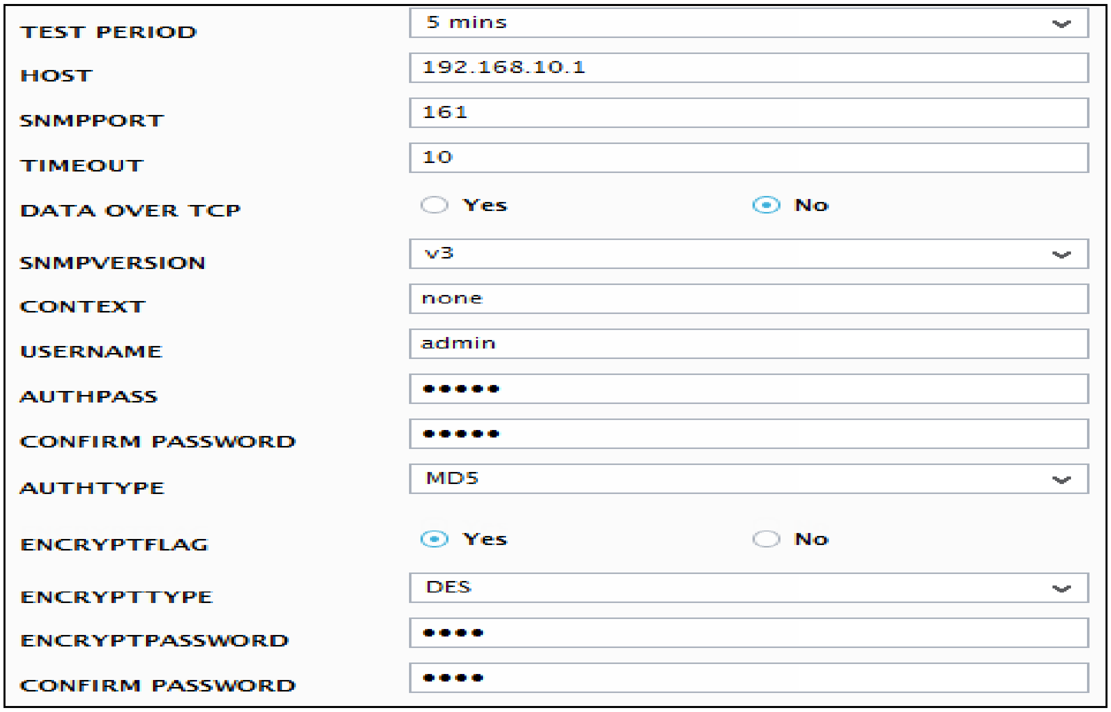


List of unconfigured tests for 'Cisco PIX'

Performance		CISPIX
Cisco CPU	Cisco Fans	Cisco Memory
Cisco Power Supply	Cisco Temperature	Cisco Voltage
Device Uptime	Network Interfaces	Pix Buffers
Pix Connection	Pix Hardware	

Figure 2.2: List of unconfigured tests to be configured for the Cisco Pix firewall

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



TEST PERIOD	5 mins
HOST	192.168.10.1
SNMPPORT	161
TIMEOUT	10
DATA OVER TCP	○ Yes ● No
SNMPVERSION	v3
CONTEXT	none
USERNAME	admin
AUTHPASS	●●●●●
CONFIRM PASSWORD	●●●●●
AUTHTYPE	MD5
ENCRYPTFLAG	● Yes ○ No
ENCRYPTTYPE	DES
ENCRYPTPASSWORD	●●●●
CONFIRM PASSWORD	●●●●

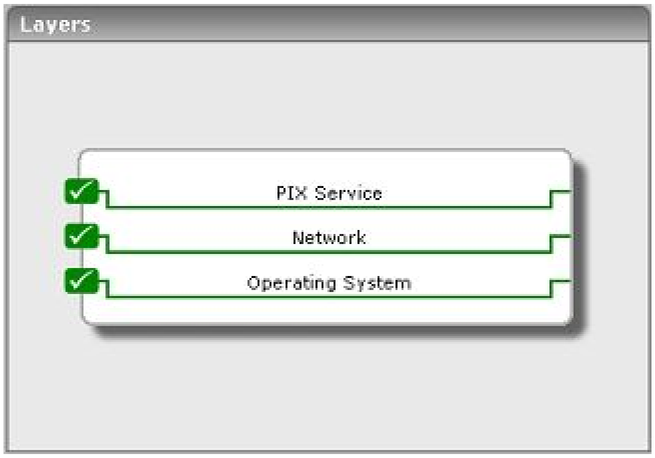
Figure 2.3: Configuring the PIX Connection test

8. To know how to configure these parameters, refer to **Monitoring Cisco PIX Firewall**. Refer to the *Monitoring Cisco Router* document for details on configuring the Cisco CPU, Cisco Fan, Cisco Memory, Cisco Voltage, Cisco Temperature, Cisco Power Supply and Network Interfaces tests.

9. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring Cisco PIX Firewall

eG Enterprise offers a 100% web-based Cisco PIX monitoring model (see Figure 3.1) that monitors the status of the hardware and connections to the Cisco PIX firewall, and in the process, reports abnormalities (if any).



Layers

✓ PIX Service

✓ Network

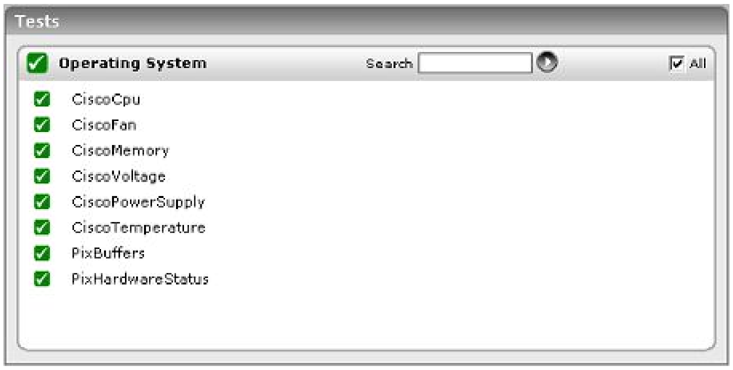
✓ Operating System

Figure 3.1: The layer model of a Cisco PIX firewall

Every layer of Figure 3.1 is mapped to one/more tests that execute on the firewall, and extract critical performance statistics from the SNMP MIB of the firewall. The sections to come discuss each layer in great detail.

3.1 The Operating System Layer

This layer reveals whether the firewall is loaded with sufficient hardware resources to enable optimum performance (see Figure 3.2).



Tests

✓ Operating System Search ☑ All

- ✓ CiscoCpu
- ✓ CiscoFan
- ✓ CiscoMemory
- ✓ CiscoVoltage
- ✓ CiscoPowerSupply
- ✓ CiscoTemperature
- ✓ PixBuffers
- ✓ PixHardwareStatus

Figure 3.2: The tests associated with the Operating System layer of a Cisco PIX firewall

To know how to configure the CiscoCpu, CiscoFan, CiscoMemory, CiscoVoltage, CiscoTemperature, and CiscoPowerSupply tests, refer to in the *Monitoring Cisco Router* document. The sections that follow will hence provide details about the PixBuffers and PixHardwareStatus test only.

3.1.1 Pix Buffers Test

This test measures the system buffer usage of a Cisco PIX device.

Target of the test : A Cisco PIX Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Cisco PIX firewall being managed.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco PIX firewall for which this test is to be configured.
SNMPPort	The port at which the Cisco PIX firewall 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

Parameter	Description
	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: • **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

Parameter	Description
	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
Maximum allocated	The maximum number of allocated blocks since system startup.	Number	
Buffers available	The current number of available blocks.	Number	A low value indicates a memory bottleneck.
Fewest available	The fewest blocks available since system startup.	Number	By tracking this value over time, an administrator can determine times when buffer availability was at its minimum.

3.1.2 Pix Hardware Status Test

This test reports the status of various hardware units of a Cisco PIX device.

Target of the test : A Cisco PIX Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for every hardware unit associated with a Cisco PIX firewall being managed.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco PIX firewall for which this test is to be configured.
SNMPPort	The port at which the Cisco PIX firewall exposes its SNMP MIB; the default is *161*.

Parameter	Description
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: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG

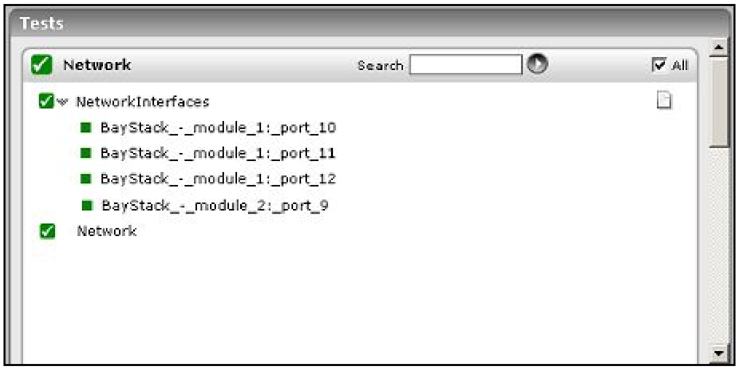
Parameter	Description
	agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption 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**.
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 enabled/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
Status	The current status of various hardware units like memory, disk, power, network interface, cpu, primary unit, secondary unit etc.	Number	The value 1 indicates that the hardware unit is functioning properly. A value of 0 indicates a problem.

3.2 The Network Layer

The Network layer, as always, checks whether the firewall device is available over the network or not, and monitors the percentage of bandwidth used by each network interface supported by the firewall.



- ☑ NetworkInterfaces
  - 🟩 BayStack_-_module_1:_port_10
  - 🟩 BayStack_-_module_1:_port_11
  - 🟩 BayStack_-_module_1:_port_12
  - 🟩 BayStack_-_module_2:_port_9
- ☑ Network

Figure 3.3: The tests mapped to the Network layer of the Cisco PIX firewall

3.3 The PIX Service Layer

The test associated with this layer measures the workload on the firewall device in terms of the number of connections to it.

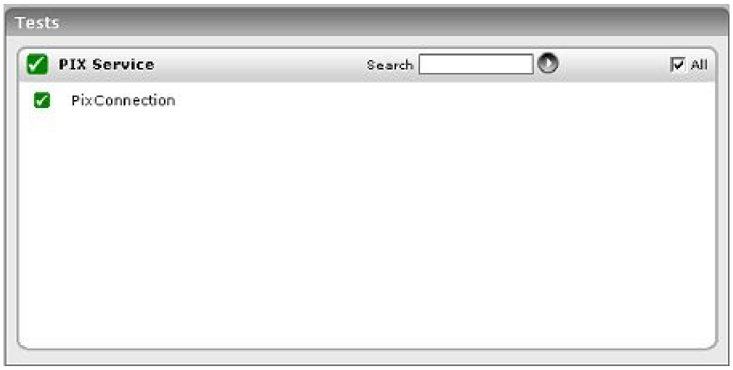


Figure 3.4: The test associated with the PIX Service layer

3.3.1 Pix Connection Test

This test reports the connection-related statistics pertaining to a Cisco PIX firewall.

Target of the test : A Cisco PIX Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Cisco PIX firewall being managed.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco PIX firewall for which this test is to be configured.
SNMPPort	The port at which the Cisco PIX firewall 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

Parameter	Description
	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: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.

Parameter	Description
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
Open connections	The number of currently opened connections	Number	This metric is an indicator of the current workload.
Closing connections	The number of currently closing connections	Number	
Half open connections	The number of half opened connections	Number	
Connections in use	The number of connections currently in use	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.

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.