Monitoring CryptoServer HSM

Table of Contents

Table of Figures

Chapter 1: Introduction to CryptoServer HSM Monitoring

CryptoServer HSM is the Hardware Security module that was developed to ensure the efficiency and security for the cryptographic operations. It is used for performing Cryptographic Operations such as Generating key, Saving the key securely, generating random numbers, Generating and verifying signatures, Encrypting and decrypting data and calculating hash values. CryptoServer HSM protects all cryptographic operations or keys and ensures the security of cryptographic key material for servers and applications.

CryptoServer HSM can be used by all industries such as manufacturing industries, automotive, banking and financial services, government agencies, healthcare, cloud, energy and utilities and media.

This means that even the slightest dip in the performance of CryptoServer HSM can adversely impact user experience with the device. To avoid this, administrators should continuously measure the performance of the device, instantly detect anomalies, and fix them before users notice. This is where eG Enterprise helps. eG Enterprise notifies administrators of abnormalities in device performance, so that they can promptly intervene and do the needful to resolve them.

This document will discuss about each of these models.

Chapter 2: How Does eG Enterprise Monitor CryptoServer HSM?

eG Enterprise monitors CryptoServer HSM using an agent- based approach. For this purpose, you need to install an eG agent on your host system. This eG agents runs native Linux commands on CryptoServer HSM to pull the desired metrics.

The broad steps for monitoring the CryptoServer HSM using eG Enterprise are as follows:

1. Manage the CryptoServer HSM using the eG admin interface
2. Configure the tests for the component.

The sections to come will discuss about the tests mapped to CryptoServer HSM.

2.1 Managing CryptoServer HSM

To manage the CryptoServer HSM , do the following:

1. Log into the eG admin interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **Add Components** page that appears next, select *CryptoServer HSM* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

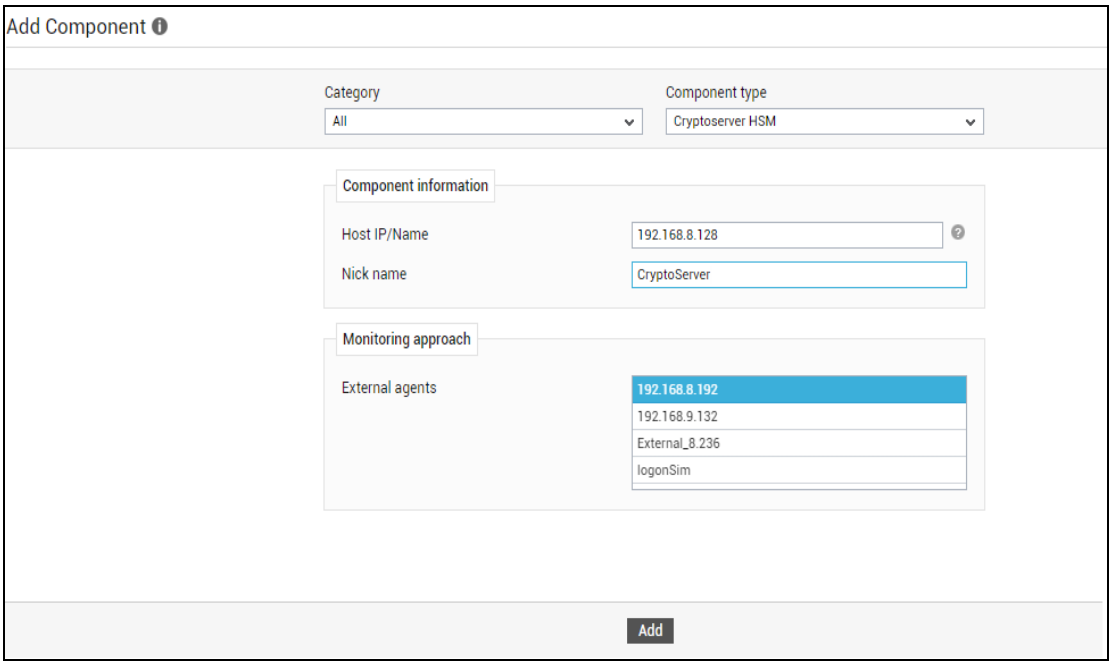

Figure 2.1: Adding the CryptoServer HSM

4. Specify the **Host Name** and **Nick name** for the CryptoServer HSM .
5. Next, assign a **External Agent** to the component.
6. Finally, click the **Add** button to add the CryptoServer HSM to the eG Enterprise system. Components manually added will be automatically managed by eG Enterprise.

2.2 Configuring Tests

Once the CryptoServer HSM is managed, try to do the following:

1. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
2. Select the **Show managed component types** only check box and then select the *CryptoServer HSM* component under **Component Type** list box. Then, the record appears in the grid as shown in Figure 2.2.

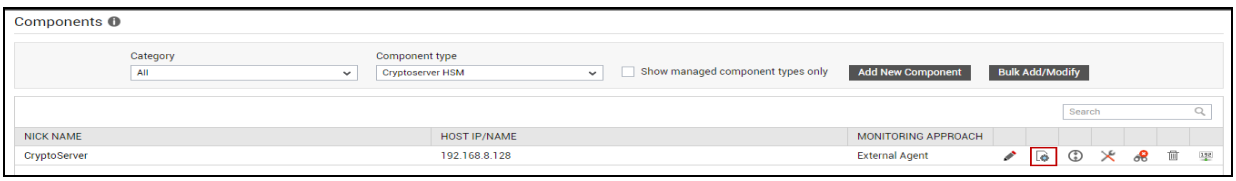

Figure 2.2: Managed CryptoServer HSM record

3. Select the Configure Tests icon as shown in Figure 2.2 in the grid to configure the tests mapped for the component. This will invoke Figure 2.3 listing all the configured tests for the CryptoServer HSM.

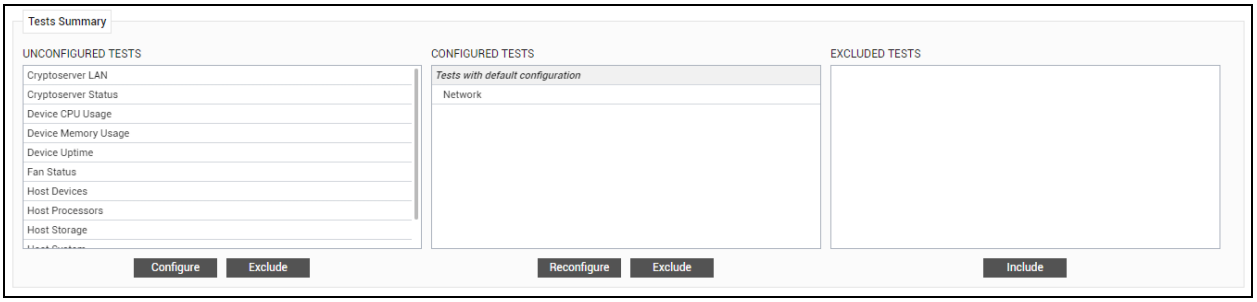

Figure 2.3: The list of unconfigured tests for the CryptoServer HSM

4. Click on any test to configure it and sign out of the eG admin interface.

Chapter 3: Monitoring CryptoServer HSM

eG Enterprise offers a dedicated monitoring model for CryptoServer HSM which periodically monitors the Fan status, Server status and LAN status of the appliance.

Figure 3.1: The layer model of CryptoServer HSM component

Using the metrics reported by the tests mapped to this layer, administrators can find quick and accurate answers to certain persistent performance queries, such as the following:

- Is the CPU temperature of the CryptoServer HSM normal ?
- What is the current status of the Redundant power supply unit and battery?
- What is the current operational mode of the CryptoServer HSM?
- Are the fans operating normally?

Since the bottom layers are discussed in *Monitoring Unix and Windows Servers* document, the section that follows will discuss the tests pertaining to the **CryptoServer LAN** layer alone.

3.1 The CryptoServer LAN Layer

Using the tests mapped to this layer, administrators can closely monitor the appliance related details such as temperature, Operational mode, Power supply unit, Battery state, Module state and operational speed of the fan.

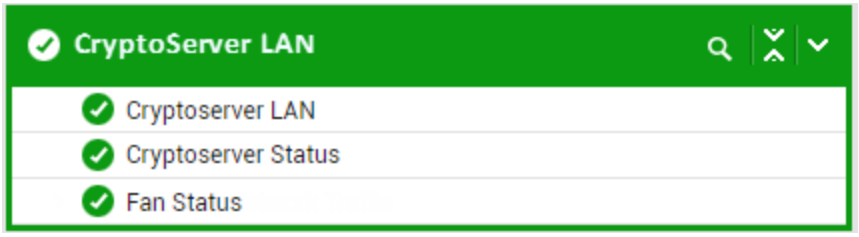

Figure 3.2: The tests mapped to the CryptoServer LAN layer

3.1.1 CryptoServer LAN Test

This test tracks the current status of the redundant power supply unit and current temperature of the CPU available in the target CryptoServer HSM device. Using this test, administrators can check if the temperature of the target CryptoServer HSM device is within admissible range and can initiate remedial measures if abnormalities are detected.

Target of the test : A CryptoServer HSM

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target CryptoServer HSM that is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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

Parameter	Description
	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 environments, you can instruct the eG agent to conduct the SNMP data traffic related

Parameter	Description
	to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU temperature	Indicates the current CPU temperature of the CryptoServer LAN in the CryptoServer HSM.	Celsius	Ideally, the value of this measure should be in a permissible range. A sudden rise/fall in the value of this measure could be a cause for concern.
Redundant powersupply status	Indicates the current status of the Redundant power supply unit in the CryptoServer LAN.	Number	The values that this measure reports and their corresponding numeric values are listed in the table below: **Measure Value** / **Numeric Value** Failed / 0 OK / 1 **Note:** By default, this measure reports the **Measure Value**s discussed in the table above to indicate the status of the Redundant power supply unit. The graph of this measure however, is represented using the numeric equivalents only.
Load average	Indicates the the load average of the Crypto server LAN in CryptoServer HSM.	Percent	
Client connection load	Indicates the client connection load of the CryptoServer LAN in CryptoServer HSM.	Percent	

3.1.2 CryptoServer Status Test

CryptoServer HSM is a network appliance that ensures the security of cryptographic key material for servers and applications. The CryptoServer HSM is equipped with two batteries(Carrier battery and External battery) to ensure that no security-critical information is lost or deleted on the hardware security model when the device is switched off, or if operation is interrupted due to power failure. Since the batteries available in the CryptoServer are not rechargeable, and if the batteries are exhausted, sensitive data will be automatically deleted which will become a burden on the administrators to rebuild the entire data. It is therefore essential to have a constant vigil on the status of the battery. The **CryptoServer Status** test helps administrators in this regard.

This test reports the overall status of the hardware components of the target CrytoServer HSM. The operational mode , temperature and battery status are also reported. Using this test, administrators can easily detect abnormalities if any, in the CryptoServer HSM and initiate remedial measures at the earliest.

Target of the test : A CryptoServer HSM

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target CryptoServer HSM that is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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

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**.

Measures made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Operational mode</td><td>Indicates the current operational mode of the target device.</td><td>RPM</td><td>The values that this measure reports and their corresponding numeric values are listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Power down</td><td>0</td></tr><tr><td>Alarm</td><td>1</td></tr><tr><td>Maintenance</td><td>2</td></tr><tr><td>Operational</td><td>3</td></tr><tr><td>Boot loader</td><td>4</td></tr></table>Note:
By default, this measure reports the Measure Values discussed in the table above to indicate the operational mode of the target device. In the graph of the measure however, the operational state is indicated using the corresponding numeric equivalents only.</td></tr>
<tr><td>State</td><td>Indicates the current state of the target device.</td><td></td><td>The values that this measure reports</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>and their corresponding numeric values are listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Max/Unknown</td><td>0</td></tr><tr><td>Blank</td><td>1</td></tr><tr><td>Manufactured</td><td>2</td></tr><tr><td>Produced</td><td>3</td></tr><tr><td>Initialized</td><td>4</td></tr><tr><td>Operational</td><td>5</td></tr><tr><td>Defect</td><td>6</td></tr></table>
Note:
By default, this measure reports the Measure Values discussed in the table above to indicate the current state of the target device. In the graph of the measure however, the global state is indicated using the corresponding numeric equivalents only.</td></tr>
<tr><td>Temperature</td><td>Indicates the current temperature of the target device.</td><td>Celsius</td><td>The CryptoServer HSM is fully operational only if its internal temperature does not exceed or fall below a well defined operational temperature range.
An abnormally high value for this measure could be a cause for concern.</td></tr>
<tr><td>Alarm state</td><td>Indicates the current alarm state of the target device.</td><td></td><td>The values that this measure can report and their corresponding numeric values are as follows:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Off</td><td>0</td></tr><tr><td>On</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>Note:
By default, this measure reports the Measure Values discussed in the table above to indicate the alarm state of the target device. In the graph of the measure however, the alarm state is indicated using the corresponding numeric equivalents only.</td></tr>
<tr><td>Battery state</td><td>Indicates the current battery state of the target device.</td><td></td><td>The values that this measure can report and their corresponding numeric values are as follows:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Absence</td><td>0</td></tr><tr><td>Low</td><td>1</td></tr><tr><td>OK</td><td>2</td></tr></table>Note:
By default, this measure reports the Measure Values discussed in the table above to indicate the battery state of the target device. In the graph of the measure however, the battery state is indicated using the corresponding numeric equivalents only.</td></tr>
<tr><td>Module state</td><td>Indicates the current module state of the target device</td><td></td><td>The values that this measure can report and their corresponding numeric values are as follows:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Failed</td><td>0</td></tr><tr><td>OK</td><td>1</td></tr></table>Note:
By default, this measure reports the</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Measure Values discussed in the table above to indicate the module state of the target device. In the graph of the measure however, the global state is indicated using the corresponding numeric equivalents only.

3.1.3 Fan Status Test

Fans ensure that the temperature of the CryptoServer HSM device are well-within operable limits. A sudden rise/fall of the fan's speed may lead to fan failures. This in turn, may cause permanent damage to the sensitive components of the device. To avoid such heavy duty damage, it is necessary to monitor the operational speed of the fans at regular intervals. This is where the **Fan Status** test exactly helps!

This test auto-discovers the fans in the CryptoServer HSM and for each fan, reports the current operational speed. Using this test, administrators can figure out the fans that do not operate within the admissible speed range and replace them at the earliest.

Target of the test : A CryptoServer HSM

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target CryptoServer HSM that is being monitored.

Descriptor of the test : Fan name

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Speed	Indicates the current operational speed of the fan.	RPM	The speed of the fan should be well within admissible range. A sudden/significant rise/fall in the value of this measure could be a cause of concern which warrants an investigation.

Restricted Rights Legend

Trademarks

Copyright