



Monitoring HP Enterprise Secure Key Manager

eG Innovations Product Documentation

www.eginnovations.com



Table of Contents

CHAPTER 1: INTRODUCTION	1
CHAPTER 2: HOW TO MONITOR A HP ENTERPRISE SECURE KEY MANAGER (ESKM) USING EG ENTERPRISE?	2
2.1 Pre-requisites for Monitoring the HP Enterprise Secure Key Manager	2
2.2 Managing the HP Enterprise Security Key Manager	2
CHAPTER 3: MONITORING THE HP ENTERPRISE SECURE KEY MANAGER	4
3.1 The ESKM Service layer	5
3.1.1 ESKM Server Requests Test	5
3.2 The Operating System layer	8
3.2.1 ESKM CPU Test	9
3.2.2 ESKM Disk Traps Test	11
3.2.3 ESKM Fan Traps Test	14
3.2.4 ESKM Memory Test	17
3.2.5 ESKM PowerSupply Traps Test	20
ABOUT EG INNOVATIONS	24

Table of Figures

Figure 2.1: Adding the HP Enterprise Security Key Manager	3
Figure 2.2: List of tests to be configured for HP Enterprise Security Key Manager	3
Figure 3.1: The layer model of the HP Enterprise Secure Key Manager	4
Figure 3.2: The tests associated with the ESKM Service layer	5
Figure 3.3: The tests associated with the Operating System layer	9

Chapter 1: Introduction

Encryption is the process of changing data into a form that cannot be read until it is deciphered with the key used to encrypt the data, protecting the data from unauthorized access and use. Encryption is primarily designed to protect the data once it is offline and to prevent it from being accessed by unauthorized users. Users will be able to read and append the encrypted data as long as a key server token containing the correct key is installed and the appropriate passwords are available.

When a key manager is enabled and properly configured, tape data will automatically be encrypted with keys delivered from the key manager. The HP Enterprise Secure Key Manager is designed to deliver keys to encrypt/decrypt data appropriately. If the keys are not delivered on time for encrypting the data or if the keys are not delivered on time for decrypting the encrypted data, then users may find it difficult to read/write the data. Therefore, it is imperative to monitor the HP Enterprise Secure Key Manager. eG Enterprise helps administrators to monitor the HP Enterprise Secure Key Manager and identify issues before end users complain of improper encryption/decryption of data. The chapters discussed below help administrators to figure out how eG Enterprise helps in monitoring the HP Enterprise Secure Key Manager.

Chapter 2: How to monitor a HP Enterprise Secure Key Manager (ESKM) using eG Enterprise?

eG Enterprise uses a single eG external agent to monitor the HP Enterprise Secure Key Manager. The external agent can be deployed on any remote host in the environment. This agent periodically tracks the SNMP traps and polls the SNMP MIB of the appliance to collect critical statistics pertaining to its performance. To enable the eG agent to communicate with the appliance, a set of pre-requisites needs to be kept in place. These requirements have been explained in the following section.

2.1 Pre-requisites for Monitoring the HP Enterprise Secure Key Manager

To ensure that the eG agent is able to use both the SNMP traps and the SNMP MIB of the HP Enterprise Secure Key Manager, the following pre-requisites should be fulfilled:

1. The SNMP service should be enabled on the HP Enterprise Secure Key Manager;
2. The eG SNMP trap receiver service should be installed on the external agent host;
3. SNMP traps should be enabled on the HP Enterprise Secure Key Manager and configured to send traps to the external agent host;

Once the above-said pre-requisites are fulfilled, proceed monitoring the HP Enterprise Secure Key Manager. To start monitoring, first manage the *HP Enterprise Security Key Manager* component using the eG administrative interface as discussed in following section.

2.2 Managing the HP Enterprise Security Key Manager

The eG Enterprise cannot automatically discover the HP Enterprise Security Key Manager component. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add a HP Enterprise Security Key Manager, do the following:

1. Log into the eG administrative interface.
2. eG Enterprise cannot automatically discover HP Enterprise Security Key Manager (ESKM). You need to manually add the server using the **COMPONENTS** page (see Chapter 2) that appears when the Infrastructure -> Components -> Add/Modify menu sequence is followed. Remember

that components manually added are managed automatically.

Figure 2.1: Adding the HP Enterprise Security Key Manager

3. Specify the **Host IP** and the **Nick name** of the HP Enterprise Security Key Manager in Chapter 2. Then click the Add button to register the changes.
4. When you attempt to sign out, a list of unconfigured tests appears.

List of unconfigured tests for 'HP Enterprise Security Key Manager'		
Performance		HPeskM
Device Uptime	ESKM CPU	ESKM Memory
ESKM Server Requests		

Figure 2.2: List of tests to be configured for HP Enterprise Security Key Manager

5. Click on the **ESKM CPU** test to configure it. To know how to configure the test, refer to Section 3.2.1.
6. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the HP Enterprise Secure Key Manager

eG Enterprise has developed a dedicated *HP Enterprise Secure Key Manager* monitoring model which periodically checks the CPU and memory utilization of the key manager, the trap messages from power supply units, disks and fans of the key manager and the requests served by the key manager so that the any abnormalities in the key manager can be identified before end users start complain about the non-availability of encrypted/decrypted data.

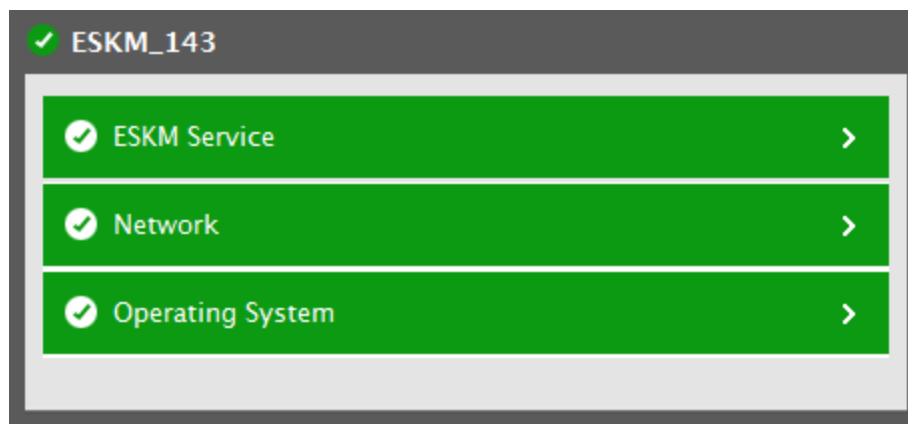


Figure 3.1: The layer model of the HP Enterprise Secure Key Manager

Every layer of Figure 1 is mapped to a variety of tests which connect to the SNMP MIBs of the target HP Enterprise Secure Key Manager to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- What is the CPU utilization of the key manager?
- How well the memory of the key manager is utilized?
- How many disk failure events were triggered on the key manager?
- How many fan failure events were triggered on the key manager?
- How many power supply failure events were triggered on the key manager?
- How well the requests were served by the key manager?
- How many requests served by the key manager were actually successful and how many actually failed?

Since the tests of the Network layer have already been discussed in the *Monitoring Unix and Windows servers* and *Monitoring Network Elements* documents in details, the sections to come will discuss all other layers of Figure 3.1 in detail.

3.1 The ESKM Service layer

Using this layer, administrators can figure out the total number of requests to the HP Enterprise Secure Key Manager and identify the requests that were successful and the requests that failed.

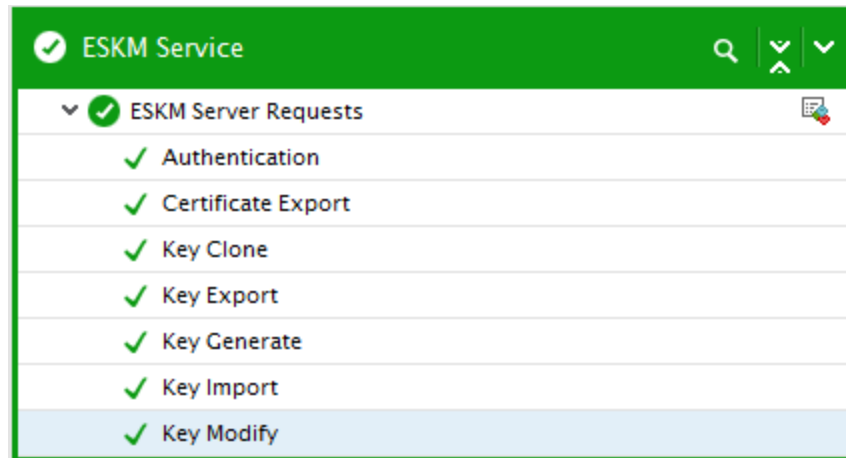


Figure 3.2: The tests associated with the ESKM Service layer

3.1.1 ESKM Server Requests Test

The HP Enterprise Secure Key Manager (ESKM) is a unified solution for encryption key management and security policy enforcement across the enterprise. The security server automates generation and retrieval of encryption keys for multiple client applications and devices based on security policies. This enables the key management transactions occur quickly and transparently to business application users. The security server encrypts or decrypts the data at rest or in motion based on the server requests received from the key server. The server requests can be any one of the following types:

- Authentication
- Certificate Export
- Key Clone
- Key Export
- Key Generate

- Key Import
- Key Modify

The HP ESKM generates and manages the keys according to the above-mentioned server requests that are received from the key server. When the server has processed the server requests, the security server sends back the encrypted keys to the key server. Then, the key server delivers the encrypted keys to users in the most secure way. For uninterrupted delivery of the keys, the administrator should make sure that the server requests are processed successfully and sent back to the key server without any delay. When the delay occurs during processing of the server requests, the server requests are stored in a queue. If the server requests are kept in the queue for longer duration or failed due to network or manual errors, then, the appliance will experience processing bottleneck. This in turn will impact performance of the key server and also cause delay in delivery of the keys. Therefore, the administrator should closely monitor the server requests processing on the appliance and quickly initiate remedial measures to prevent the delay before the users complaint about slowness in key delivery. The **ESKM Server Requests** test aids the administrator in this regard!

For each type of server request, this test reports total number of requests processed by the security server and also reveals number of requests that were processed successfully and number of requests that failed. This way, this test alerts the administrator to processing bottleneck at the security server.

Target of the test : A HP Enterprise Security Key Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the each type of server requests processed by the target HP Enterprise Security Key Manager that is to be monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SNMP Port	The port number through which the target router exposes its SNMP MIB; the default is 161.
SNMP Version	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMP version 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

Parameters	Description
	list.
SNMP Community	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 SNMP version chosen is v3, then this parameter will not appear.
User Name	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 the username 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 this text box. By default, this parameter is set to none.
Auth Pass	Specify the password that corresponds to the above-mentioned user name. This parameter once again appears only if the snmpversion selected is v3.
Confirm Password	Confirm the authpass by retyping it here.
Auth Type	<p>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:</p> <ul style="list-style-type: none"> • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
Encrypt Flag	This flag appears only when v3 is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, this is set to no by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the yes option.
Encrypt Type	If this is set to yes, then you will have to mention the encryption type by selecting an

Parameters	Description
	option from the encrypt type list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> • DES – Data Encryption Standard • AES – Advanced Encryption Standard
Encrypt Password	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
Total requests	Indicates the total number of server requests of this type that were processed on the security server.	Number	
Successful requests	Indicates the number of server requests of this type that were processed successfully.	Number	A high value is desired for this measure.
Failed requests	Indicates the number of server requests of this type that failed.	Number	Ideally, the value of this measure should be zero.

3.2 The Operating System layer

Using the test mapped to this layer, administrators can figure out the CPU and memory utilization, proactively identify the trap messages sent by the security server due to the failure of various critical

components of the HP Enterprise Secure Key Manager and take remedial measures before any serious issues occur.

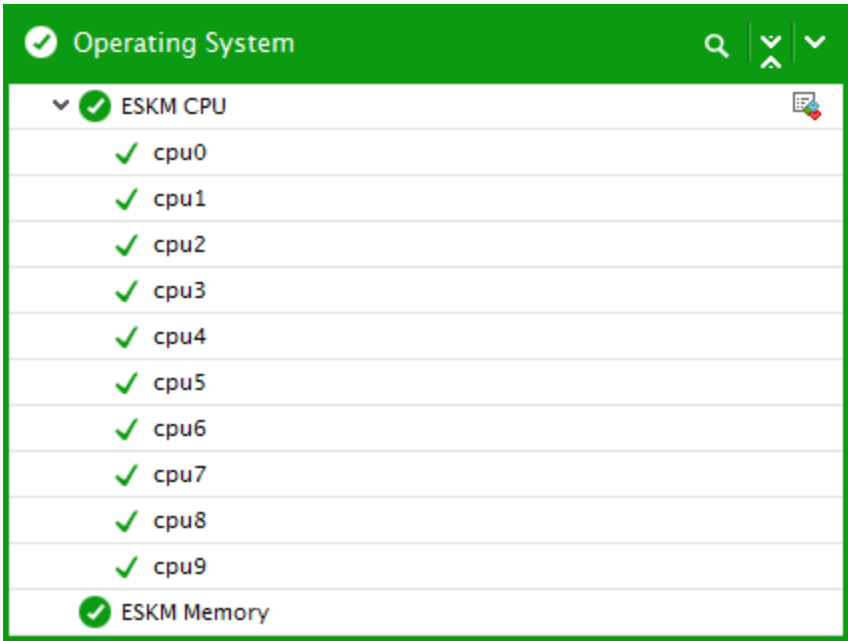


Figure 3.3: The tests associated with the Operating System layer

3.2.1 ESKM CPU Test

This test auto-discovers the CPUs available in the HP Enterprise Secure Key Manager (ESKM) security server and reports the utilization of each CPU. Using this test, administrators can be proactively alerted to abnormal CPU utilization so that further investigation could be warranted and the real reason behind resource contention be determined.

Target of the test : A HP Enterprise Security Key Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each CPU available in the target HP Enterprise Security Key Manager that is to be monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.

Parameters	Description
SNMP Port	The port number through which the target router exposes its SNMP MIB; the default is 161.
SNMP Version	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMP version 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.
SNMP Community	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 SNMP version chosen is v3, then this parameter will not appear.
User Name	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 the username 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 this text box. By default, this parameter is set to none.
Auth Pass	Specify the password that corresponds to the above-mentioned user name. This parameter once again appears only if the snmpversion selected is v3.
Confirm Password	Confirm the authpass by retyping it here.
Auth Type	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: <ul style="list-style-type: none"> • MD5 – Message Digest Algorithm

Parameters	Description
	<ul style="list-style-type: none"> • SHA – Secure Hash Algorithm
Encrypt Flag	This flag appears only when v3 is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, this is set to no by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the yes option.
Encrypt Type	<p>If this is set to yes, then you will have to mention the encryption type by selecting an option from the encrypt type list. SNMP v3 supports the following encryption types:</p> <ul style="list-style-type: none"> • DES – Data Encryption Standard • AES – Advanced Encryption Standard
Encrypt Password	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
CPU utilization	Indicates the percentage of resources utilized by this CPU.	Percentage	A value close to 100% indicates excessive usage of CPU. Compare the value of this measure across the CPUs to know which CPU is resource-intensive.

3.2.2 ESKM Disk Traps Test

This test intercepts the disk failure traps sent by the HP Enterprise Security Key Manager, extracts relevant information related to the failure from the traps, and reports the count of disk failure events

to the eG manager. This information enables administrators to detect the disk failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A HP Enterprise Security Key Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Enterprise Security Key Manager that is to be monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
Port	The port at which the specified HOST listens. By default, this is NULL.
Source Address	Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
OID Value	Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

In this case the oidvalue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.

An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.

Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the

Parameters	Description
	<p>OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:</p> <p>Trap5: .1.3.6.1.4.1.9156.1.1.5-any.</p> <p>In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be:</p> <p>Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any.</p> <p>Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.</p>
ShowOID	Specifying True against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
TrapOIDs	By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against DD frequency.
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.

Parameters	Description
	<p>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:</p> <ul style="list-style-type: none"> • 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
Disk failures	Indicates the number of times the disk failure event was triggered during the last measurement period.	Number	<p>The failure events may be generated due to the failure of disks of the security server. If the failure events are not rectified within a certain pre-defined timeperiod, the security server will be shutdown automatically.</p> <p>Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the security server.</p>

3.2.3 ESKM Fan Traps Test

The HP Enterprise Secure Key Manager (ESKM) comprises of six fans that provide variable speed redundant cooling effect to maintain the temperature of the core hardware components within the server. If any of these fans fails due to physical damage or unstable power fluctuations, then, the temperature of the core hardware components may suddenly soar, causing irreparable damage to the hardware components. This in turn would degrade the performance of the security server, if left unnoticed. To avoid such damage, administrators should monitor the fans regularly. The ESKM Fan Traps test helps the administrators in this regard!

This test intercepts the fan failure traps sent by the security server, extracts relevant information related to the failure from the traps, and reports the count of fan failure events to the eG manager. This information enables administrators to detect the fan failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A HP Enterprise Security Key Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Enterprise Security Key Manager that is to be monitored

Configurable parameters for the test

Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
Port	The port at which the specified HOST listens. By default, this is NULL.
Source Address	Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
OID Value	Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

In this case the oidvalue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2- Host_ system,Trap2:.1.3.6.1.4.1.9156.1.1.3- Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.

An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.

Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example

above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:

Trap5: .1.3.6.1.4.1.9156.1.1.5-any.

In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be:

Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any.

Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.

ShowOID Specifying True against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.

TrapOIDs By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.

DD Frequency Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against DD frequency.

To make diagnosis more efficient and accurate, the eG Enterprise suite

Detailed Diagnosis embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

- The eG manager license should allow the detailed diagnosis capability
- Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Fan failures	Indicates the number of times the fan failure event was triggered during the last measurement period.	Number	<p>The failure events may be generated due to the failure of fans of the security server. If the failure events are not rectified within a certain pre-defined timeperiod, the security server will be shutdown automatically.</p> <p>Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the security server.</p>

3.2.4 ESKM Memory Test

This test monitors the memory utilization of the HP Enterprise Security Key Manager (ESKM) security server and proactively alerts administrators to potential resource contention, if any.

Target of the test : A HP Enterprise Security Key Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Enterprise Security Key Manager that is to be monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SNMP Port	The port number through which the target router exposes its SNMP MIB; the default is 161.
SNMP Version	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMP version 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.
SNMP Community	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 SNMP version chosen is v3, then this parameter will not appear.
User Name	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 the username 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 this text box. By default, this parameter is set to none.
Auth Pass	Specify the password that corresponds to the above-mentioned user name. This parameter once again appears only if the snmpversion selected is v3.
Confirm Password	Confirm the authpass by retyping it here.
Auth Type	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

Parameters	Description
	<p>the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:</p> <ul style="list-style-type: none"> • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
Encrypt Flag	This flag appears only when v3 is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, this is set to no by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the yes option.
Encrypt Type	<p>If this is set to yes, then you will have to mention the encryption type by selecting an option from the encrypt type list. SNMP v3 supports the following encryption types:</p> <ul style="list-style-type: none"> • DES – Data Encryption Standard • AES – Advanced Encryption Standard
Encrypt Password	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
Total memory	Indicates the total amount of memory allocated for the security server.	MB	
Used memory	Indicates the amount of memory that is currently utilized by the security server.	MB	A value close to the <i>Total memory</i> measure indicates that the memory resources are depleting rapidly.

Measurement	Description	Measurement Unit	Interpretation
Free memory	Indicates the amount of memory that is currently available for use in the security server.	MB	A sudden decrease in this value could indicate an unexpected/sporadic spike in the memory utilization of the security server. A consistent decrease however could indicate a gradual, yet steady erosion of memory resources, and is hence a cause for concern.
Memory utilization	Indicates the percentage of memory that is utilized by the security server.	Percentage	If the value of this measure is close to 100%, it indicates that the memory utilization of the security server is at its peak. Therefore, the administrator may need to allocate additional memory resources to the security server.

3.2.5 ESKM PowerSupply Traps Test

Abnormal power fluctuation to the hardware components would often lead to the malfunctioning of the HP Enterprise Security Key manager (ESKM) which when left unnoticed can prove to be fatal! This test intercepts the traps sent by the security server, extracts information related to power supply failures from the traps, and reports the count of power failure occurrences to the eG manager. This information enables administrators to detect the abnormalities in the power supply if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A HP Enterprise Security Key Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Enterprise Security Key Manager that is to be monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
Port	The port at which the specified HOST listens. By default, this is NULL.

Parameters	Description
Source Address	Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
OID Value	Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

In this case the oidvalue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system, Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.

An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.

Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:

Trap5: .1.3.6.1.4.1.9156.1.1.5-any.

In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (.1.3.6.1.4.1.9156.1.1.4 and .1.3.6.1.4.1.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be:

Trap6: .1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.1.9156.1.1.5-any.

Parameters	Description
	Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.
ShowOID	Specifying True against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
TrapOIDs	By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against DD frequency.
Detailed Diagnosis	<p>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.</p> <p>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:</p> <ul style="list-style-type: none"> • 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
Power failures	Indicates the number of times the power failure event was triggered during	Number	The failure events may be generated due to the failure of the power supply units of the security server. If the

Measurement	Description	Measurement Unit	Interpretation
	the last measurement period.		<p>failure events are not rectified within a certain pre-defined timeperiod, the security server will be shutdown automatically.</p> <p>Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the security server.</p>

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.

Copyright © 2018 eG Innovations Inc. All rights reserved.

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.