eG Total Performance Visibility

Monitoring HP Enterprise Security Key Manager

Restricted Rights Legend

Trademarks

Copyright

Table of contents

Table of Figures

1

Introduction

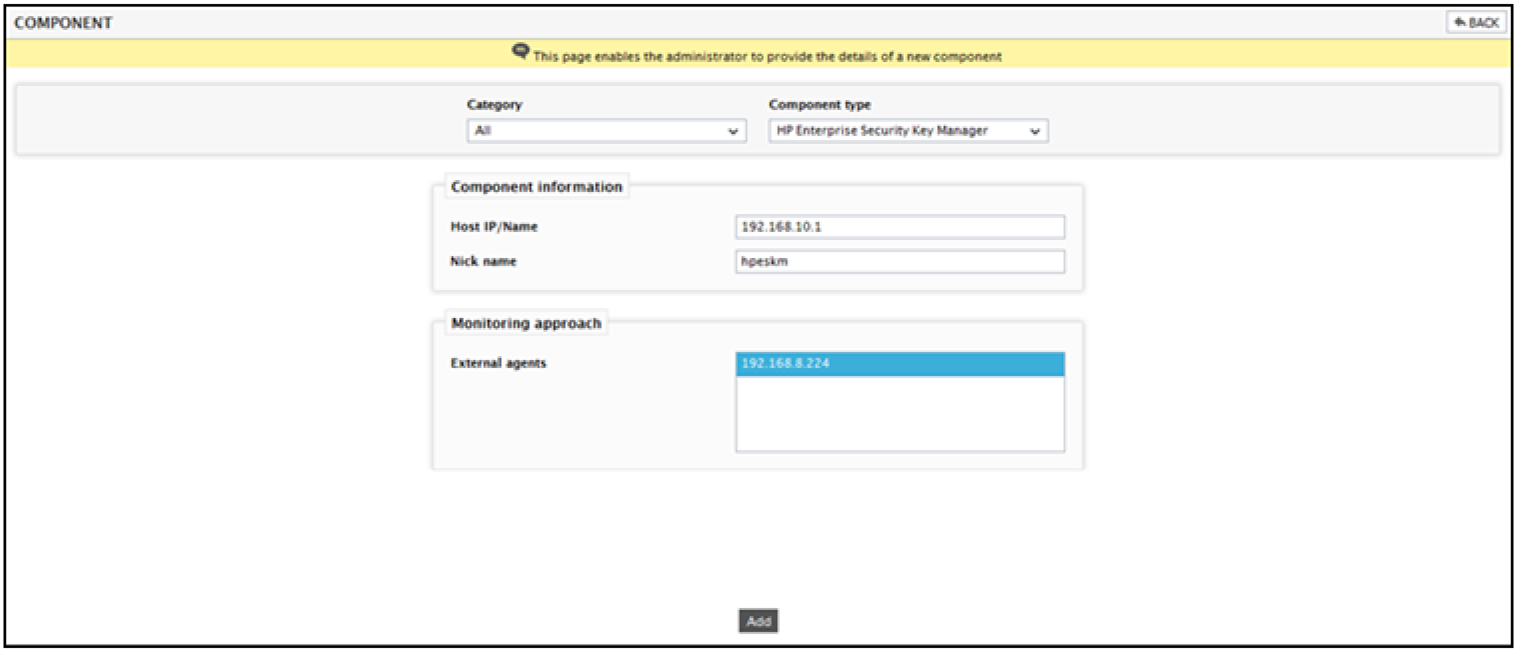
Encryption is the process of changing data into a form that cannot be read until it is deciphered with the key used to encrypt the data, protecting the data from unauthorized access and use. Encryption is primarily designed to protect the data once it is offline and to prevent it from being accessed 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 helps administrators to figure out how eG Enterprise helps in monitoring the HP Enterprise Secure Key Manager.

2

Administering the the eG Manager to monitor a HP Enterprise Security Key Manager (ESKM)

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) that appears when the Infrastructure -> Components -> Add/Modify menu sequence is followed. Remember that components manually added are managed automatically.



COMPONENT

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

Category: All

Component type: HP Enterprise Security Key Manager

Component information

Host IP/Name: 192.168.10.1

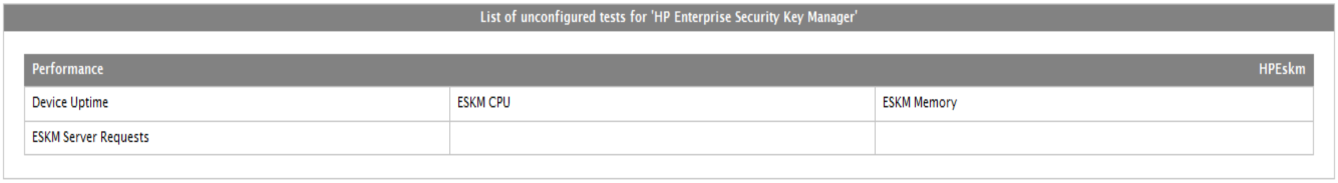
Nick name: hpeskm

Monitoring approach

External agents: 192.168.8.224

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 . 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, click here.
6. Finally, signout of the eG administrative interface.

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.

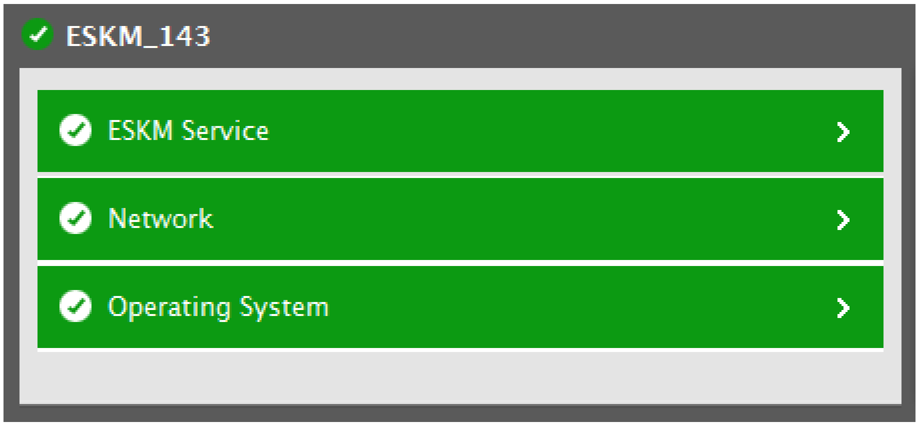


Figure 3.1: The layer model of the HP Enterprise Secure Key Manager

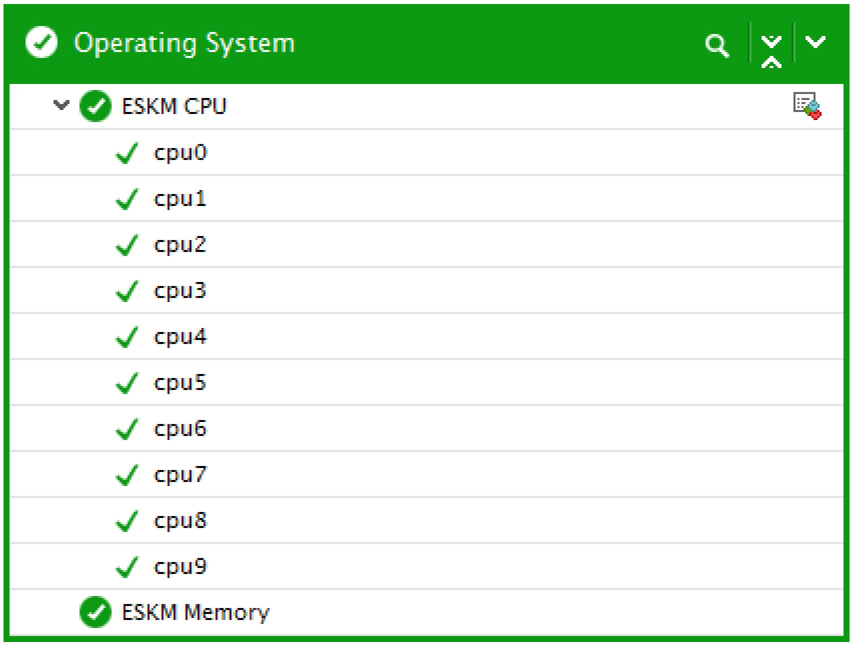
Every layer of Figure 1 is mapped to a variety of tests which connect to the SNMP MIBs of the target HP Enterprise Secure Key Manager to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- 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?

The sections to come will discuss each layer of Figure 1 in detail.

3.1 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.



Operating System

ESKM CPU

cpu0

cpu1

cpu2

cpu3

cpu4

cpu5

cpu6

cpu7

cpu8

cpu9

ESKM Memory

Figure 3.2: The tests associated with the Operating System layer

3.1.1 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 the target HP Enterprise Security Key Manager that is to be monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the target router exposes its SNMP MIB; the default is 161.

4. **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.
5. **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.
6. **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 the **USERNAME** parameter.
7. **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*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE** – If the **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
13. **ENCRYPTPASSWORD**– Specify the encryption password here.

14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **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 the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures 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. . .

3.1.2 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

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the target router exposes its SNMP MIB; the default is 161.
4. **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.

5. **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.
6. **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 the **USERNAME** parameter.
7. **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*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE** – If the **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
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.

15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **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 the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures 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 *Total memory* measure indicates that the memory resources are depleting rapidly.
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 utlization of the security server is at its peak. Therefore, the administrator may need to allocate additional memory resources to the security server.

3.1.3 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

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PORT** – The port at which the specified **HOST** listens. By default, this is *NULL*.
4. **SOURCEADDRESS**– 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.
5. **OIDVALUE** – 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 **HOST** 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.

6. **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.
7. **TRAPOIDS**– By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified **SOURCEADDRESS**es. 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.
8. **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**.
9. **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.

Measures 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	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

Measurement	Description	Measurement Unit	Interpretation
			timeperiod, the security server will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the security server.

3.1.4 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, the administrators should monitor the fans regularly. The ESKMFanTrap 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

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PORT** – The port at which the specified **HOST** listens. By default, this is *NULL*.
4. **SOURCEADDRESS**– 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.
5. **OIDVALUE** – 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 **HOST** 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.

6. **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.

7. **TRAPOIDS**– By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified **SOURCEADDRESS**es. 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.

8. **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**.

9. **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.

Measures 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	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. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the security server.

3.1.5 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

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PORT** – The port at which the specified **HOST** listens. By default, this is *NULL*.
4. **SOURCEADDRESS**– 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.
5. **OIDVALUE** – 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 **HOST** 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.

6. **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.

7. **TRAPOIDS**– By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified **SOURCEADDRESS**es. 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.
8. **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**.
9. **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:

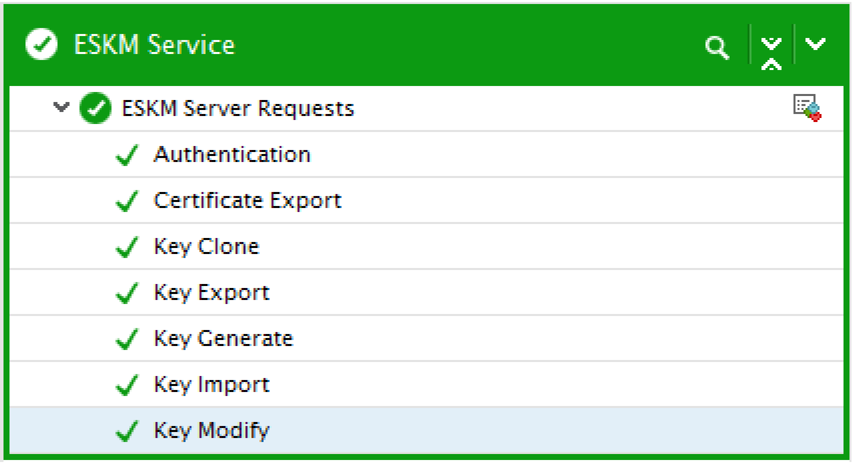
   - The eG manager license should allow the detailed diagnosis capability
   - Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measures made by the test:

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

3.2 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.



ESKM Service

ESKM Server Requests

✓ Authentication

✓ Certificate Export

✓ Key Clone

✓ Key Export

✓ Key Generate

✓ Key Import

✓ Key Modify

Figure 3.3: The tests associated with the ESKM Service layer

3.2.1 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 adminstrator 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 appliance.

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

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the target router exposes its SNMP MIB; the default is 161.
4. **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.
5. **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.
6. **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 the **USERNAME** parameter.
7. **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*.

8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE** – If the **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
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **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 the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures 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	Number	A high value is desired for this measure.

Measurement	Description	Measurement Unit	Interpretation
	that were processed successfully.		
Failed requests:	Indicates the number of server requests of this type that failed.	Number	Ideally, the value of this measure should be zero.

4

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **HP Enterprise Security Key Manager**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.