Monitoring Hitachi Compute Blade

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Hitachi Compute Blade 500 is an enterprise-class blade server platform that extends high-performance, high-density blade computing and virtualization benefits to new areas of the data center. Hitachi Compute Blade 500 with logical partitioning (LPAR) combines all the benefits of virtualization with all the advantages of the blade server format: simplicity, flexibility, high compute density and power efficiency. This combination allows organizations to consolidate more resources, extend the benefits of virtualization solutions (VMware, Microsoft® Hyper-V® and so forth) to more areas of the enterprise data center, and cut costs without sacrificing performance.

The Hitachi Compute Blade comprises of the following:

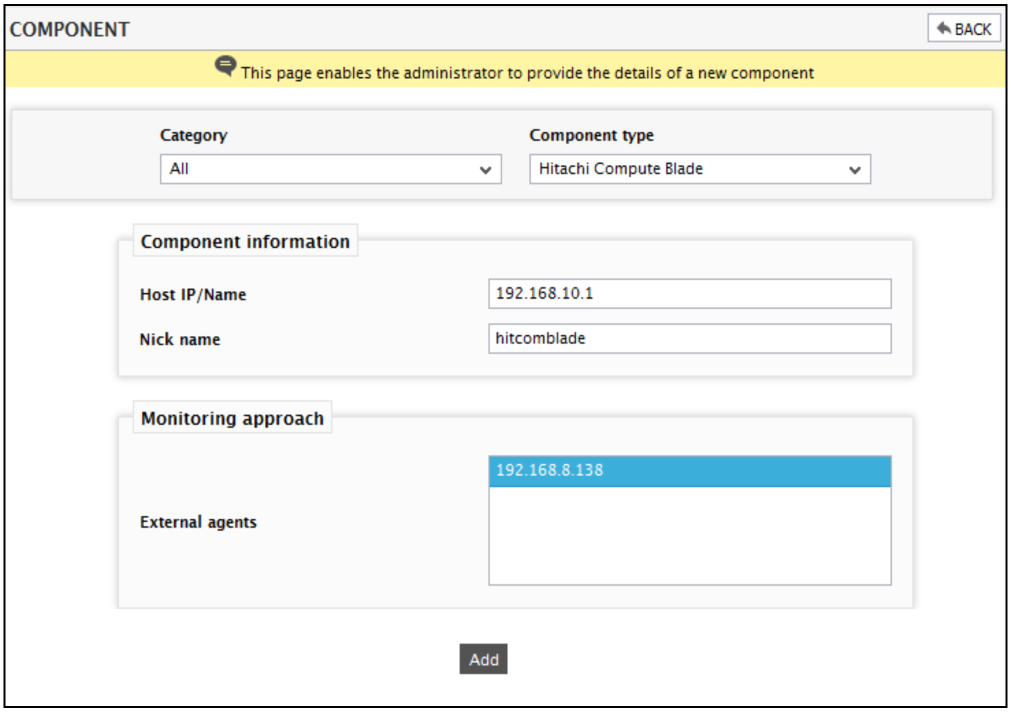
- Server Chassis (enclosure)
- Server Blades
- HDD slot, order of installation, and indicators
- Management Modules
- Switch Modules
- Power Supply Modules and
- Fan Modules

To ensure the high uptime of the blades and the virtualization benefits it provides, it is essential to periodically monitor the individual components of the Hitachi Compute Blade and ensure the health of the hardware components. eG Enterprise helps administrators to monitor the Hitachi Compute Blade and prompt them to abnormalities. The chapters discussed below helps administrators to figure out how eG Enterprise helps in monitoring the Hitachi Compute Blade.

Chapter 2: Administering the eG Manager to monitor a Hitachi Compute Blade

1. Log into the eG administrative interface.

2. eG Enterprise cannot automatically discover the Hitachi Compute Blade. You need to manually add the server using the **COMPONENTS** page (see Figure 2.1) 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: Hitachi Compute Blade

Component information

Host IP/Name: 192.168.10.1

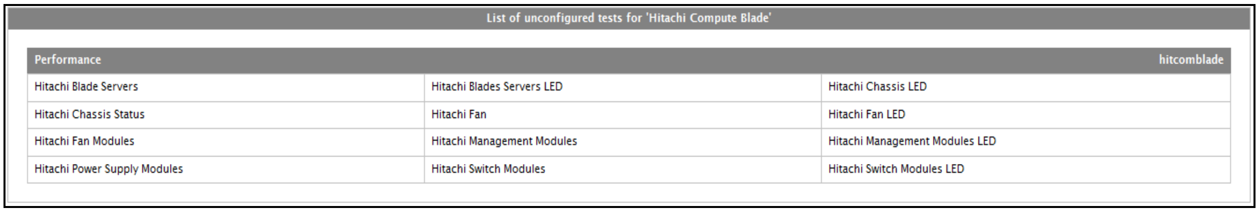
Nick name: hitcomblade

Monitoring approach

External agents: 192.168.8.138

Figure 2.1: Adding the Hitachi Compute Blade

3. When you attempt to sign out, a list of unconfigured tests appears.



List of unconfigured tests for 'Hitachi Compute Blade'

Performance		hitcomblade
Hitachi Blade Servers	Hitachi Blades Servers LED	Hitachi Chassis LED
Hitachi Chassis Status	Hitachi Fan	Hitachi Fan LED
Hitachi Fan Modules	Hitachi Management Modules	Hitachi Management Modules LED
Hitachi Power Supply Modules	Hitachi Switch Modules	Hitachi Switch Modules LED

Figure 2.2: List of tests to be configured for Hitachi Compute Blade

4. Click on the **Hitachi Blade Servers** test to configure it. To know how to configure the test, click here. All other tests will be configured automatically.

5. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the Hitachi Compute Blade

eG Enterprise offers a specialized Hitachi Compute Blade monitoring model that monitors the core hardware components of the Hitachi Compute Blade, and proactively alerts administrators to issues in its overall health and performance, so that abnormalities can be fixed before irreparable damage occurs.

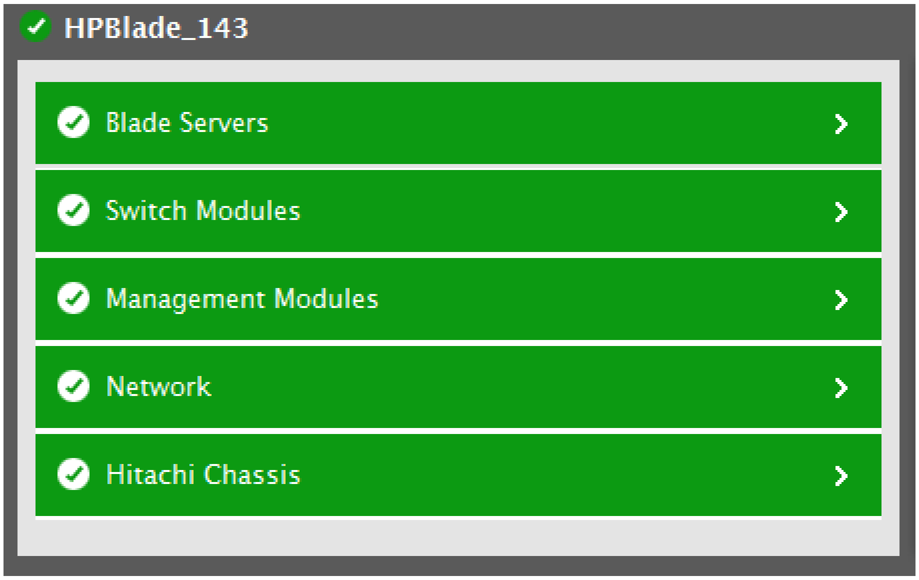


Figure 3.1: The layer model of the Hitachi Compute Blade

By continuously monitoring the Hitachi Compute Blade, administrators can answer the following performance questions:

- What is the current status and color of each LED available in each Switch Module?
- What is the health and power supply status of each Switch Module?
- Is any Switch Module under maintenance mode?
- What is the current health and power supply status of each Power Supply Module?
- What is the current health and power supply status of each Management Module?
- Is any Management Module under maintenance mode?
- What is the current status and color of each LED available in each Management Module?
- What is the current status and color of the LED available in each Fan Module?
- What is the current health and power supply status of each Fan Module?
- Is any Fan Module under maintenance mode?

- What is the current speed of each fan in each Fan Module?
- What is the current voltage of the chassis?
- What is the current temperature of the chassis?
- What is the power consumed by the chassis?
- What is the power supply status of the chassis?
- What is the current status and color of each LED available in the chassis?
- What is the current health, power supply status and temperature of each blade server?
- Is the blade server in maintenance mode?
- In a redundant configuration, is the blade server a primary blade?
- What is the current status and color of each LED in the blade server?

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 Hitachi Chassis layer

By continuously monitoring the chassis of the target Hitachi Compute Blade, administrators can figure out the following:

The health and power supply status of the chassis;

The status and color of each LED in the chassis;

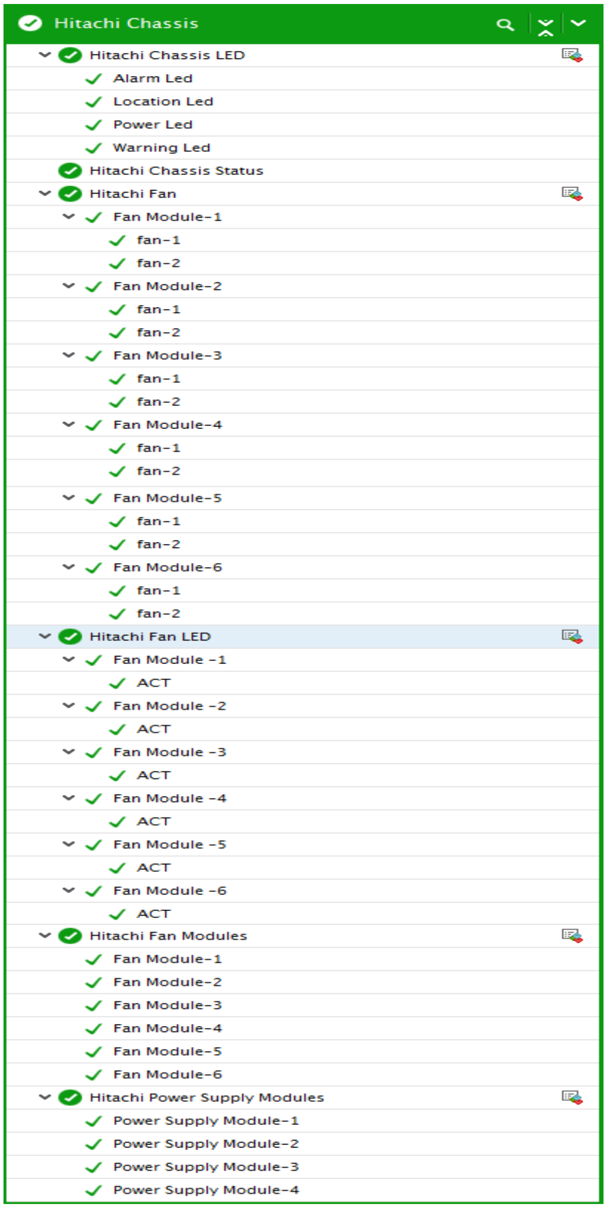
The health and power supply status of each Power Supply Module;

The health and power supply status of each Fan in the Fan Module;

The speed of each fan;

The status and color of the LED in each Fan Module;

Using this layer, administrators can be proactively alerted to defects in the chassis of the target Hitachi Compute Blade.



Hitachi Chassis

- Hitachi Chassis LED
  - Alarm Led
  - Location Led
  - Power Led
  - Warning Led
- Hitachi Chassis Status
- Hitachi Fan
  - Fan Module-1
    - fan-1
    - fan-2
  - Fan Module-2
    - fan-1
    - fan-2
  - Fan Module-3
    - fan-1
    - fan-2
  - Fan Module-4
    - fan-1
    - fan-2
  - Fan Module-5
    - fan-1
    - fan-2
  - Fan Module-6
    - fan-1
    - fan-2
- Hitachi Fan LED
  - Fan Module -1
    - ACT
  - Fan Module -2
    - ACT
  - Fan Module -3
    - ACT
  - Fan Module -4
    - ACT
  - Fan Module -5
    - ACT
  - Fan Module -6
    - ACT
- Hitachi Fan Modules
  - Fan Module-1
  - Fan Module-2
  - Fan Module-3
  - Fan Module-4
  - Fan Module-5
  - Fan Module-6
- Hitachi Power Supply Modules
  - Power Supply Module-1
  - Power Supply Module-2
  - Power Supply Module-3
  - Power Supply Module-4

Figure 3.2: The tests associated with the Hitachi Chassis layer

The sections that follow will discuss each test associated with this layer in great detail.

3.1.1 Hitachi Chassis Status Test

The Hitachi Compute Blade consists of a robust, fully-redundant 6U chassis i.e. 19-inch rack compatible. The chassis can house up to eight multi-core 2-socket processor half-wide blades or four multi-core 4-socket processor full-wide blades. The chassis is provided with hot-swappable management modules, switch modules, power supply modules and fan modules. These modules provide continuous management, network connectivity, power supply and cooling services to the blades.

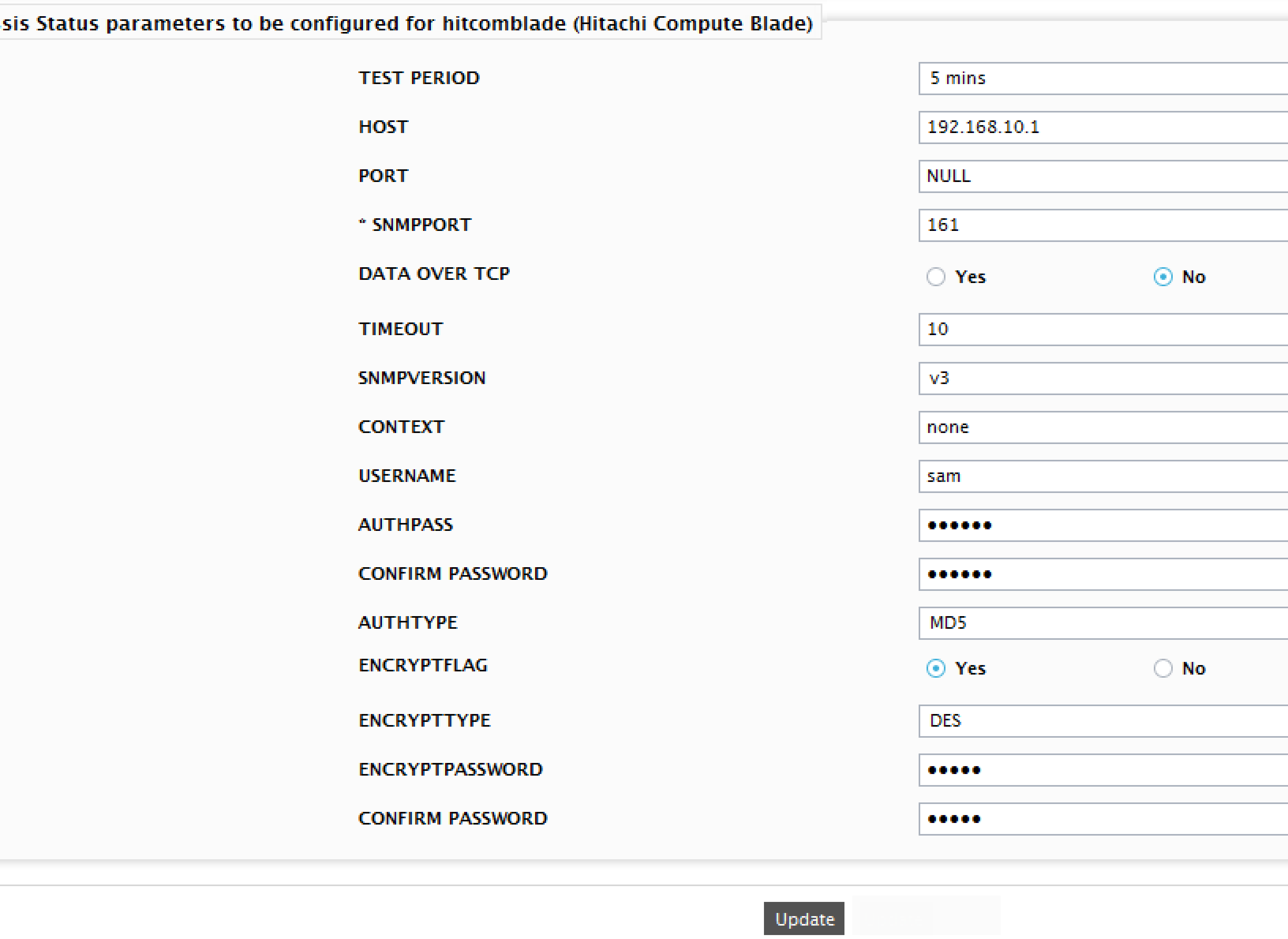
Built-in logical partitioning, a key feature of Hitachi Compute Blade 500 complements existing software-based virtualization solutions and can be used in conjunction with VMware, Hyper-V or Red Hat KVM. These multiple virtualization platforms can be combined in a single chassis and can be configured to share the same physical resources. For these virtualization platforms to function without a glitch, it is essential that the chassis on which the physical resources are available should be operational round the clock. Frequent power failures, voltage and temperature fluctuations may damage the chassis resulting in the failure of the virtual platforms. Therefore, it is mandatory for the administrators to keep a constant vigil on the power supply, voltage and temperature of the chassis. This is exactly where the **Hitachi Chassis Status** test helps!

Using this test, administrators can determine the current power supply status of the chassis, the current temperature and voltage of the chassis as well as be proactively alerted if the chassis is under maintenance! This way, administrators can be alerted to abnormalities in the temperature and voltage of the chassis and rectify the same before end users utilizing the virtualized solutions provisioned from the Hitachi Compute Blade are not put into terrible hardship!

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for the chassis on the Hitachi Compute Blade being monitored



sis Status parameters to be configured for hitcomblade (Hitachi Compute Blade)

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

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The IP address of the Hitachi Compute Blade.
3. **SNMPPORT** – The port at which the Hitachi Compute Blade 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**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>PowerSupply status</td><td>Indicates the power supply status of the chassis.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>PowerOff</td><td>1</td></tr>
<tr><td>Standby</td><td>2</td></tr>
<tr><td>PowerOn</td><td>3</td></tr>
<tr><td>Unknown</td><td>4</td></tr>
<tr><td>PowerOn</td><td>5</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Executing</td><td></td></tr><tr><td>PowerOff Executing</td><td>6</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b> s mentioned above while indicating the power status of the chassis. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Current voltage</td><td>Indicates the current voltage of the chassis.</td><td>Volts</td><td>A sudden / gradual rise in the value of this measure is a cause of concern.</td></tr>
<tr><td>Power consumption</td><td>Indicates the amount of power consumed by the chassis.</td><td>Amps</td><td></td></tr>
<tr><td>Temperature</td><td>Indicates the current temperature status of the chassis.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Normal</td><td>1</td></tr><tr><td>Higher Warning</td><td>2</td></tr><tr><td>Higher Error</td><td>3</td></tr><tr><td>Lower Warning</td><td>4</td></tr><tr><td>Lower Unknown</td><td>5</td></tr></table>
<b>Note:</b></td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>By default, this measure can report the <b>Measure Value</b> s mentioned above while indicating the current temperature status of the chassis. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Maintenance mode</td><td>Indicates the current maintenance mode of the chassis.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>CE Maintenance Mode</td><td>2</td></tr>
<tr><td>User Maintenance Mode</td><td>3</td></tr>
<tr><td>Unknown</td><td>4</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b> s mentioned above while indicating the current maintenance mode of the chassis. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.1.2 Hitachi Chassis LED Test

If multiple virtualization platforms are combined in a single chassis of the Hitachi Compute Blade and are configured to share the same physical resources, then it is the onus of the administrators to keep a constant vigil on the chassis! For easy identification of problem scenarios, the chassis is provided with the following LEDs:

- Power LED
- Alarm LED
- Attention LED
- Location identify LED

If the LEDs fail or if the LEDs are damaged, then, administrators may be deprived of identifying the problems that occur on the chassis. To avoid this issue, it is necessary to figure out the fauly LEDs and replace them at the earliest. The **Hitachi Chassis LED** test aids administrators in this exercise by constantly keeping a vigil on the status of the LEDs and the color of the LEDs.

This test reports the current status and color of each LED available in the server chassis.

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for each LED in the chassis being monitored.

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The IP address of the Hitachi Compute Blade.
3. **SNMPPORT** – The port at which the Hitachi Compute Blade 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**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>LED status</td><td>Indicates the current status of this LED.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Turn Off</td><td>1</td></tr>
<tr><td>Turn On</td><td>2</td></tr>
<tr><td>Unknown</td><td>3</td></tr>
<tr><td>Blink</td><td>4</td></tr>
<tr><td>Blink Fast</td><td>5</td></tr>
<tr><td>Blink Slow</td><td>6</td></tr>
</table>

Note:
By default, this measure can report the **Measure Value** s mentioned above while indicating the status of this LED on the chassis. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>LED color</td><td>Indicates the color of this LED.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Color</th><th>Numeric Value</th></tr>
<tr><td>Blue</td><td>1</td></tr>
<tr><td>Green</td><td>2</td></tr>
<tr><td>Red</td><td>3</td></tr>
<tr><td>Amber</td><td>4</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Color</b>s mentioned above while indicating the color of this LED on the chassis. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.1.3 Hitachi Fan Modules Test

The cooling of the Hitachi Compute Blade is governed by six efficient, variable-speed, redundant fan modules. Each fan module includes three fans to tolerate fan failures within a module; an entire module can fail while the other fan modules continue to support the cooling requirements of the chassis. If the fan modules fail frequently, then the cooling of the hardware components of the Hitachi Compute Blade may fluctuate leading to abnormal rise in temperature. This may sometimes cause a permanent damage of the Hitachi Compute Blade. To avoid such critical damage, administrators should constantly monitor the health of the fan modules. The **Hitachi Fan Modules** test comes in handy to those administrators who would like to monitor the fan modules round the clock!

This test reports the current health of each fan module in the chassis, thus turning the spotlight on those modules that have failed. In addition, the test also checks the status of the power supply to each fan module and also alerts administrators to the redundancy status of each fan module.

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan module in the Hitachi Compute Blade being monitored.

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST –** The IP address of the Hitachi Compute Blade.
3. **SNMPPORT –** The port at which the Hitachi Compute Blade 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**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Health status</td><td>Indicates the current health of this fan module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Failed</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the health of each fan module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>PowerSupply status</td><td>Indicates the current power supply status of this fan module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>PowerOff</td><td>1</td></tr>
<tr><td>Standby</td><td>2</td></tr>
<tr><td>PowerOn</td><td>3</td></tr>
<tr><td>Unknown</td><td>4</td></tr>
<tr><td>PowerOn Executing</td><td>5</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>PowerOff Executing</td><td>6</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the current power supply status of each fan module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Redundancy status</td><td>Indicates the current redundancy status of this fan module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Mode</th><th>Numeric Value</th></tr><tr><td>Redundancy</td><td>1</td></tr><tr><td>Non Redundancy</td><td>2</td></tr><tr><td>Unknown</td><td>3</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>Mode</b>s mentioned above while indicating the redundancy status of each fan module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.1.4 Hitachi Fan Test

For every fan in the fan module, this test reports the current speed of the fan. Using this test, administrators can figure out the fans that do not operate within the admissible range and replace the same to maintain smooth operation of the target Hitachi Compute Blade.

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for the *Fan module:Fan* pair on the Hitachi Compute Blade being monitored.

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The IP address of the Hitachi Compute Blade.
3. **SNMPPORT** – The port at which the Hitachi Compute Blade 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**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Fan speed:	Indicates the current fan speed of this fan module.	Rpm	Ideally, the speed of the fan should be within the admissible range mentioned in the specification of the target Hitachi Compute Blade.

3.1.5 Hitachi Fan LED Test

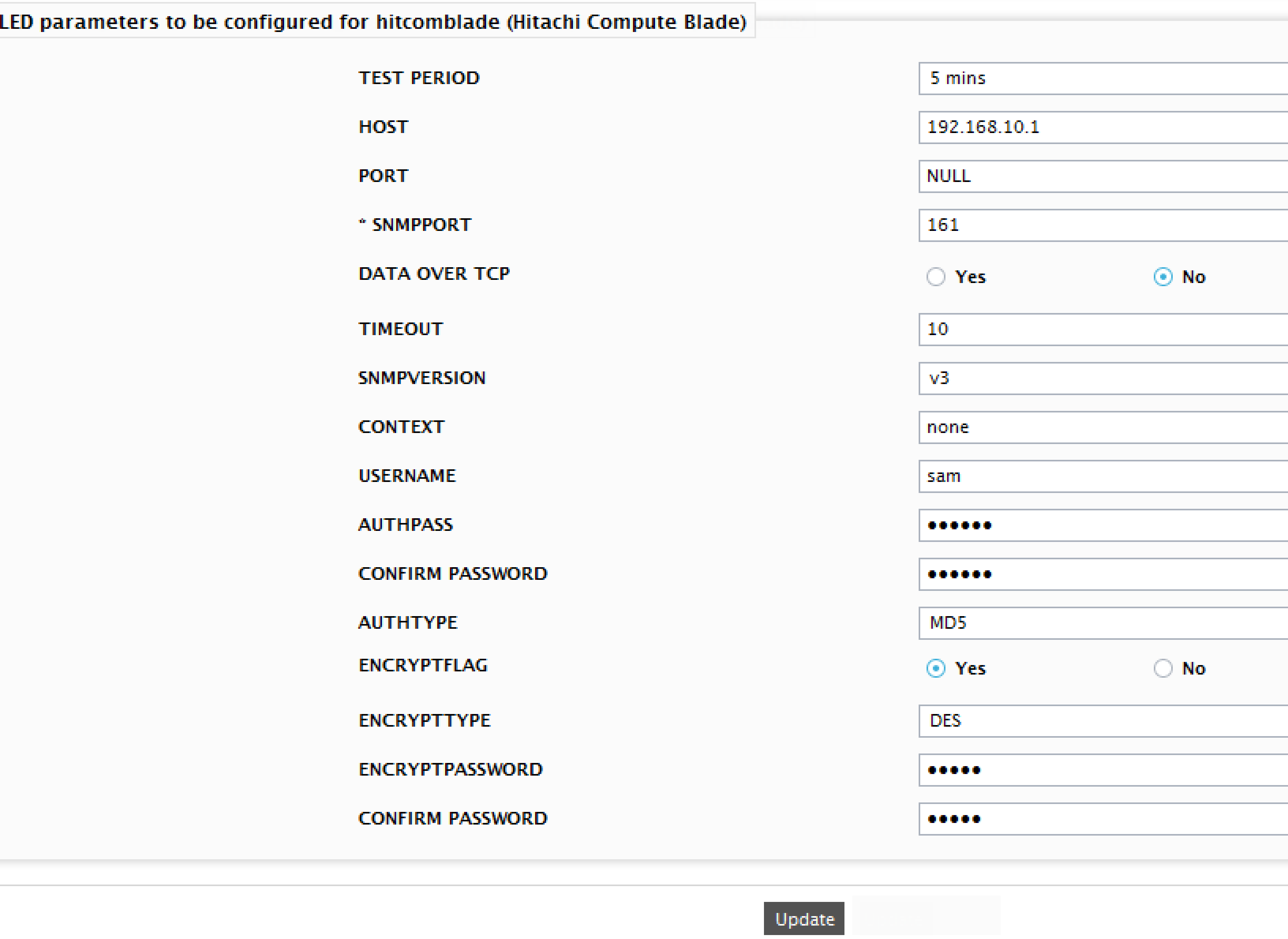
Each fan module of the Hitachi Compute Blade comprises of a LED which indicates the administrators at a single glance about the current status of the fan module. If thecolor of the LED is green, then the administrators can identify that the fan module is in normal condition. If the color of the LED is Amber, then the administrators can be notified of the failure of the fan module. If the LED is faulty, administrators cannot view the failure of the fan modules instantly. Therefore, it is essential to replace the faulty LEDs so that the failure of the fan modules can be identified easily. The **Hitachi Fan LED** test helps administrators to figure out the faulty LEDs by monitoring the status of the LED available in each fan module and the color of the LED in each fan module!

This test helps administrators to monitor the current status of the LED available in each fan module and the color of the LED. This way, administrators can easily figure out the faulty LEDs and replace them at the earliest!

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for the *Fan module:LED* pair on the Hitachi Compute Blade being monitored.



LED parameters to be configured for hitcomblade (Hitachi Compute Blade)

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

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The IP address of the Hitachi Compute Blade.
3. **SNMPPORT** – The port at which the Hitachi Compute Blade 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**.

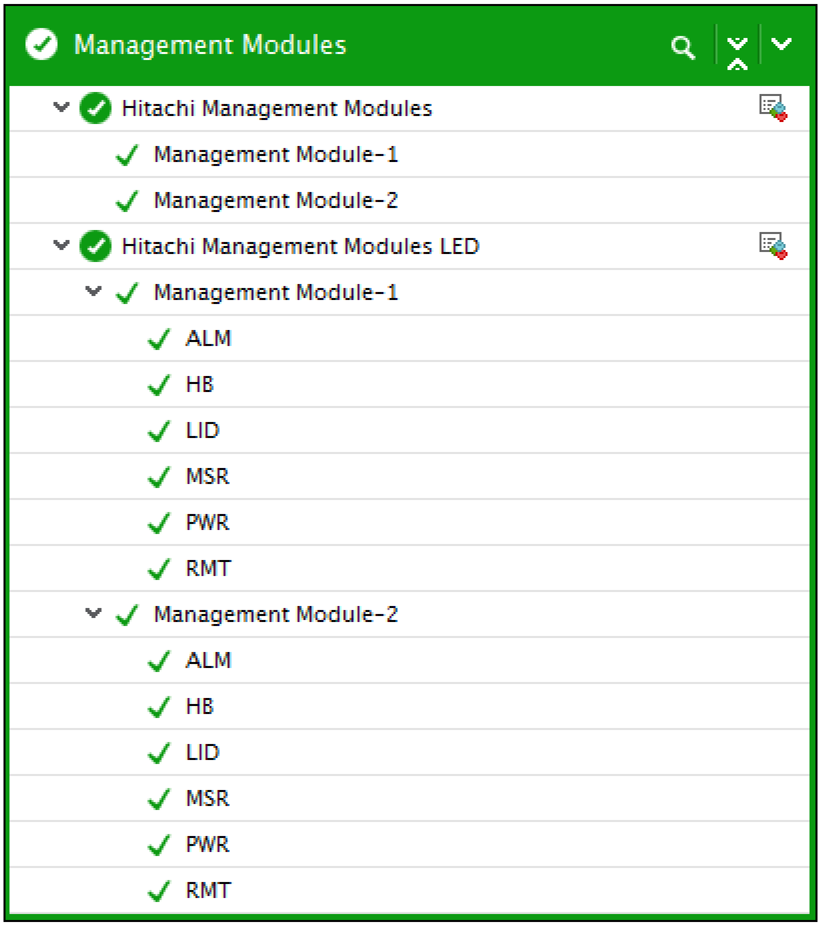
Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>LED status:</td><td>Indicates the current status of this LED.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Turn Off</td><td>1</td></tr>
<tr><td>Turn On</td><td>2</td></tr>
<tr><td>Unknown</td><td>3</td></tr>
<tr><td>Blink</td><td>4</td></tr>
<tr><td>Blink Fast</td><td>5</td></tr>
<tr><td>Blink Slow</td><td>6</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the status of the LED in the fan module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>LED color:</td><td>Indicates the color emitted by this LED.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Color</th><th>Numeric Value</th></tr><tr><td>Blue</td><td>1</td></tr><tr><td>Green</td><td>2</td></tr><tr><td>Red</td><td>3</td></tr><tr><td>Amber</td><td>4</td></tr><tr><td>Unknown</td><td>0</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>Color</b>s mentioned above while indicating the color of the LED in the fan module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.2 The Management Modules layer

Using this layer, the administrators can easily detect the abnormalities in the management modules by continuously monitoring the health and power supply status of each management module. In addition, administrators can also be alerted towards the faulty LEDs that needs immediate replacement.



Management Modules

- Hitachi Management Modules
  - Management Module-1
  - Management Module-2
- Hitachi Management Modules LED
  - Management Module-1
    - ALM
    - HB
    - LID
    - MSR
    - PWR
    - RMT
  - Management Module-2
    - ALM
    - HB
    - LID
    - MSR
    - PWR
    - RMT

Figure 3.3: The tests associated with the Management Modules layer

The sections that follow will discuss each test associated with this layer in great detail.

3.2.1 Hitachi Management Modules Test

The management module provides power control of the modules, status monitoring, system console, and management network functions. One (standard) or two (maximum) management modules can be mounted in the server chassis of the Hitachi Compute Blade. With two management modules installed, the modules provide a redundant configuration. Each module is hot-swappable and supports live firmware updates without the need for shutting down the blades. Each module supports an independent management LAN interface from the data network for remote and secure management of the chassis and all blades. Each module supports a serial CLI and a Web interface. The management modules also support SNMP and email alert notification so that administrators are always notified of any issues. If the management modules fail to function, then the target Hitachi Compute Blade may malfunction resulting in the failure of several hardware and software components interconnected with the blade. To avoid such fatal failures, administrators should constantly maintain a vigil over the management modules. The **Hitachi management Modules** test helps administrators in this regard!

For each management module in the chassis of the target Hitachi Compute Blade, this test reports the current health and power supply status. In addition, this test also reports the operational status as well as the maintenance mode of each management module. Using this test, administrators can easily figure out abnormalities in the management module and take necessary measures to combat the abnormalities at the earliest!

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for each management module in the Hitachi Compute Blade being monitored.

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The IP address of the Hitachi Compute Blade
3. **SNMPPORT** – The port at which the Hitachi Compute Blade 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**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Health status</td><td>Indicates the current health of this management module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Normal</td><td>1</td></tr><tr><td>Failed</td><td>2</td></tr><tr><td>Unknown</td><td>0</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b> s mentioned above while indicating the health of each management module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>PowerSupply status</td><td>Indicates the current power supply status of this management module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>PowerOff</td><td>1</td></tr>
<tr><td>Standby</td><td>2</td></tr>
<tr><td>PowerOn</td><td>3</td></tr>
<tr><td>Unknown</td><td>4</td></tr>
<tr><td>PowerOn Executing</td><td>5</td></tr>
<tr><td>PowerOff Executing</td><td>6</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the current power supply status of each management module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Operation mode</td><td>Indicates the current operation mode of this management module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Mode</th><th>Numeric Value</th></tr>
<tr><td>Active</td><td>1</td></tr>
<tr><td>Standby</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure can report</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>the <b>Mode</b>s mentioned above while indicating the current operation mode of the management module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Maintenance mode</td><td>Indicates the current maintenance mode of this switch module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>CE Maintenance Mode</td><td>2</td></tr>
<tr><td>User Maintenance Mode</td><td>3</td></tr>
<tr><td>Unknown</td><td>4</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the current maintenance mode of the management module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.2.2 Hitachi Management Modules LED Test

Each management module of the target Hitachi Compute Blade is provided with a set of LEDs to visually notify the administrators on the functioning of the management module. The following LEDs are available in each management module:

- Heartbeat LED flashes green light when the management module works normally
- Power LED notifies power-on and power-off status of the management module
- Identify LED is manually turned on by the administrators for visually locating the management module
- Alarm LED flashes red light when the errors or redundant failures occur
- Primary LED indicates whether/not the management module is currently active
- Remote LED indicates whether/not the management module is accessed remotely

With the help of these LEDs, administrators can easily figure out the health and working mode of the management module at a single glance. If the LEDs fail, administrators may not be notified to critical issues of the management module. This may result in the failure of the management module and if left unattended may cause irreparable damage to the target Hitachi Compute Blade. Therefore, it is imperative to replace the faulty LEDs. The **Hitachi Management Modules LED** test aids administrators to monitor the status of the LEDs and figure out the LEDs that are faulty.

This test auto-discovers each LED in the management module, and reveals the current status of the LED and color of the LED.

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for the *Management module:LED* pair on the Hitachi Compute Blade being monitored.

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The IP address of the Hitachi Compute Blade.
3. **SNMPPORT –** The port at which the Hitachi Compute Blade 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**.

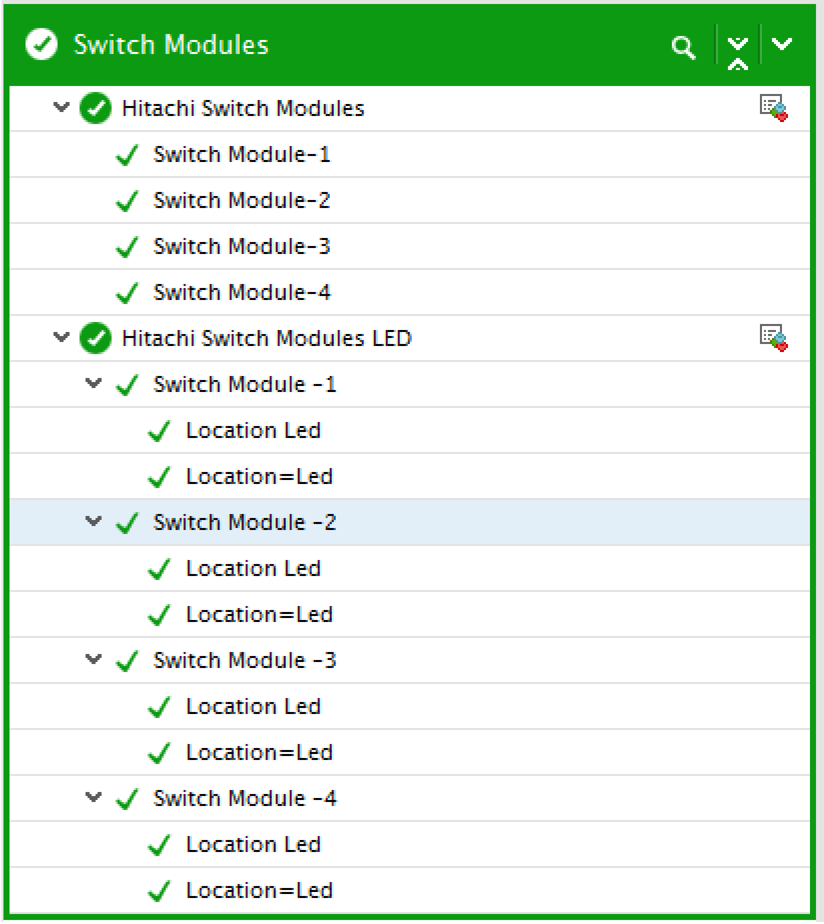
Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>LED status</td><td>Indicates the current status of this LED.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Turn Off</td><td>1</td></tr>
<tr><td>Turn On</td><td>2</td></tr>
<tr><td>Unknown</td><td>3</td></tr>
<tr><td>Blink</td><td>4</td></tr>
<tr><td>Blink Fast</td><td>5</td></tr>
<tr><td>Blink Slow</td><td>6</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the current</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>status of each LED on the management module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>LED color</td><td>Indicates the color emitted by this LED.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Color</th><th>Numeric Value</th></tr>
<tr><td>Blue</td><td>1</td></tr>
<tr><td>Green</td><td>2</td></tr>
<tr><td>Red</td><td>3</td></tr>
<tr><td>Amber</td><td>4</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Color</b>s mentioned above while indicating the color of this LED. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.3 The Switch Modules layer

Using this layer, administrators can instantly detect abnormalities in the Switch Modules of the Hitachi Compute Blade by continuously monitoring the power supply status and health. This layer also helps administrators to replace the LEDs of the Switch Modules that are faulty.



Switch Modules

- Hitachi Switch Modules
  - ✓ Switch Module-1
  - ✓ Switch Module-2
  - ✓ Switch Module-3
  - ✓ Switch Module-4
- Hitachi Switch Modules LED
  - ✓ Switch Module -1
    - ✓ Location Led
    - ✓ Location=Led
  - ✓ Switch Module -2
    - ✓ Location Led
    - ✓ Location=Led
  - ✓ Switch Module -3
    - ✓ Location Led
    - ✓ Location=Led
  - ✓ Switch Module -4
    - ✓ Location Led
    - ✓ Location=Led

Figure 3.4: The tests associated with the Switch Modules layer

The tests associated with this layer are discussed in the forthcoming sections.

3.4 Hitachi Switch Modules Test

The Hitachi Compute Blade is designed to contain upto 4 high-throughput flexible IO switch modules. The backplane within the server chassis of the target Hitachi Compute Blade interconnects the switch module to the server blades. Each server blade connects to the backplane and thus to the switch modules through an onboard CNA or Mezzanine cards on the server blade. All external ports of a switch module are available even if only one server blade is installed. These switch modules enable the Hitachi Compute Blade to support flexible connectivity for cloud architectures including loseless Ethernet fabrics. If any of these switch modules fail or if these switch modules are under maintenance for a longer duration, then, the switch modules may not be available for use resulting in connectivity failure among the blades. To prevent such failures, administrators should monitor the switch modules round the clock. The **Hitachi Switch Modules** test helps administrators in this regard!

This test auto-discovers the switch modules within the chassis of the target Hitachi Compute Blade, and reports the current health and power supply status of each switch module. In addition, this test also reveals the switch modules that are currently undermaintenance.

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for each switch module on the Hitachi Compute Blade being monitored.

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The IP address of the Hitachi Compute Blade
3. **SNMPPORT** – The port at which the Hitachi Compute Blade 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**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Health status</td><td>Indicates the current health of this switch module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Failed</td><td>2</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b> s mentioned above while indicating the health of each switch module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>PowerSupply status</td><td>Indicates the current power supply status of this switch module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>PowerOff</td><td>1</td></tr>
<tr><td>Standby</td><td>2</td></tr>
<tr><td>PowerOn</td><td>3</td></tr>
<tr><td>Unknown</td><td>4</td></tr>
<tr><td>PowerOn</td><td>5</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Executing</td><td></td></tr><tr><td>PowerOff Executing</td><td>6</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b> s mentioned above while indicating the current power supply status of each switch module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Maintenance mode</td><td>Indicates the current maintenance mode of this switch module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Normal</td><td>1</td></tr><tr><td>CE Maintenance Mode</td><td>2</td></tr><tr><td>User Maintenance Mode</td><td>3</td></tr><tr><td>Unknown</td><td>4</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b> s mentioned above while indicating the current maintenance mode of the switch module. However, the graph of this</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			measure is indicated using the numeric equivalents.

3.4.1 Hitachi Switch Modules LED Test

Each switch module of the target Hitachi Compute Blade contains a set of LEDs using which the administrator can easily identify the health of the switch module. If the LEDs are found to be faulty or is damaged, then problematic switch modules may not be identified instantly which may sometimes lead to malfunctioning of the target Hitachi Compute Blade and its corresponding business services. In order to avoid such issues, it is necessary for the administrators to replace the faulty LEDs at the earliest. This is where the **Hitachi Switch Modules LED** test helps!

Using this test, administrators can determine the current status of each LED on the switch module and color of each LED. This way, administrators may be alerted to failure of the LEDs and help them replace the LEDs immediately.

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Switch Module:LED* pair on the Hitachi Compute Blade being monitored.

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The IP address of the Hitachi Compute Blade
3. **SNMPPORT** – The port at which the Hitachi Compute Blade 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**.

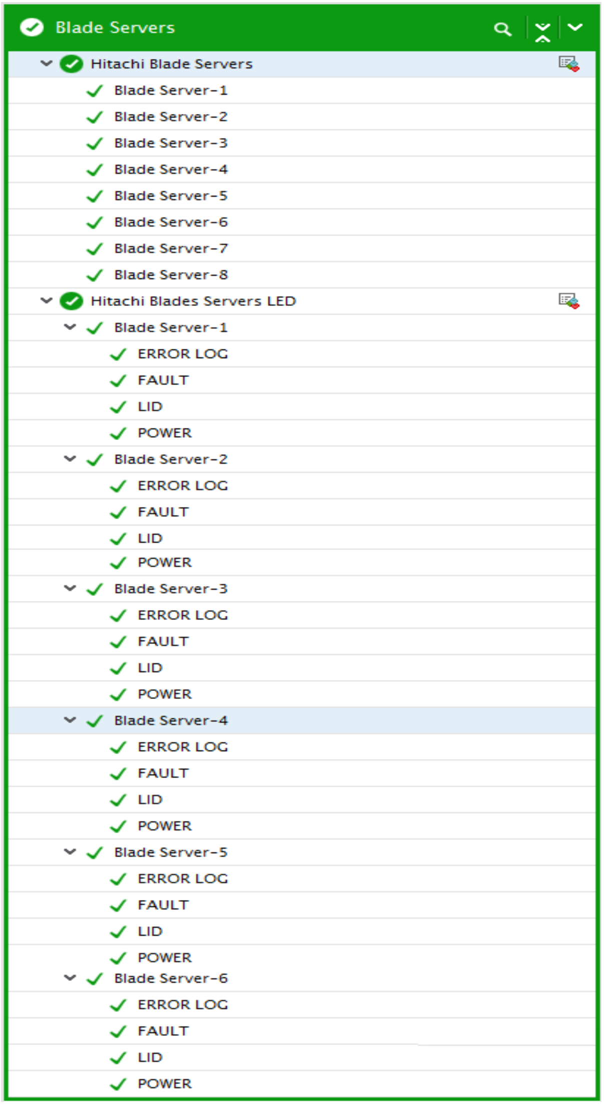
Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>LED status:</td><td>Indicates the current status of this LED.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Turn Off</td><td>1</td></tr>
<tr><td>Turn On</td><td>2</td></tr>
<tr><td>Unknown</td><td>3</td></tr>
<tr><td>Blink</td><td>4</td></tr>
<tr><td>Blink Fast</td><td>5</td></tr>
<tr><td>Blink Slow</td><td>6</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the current</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>status of each LED in the switch module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>LED color:</td><td>Indicates the color emitted by this LED.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Color</th><th>Numeric Value</th></tr>
<tr><td>Blue</td><td>1</td></tr>
<tr><td>Green</td><td>2</td></tr>
<tr><td>Red</td><td>3</td></tr>
<tr><td>Amber</td><td>4</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Color</b>s mentioned above while indicating the color of this LED. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.5 The Blade Servers Layer

Using the tests mapped to this layer, administrators can instantly detect the health, power state and operational and maintenance modes of each blade server, and accurately identify the current status and color of the LEDs provided in the blade servers.



Blade Servers

- ✓ Hitachi Blade Servers
  - ✓ Blade Server-1
  - ✓ Blade Server-2
  - ✓ Blade Server-3
  - ✓ Blade Server-4
  - ✓ Blade Server-5
  - ✓ Blade Server-6
  - ✓ Blade Server-7
  - ✓ Blade Server-8
- ✓ Hitachi Blades Servers LED
  - ✓ Blade Server-1
    - ✓ ERROR LOG
    - ✓ FAULT
    - ✓ LID
    - ✓ POWER
  - ✓ Blade Server-2
    - ✓ ERROR LOG
    - ✓ FAULT
    - ✓ LID
    - ✓ POWER
  - ✓ Blade Server-3
    - ✓ ERROR LOG
    - ✓ FAULT
    - ✓ LID
    - ✓ POWER
  - ✓ Blade Server-4
    - ✓ ERROR LOG
    - ✓ FAULT
    - ✓ LID
    - ✓ POWER
  - ✓ Blade Server-5
    - ✓ ERROR LOG
    - ✓ FAULT
    - ✓ LID
    - ✓ POWER
  - ✓ Blade Server-6
    - ✓ ERROR LOG
    - ✓ FAULT
    - ✓ LID
    - ✓ POWER

Figure 3.5: The tests mapped to the Blade Servers layer

The tests of this layer are discussed in the forthcoming sections.

3.5.1 Hitachi Blade Servers Test

The Hitachi Compute Blade allows accommodating upto eight dual-socket-based blade servers in the chassis. The blade servers are configured in redundant scenario to ensure high-availability and operation continuity and are powered by Intel Xeon processors. With this configuration, the Hitachi Compute Blade meets performance needs of large-scale systems that require extremely high compute power and I/O performance. Each blade server supports upto 30 logical partitions, which in turn simplifies building virtual environment and enables using virtualization to consolidate application and database servers. In addition, the blade servers provide flexible solution for scaling up your infrastructure without any complex requirements. Critical or fatal physical damages, power failures or network connectivity failures can render the blade servers unavailable/inoperable. This in turn degrades performance of the Hitachi Compute Blade. To prevent such eventualities, it is imperative that administrators should closely monitor the blade servers and take immediate measures before the clients complaint. This can be achieved by the **Hitachi Blade Servers** test!

By continuously monitoring each blade server in the chassis, administrators can obtain the overall health, power status and maintenance mode of each blade server. This way, administrators are alerted to abnormalities as soon as they occur and can take necessary corrective actions before mission-critical services begin to suffer. This test also reports the current voltage and power consumption of each blade server.

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for each blade server on the Hitachi Compute Blade being monitored.

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed
2. **HOST** – The IP address of the Hitachi Compute Blade.
3. **PORT -** The port at which the monitored target listens. By default, this is set to NULL.
4. **SNMPPORT** – The port at which the Hitachi Compute Blade exposes its SNMP MIB; the default is 161.
5. **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.
6. **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.
7. **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.

8. **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*.
9. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
10. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
11. **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

12. **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.
13. **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

14. **ENCRYPTPASSWORD** – Specify the encryption password here.
15. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
16. **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.

17. **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**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Health status</td><td>Indicates the current health of this blade server.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>State</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>0.5</td></tr>
<tr><td>No Blade Server is Installed</td><td>0</td></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Failed</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>State</b>s mentioned above while indicating the health of each blade server. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>PowerSupply status</td><td>Indicates the current power supply status of this blade server.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>PowerOff</td><td>1</td></tr><tr><td>Standby</td><td>2</td></tr><tr><td>PowerOn</td><td>3</td></tr><tr><td>Unknown</td><td>4</td></tr><tr><td>PowerOn Executing</td><td>5</td></tr><tr><td>PowerOff Executing</td><td>6</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>State</b>s mentioned above while indicating the current power supply status of each blade server. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Current voltage</td><td>Indicates the current voltage of this blade server.</td><td>Volts</td><td>A sudden and significant rise in the value of this measure could be a cause of concern.</td></tr>
<tr><td>Power consumption</td><td>Indicates the amount of power consumed by this blade server.</td><td>Amps</td><td>Compare the value of this measure across the blade servers to figure out which blade server is power-intensive.</td></tr>
<tr><td>Primary Status</td><td>Indicates whether/not this blade server is primary.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Primary</td><td>1</td></tr><tr><td>Non Primary</td><td>2</td></tr><tr><td>Unknown</td><td>3</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>State</b>s mentioned above while indicating the whether/not this blade server is primary. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Maintenance mode</td><td>Indicates the current maintenance mode of this blade server.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Mode</th><th>Numeric Value</th></tr><tr><td>Normal</td><td>1</td></tr><tr><td>CE Maintenance Mode</td><td>2</td></tr><tr><td>User Maintenance Mode</td><td>3</td></tr><tr><td>Unknown</td><td>4</td></tr></table>
<b>Note:</b>
By default, this measure can report the <b>Mode</b>s mentioned above while indicating the current maintenance mode of the blade server. However,</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			the graph of this measure is indicated using the numeric equivalents.

3.5.2 Hitachi Blades Servers LED Test

The Hitachi Compute Blade allows accommodating upto eight dual-socket-based blade servers in the chassis. Critical or fatal physical damages, power failures or network connectivity failures can render the blade servers unavailable/inoperable. In environments where all the eight blade servers are accommodated in the chassis, if a single blade server fails or is critically damaged, then administrators may not be able to figure out the exact blade server that is problematic at a singe glance. To avoid such identification problems, each blade server is provided with the following LEDs:

- Power LED and Alarm LED - visually indicate administrators to various power state changes and alarms generated in each blade server.
- Attention LED - automatically turns on when the power button with LED was pressed explicitly. The attention automatically turns off when the main power is turned off.
- Location identify LED - helps administrators in identifying the blade server.

If the LEDs fail or if the LEDs are damaged, then, administrators may be deprived of identifying the problematic blade server at a single glance. To avoid this issue, faulty LEDs should be identified and replaced immediately. The **Hitachi Blades Servers LED** test helps administrators to constantly keep a constant vigil on the status of the LEDs and the color of the LEDs.

This test auto-discovers the LEDs of each blade server and reports the current status of each LED and the color of the LED on each blade server. This way, administrators can be alerted to faulty LEDs and replace them at the earliest!

Target of the test : Hitachi Compute Blade

Agent deploying the test : An external agent

Outputs of the test : One set of results for the *blade server:LED* pair in the Hitachi Compute Blade being monitored.

Configurable parameters for the tests

1. **TEST PERIOD -** How often should the test be executed

2. **HOST** – The IP address of the Hitachi Compute Blade

3. **SNMPPORT** – The port at which the Hitachi Compute Blade 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**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
LED status	Indicates the current status of this LED.		The values that this measure can report and the numeric values they indicate have been listed in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric value</th></tr>
<tr><td>Turn Off</td><td>1</td></tr>
<tr><td>Turn On</td><td>2</td></tr>
<tr><td>Unknown</td><td>3</td></tr>
<tr><td>Blink</td><td>4</td></tr>
<tr><td>Blink Fast</td><td>5</td></tr>
<tr><td>Blink Slow</td><td>6</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the States mentioned above while indicating the current status of this LED in the blade server. However, the graph of this measure is indicated using the numeric equivalents.
</td></tr>
<tr><td>LED color</td><td>Indicates the color of this LED.</td><td></td><td>
The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Color</th><th>Numeric Value</th></tr>
<tr><td>Blue</td><td>1</td></tr>
<tr><td>Green</td><td>2</td></tr>
<tr><td>Red</td><td>3</td></tr>
<tr><td>Amber</td><td>4</td></tr>
<tr><td>Unknown</td><td>0</td></tr>
</table>
<b>Note:</b>
</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure can report the **Color**s mentioned above while indicating the color emitted by this LED. However, the graph of this measure is indicated using the numeric equivalents.

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.