Monitoring Delta UPS

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

In large environments where power issues such as power failure, power sag, power surge, under voltage or over voltage, frequency variation, harmonic distortion and line noise are a big concern, Delta UPS emphasizes the areas of redundant power supply, voltage regulation, equipment protection and adjustment, thus providing the much needed protection to the computers, datacenters, electrical/telecommunication equipments in the environment.

Since the UPS plays a crucial role in protecting the environment, issues in its performance can cause serious fatalities, data loss etc. Therefore, it is essential to periodically monitor the Delta UPS round the clock. This is exactly what the eG Enterprise does.

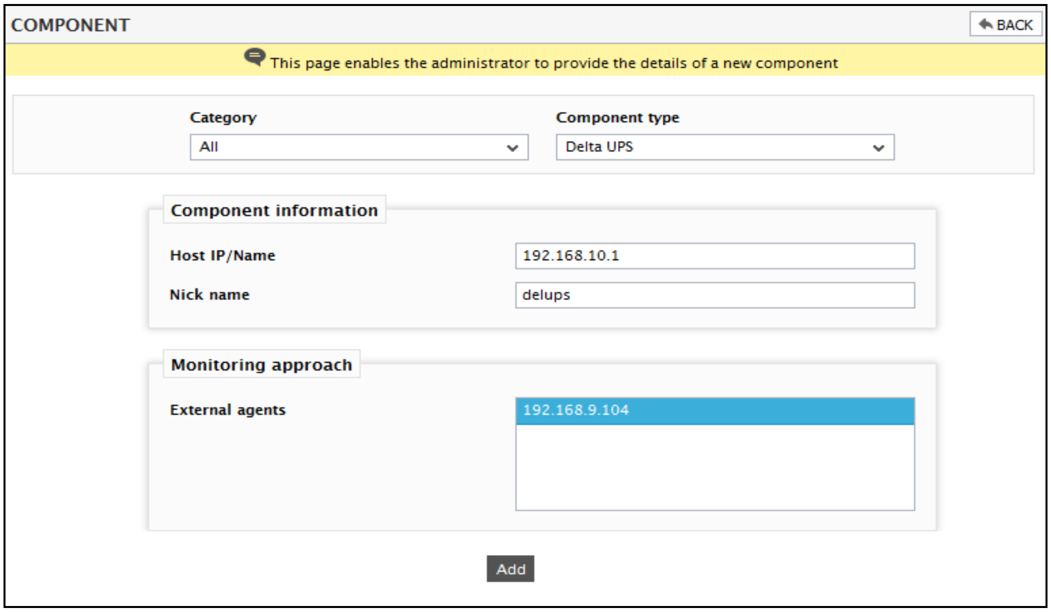
Chapter 2: How to Monitor Delta UPS using eG Enterprise?

eG Enterprise monitors the Delta UPS in an agentless manner. For this purpose, deploy an eG agent on any remote Windows host in the environment. This agent is capable of polling the SNMP MIB Of the Delta UPS at regular intervals and fetching critical measures related to its performance. To make the eG agent communicate with the Delta UPS and pullout performance metrics, ensure that the Delta UPS is SNMP-enabled before attempting to monitor.

2.1 Managing the Delta UPS

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

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



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

Category: All

Component type: Delta UPS

Component information

Host IP/Name: 192.168.10.1

Nick name: delups

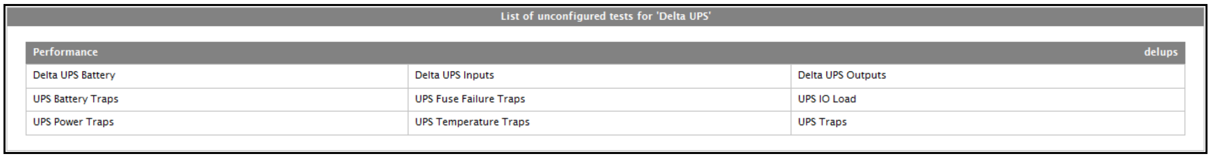
Monitoring approach

External agents: 192.168.9.104

Figure 2.1: Adding a Delta UPS

4. Specify the **Host IP/Name** and **Nick name** of the Delta UPS component as shown in Figure 2.1. Then click on the **Add** button to register the changes.

5. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).



List of unconfigured tests for 'Delta UPS'

Performance		delups
Delta UPS Battery	Delta UPS Inputs	Delta UPS Outputs
UPS Battery Traps	UPS Fuse Failure Traps	UPS IO Load
UPS Power Traps	UPS Temperature Traps	UPS Traps

Figure 2.2: List of Unconfigured tests for the Delta UPS

6. Click on any test in the list of unconfigured tests. To know how to configure the tests, refer to **Monitoring Delta UPS** chapter.

7. Once all the tests are configured, signout of the eG administrative interface.

Chapter 3: Monitoring Delta UPS

eG Enterprise provides a specialized *Delta UPS* monitoring model (see Figure 3.1) to monitor the external availability and internal health of a Delta UPS and its core components.

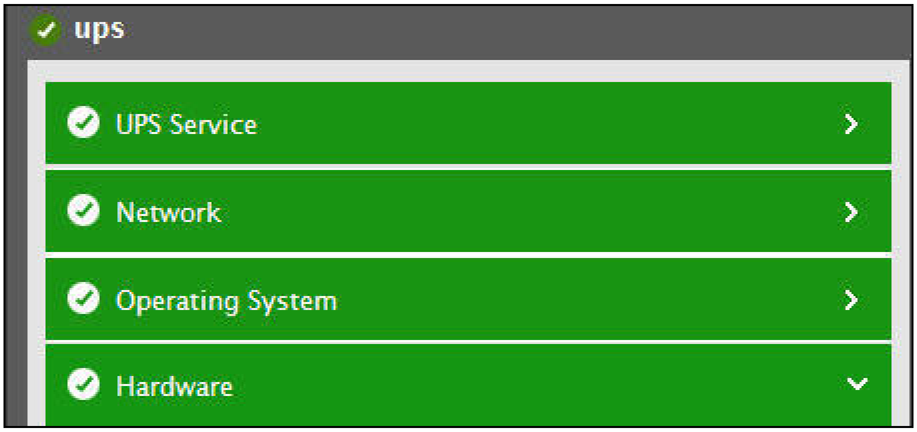


Figure 3.1: The layer model of a Delta UPS

Every layer of Figure 3.1 is mapped to a variety of tests which connect to the SNMP MIB of the UPS to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- Is the UPS currently running on battery or on power?
- If running on battery, what is the time for which the battery has been used? Is very little running time left with the battery?
- How much charge is still remaining with the battery? Has the battery status already turned to Deplete?
- Has the battery temperature suddenly spiked?
- Were any severe power/voltage fluctuations discovered in the input lines?
- Is any output line consuming the power capacity of the UPS excessively?

Since the **Network** layer has been dealt with *Monitoring Windows and Unix Servers* document, the sections to come will discuss the remaining layers of Figure 1.

3.1 The Hardware Layer

One of the key components of a UPS is its battery. A defective battery can often cause failure of the UPS, thus disrupting the delivery of the critical business services it supports. Using the tests mapped to the **Hardware** layer, users can accurately determine the current health of the UPS battery, the performance of the battery and the traps captured whenever the battery is low.

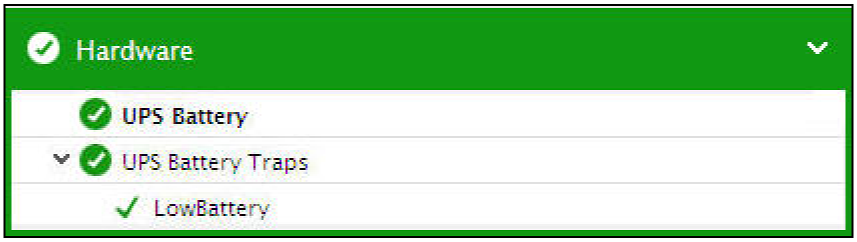


Figure 3.2: The tests mapped to the Hardware layer

3.1.1 Delta UPS Battery Test

This test reports critical statistics indicating the level of performance and overall health of the UPS battery along with the current status of the battery.

Target of the test : A Delta UPS

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Delta UPS monitored .

Configurable parameters for the test

Parameter	**Description**
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the host listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen

Parameter	Description
	is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:

Parameter	Description
	• **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Battery status</td><td>Indicates the current state of the battery available in this Delta UPS.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Ok</td><td>0</td></tr>
<tr><td>Low</td><td>1</td></tr>
<tr><td>Depleted</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of the battery. However, in the graph of this measure, the current state of the battery is indicated using only the Numeric Values listed in the above table.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Battery usage time	Indicates the battery discharge time.	Secs	This measure indicates the value in secs if the unit is on battery power. The value might return to Zero if the unit is not on battery power.
Running time left	Indicates the running time left in mins, to battery charge depletion under the present load conditions if the utility power is off.	Mins	Ideally, the value of this measure should be high. A low value or a value that is consistently decreasing is indicative of rapid depletion of the battery charge. If this condition is left unattended, it could result in a UPS failure. Under such circumstances, you might want to turn on the utility power and make sure that the UPS is no longer on battery power, so as to safeguard your equipment and data from irrepairable damage/loss.
Charge remaining	Indicates the percentage of charge currently remaining in the battery.	Percent	Ideally, this value should be high. If the charge is full, this value would be 100. A value close to 0 or a value that is consistently decreasing is indicative of rapid depletion of the battery charge. If this condition is left unattended, it could result in a UPS failure. Under such circumstances, you might want to turn on the utility power and make sure that the UPS is no longer on battery power, so as to safeguard your equipment and data from irrepairable damage/loss.
Battery voltage	Indicates the current battery voltage.	Volts	
Battery current	Indicates the amount of current presently conducted by the battery.	Amps	A high value is indicative of excessive usage of the UPS.
Battery temperature	Indicates the current ambient temperature at or near the UPS battery.	Celcius	Ideally, the value of this measure should be low. A very high value is indicative of a rise in battery temperature that can be caused by

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>excessive usage of the UPS. The temperature of the battery should always be maintained at optimal levels, so as to avoid failure of the UPS and the resultant disruption of power supply. To ensure this, it is recommended that you install a cooling unit (AC unit) in the area where the UPS is installed.</td></tr>
<tr><td>Battery condition</td><td>Indicates the current condition of the battery.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Good</td><td>0</td></tr>
<tr><td>Weak</td><td>1</td></tr>
<tr><td>Replace</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current condition of the battery. However, in the graph of this measure, the current condition of the battery is indicated using only the Numeric Values listed in the above table.</td></tr>
</table>

3.1.2 UPS Battery Traps Test

This test intercepts the low battery traps sent by the UPS, extracts relevant information related to the low battery from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the abnormalities in the battery if any, understand the nature of these abnormalities, and accordingly decide on the remedial measures.

Target of the test : A Delta UPS

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event that occurred on the target Delta UPS.

Configurable parameters for the test

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Test Period</td><td>How often should the test be executed</td></tr>
<tr><td>Host</td><td>The host for which the test is to be configured.</td></tr>
<tr><td>Port</td><td>The port at which the specified Host listens. By default, this is NULL.</td></tr>
<tr><td>Source Address</td><td>Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.</td></tr>
<tr><td>OID Value</td><td>
<p>Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:</p>
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table>
<p>In this case the OIDValue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.</p>
<p>An * can be used in the OID-value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.</p>
<p>Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent</p>
</td></tr>
</table>

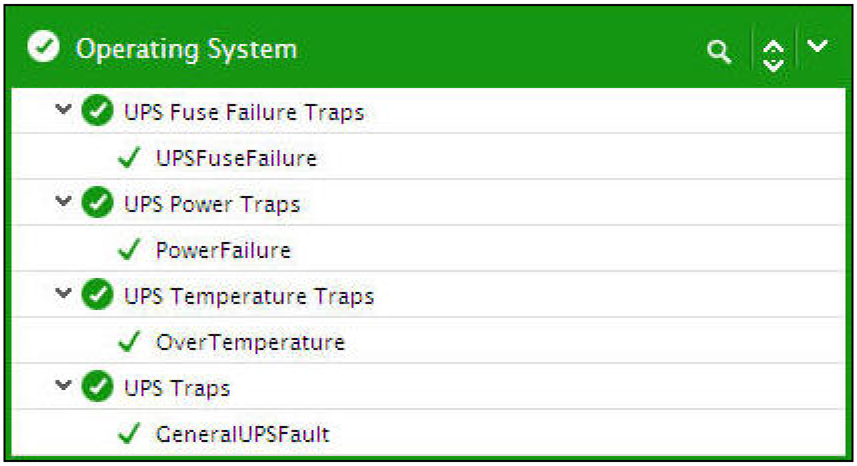
Parameter	Description
	a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be: Trap5: .1.3.6.1.4.1.9156.1.1.5-any.
ShowOID	Specifying True against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
TrapOIDs	By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Battery failure	Indicates the number of events of this type that were triggered during the last measurement period.	Number	The failure events may be generated due to the failure of the fans of the Juniper EX Switch. If the failure events are not rectified within a certain pre-defined timeperiod, the UPS will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Juniper EX Switch.

3.2 The Operating System Layer

This layer helps you in identifying the number of trap messages that were sent by the UPS for failures of the fuse, power supply and abnormal deduction in temperature of the hardware components.


Operating System

UPS Fuse Failure Traps

UPSFuseFailure

UPS Power Traps

PowerFailure

UPS Temperature Traps

OverTemperature

UPS Traps

GeneralUPSFault

Figure 3.3: The tests mapped to the Operating System layer

3.2.1 UPS Fuse Failure Traps Test

This test intercepts the fuse failure traps sent by the UPS, extracts relevant information related to the fuse failure from the traps, and reports the count of these trap messages to the eG manager.

Target of the test : A Delta UPS

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event that occurred on the target Delta UPS.

Configurable parameters for the test

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Test Period</td><td>How often should the test be executed</td></tr>
<tr><td>Host</td><td>The host for which the test is to be configured.</td></tr>
<tr><td>Port</td><td>The port at which the specified Host listens. By default, this is <i>NULL</i>.</td></tr>
<tr><td>Source Address</td><td>Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.</td></tr>
<tr><td>OID Value</td><td>Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table>
<p>In this case the OIDValue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.</p>
<p>An * can be used in the OID-value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.</p>
<p>Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent</p></td></tr>
</table>

Parameter	Description
	a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be: Trap5: .1.3.6.1.4.1.9156.1.1.5-any.
ShowOID	Specifying True against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
TrapOIDs	By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Fuse failure	Indicates the number of events of this type that were triggered during the last measurement period.	Number	The failure events may be generated due to the failure of the battery fuse of the UPS. If the failure events are not rectified within a certain pre-defined timeperiod, the UPS will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Delta UPS.

3.2.2 UPS Power Traps Test

This test intercepts the power failure traps sent by the UPS, extracts relevant information related to the power failure from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the abnormalities in the battery if any, understand the nature of these abnormalities, and accordingly decide on the remedial measures.

Target of the test : A Delta UPS

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event that occurred on the target Delta UPS.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
Port	The port at which the specified Host listens. By default, this is NULL.
Source Address	Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>OID Value</td><td>Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table>

In this case the OIDValue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.
An * can be used in the OID-value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.
Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:
Trap5: .1.3.6.1.4.1.9156.1.1.5-any.</td></tr>
<tr><td>ShowOID</td><td>Specifying True against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.</td></tr>
<tr><td>TrapOIDs</td><td>By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing</td></tr>
</table>

Parameter	Description
	spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Power failure	Indicates the number of events of this type that were triggered during the last measurement period.	Number	The failure events may be generated due to the power failure of the UPS. If the failure events are not rectified within a certain pre-defined timeperiod, the UPS will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Delta UPS.

3.2.3 UPS Temperature Traps Test

This test intercepts the temperature failure traps sent by the UPS, extracts relevant information related to the temperature failure from the traps, and reports the count of these trap messages to the eG manager.

Target of the test : A Delta UPS

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event that occurred on the target Delta UPS.

Configurable parameters for the test

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

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

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

An * can be used in the OID-value patterns to denote any number of leading or trailing

Parameter	Description
	characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*. Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be: Trap5: .1.3.6.1.4.1.9156.1.1.5-any.
ShowOID	Specifying True against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
TrapOIDs	By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Temperature failure	Indicates the number of events of this type that weretriggered during the last measurement period.	Number	The failure events may be generated due to the temperature failure of the UPS. If the failure events are not rectified within a certain pre-defined timeperiod, the UPS will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Delta UPS.

3.2.4 UPS Traps Test

This test intercepts the failure traps sent by the UPS, extracts relevant information related to the UPS failure from the traps, and reports the count of these trap messages to the eG manager.

Target of the test : A Delta UPS

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event that occurred on the target Delta UPS.

Configurable parameters for the test

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

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Port</td><td>The port at which the specified Host listens. By default, this is NULL.</td></tr>
<tr><td>Source Address</td><td>Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.</td></tr>
<tr><td>OID Value</td><td><p>Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:</p>
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table>
<p>In this case the OIDValue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.</p>
<p>An * can be used in the OID-value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.</p>
<p>Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:</p>
<p>Trap5: .1.3.6.1.4.1.9156.1.1.5-any.</p></td></tr>
<tr><td>ShowOID</td><td>Specifying True against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.</td></tr>
</table>

Parameter	Description
TrapOIDs	By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
UPS failure	Indicates the number of events of this type that were triggered during the last measurement period.	Number	The failure events may be generated due to the failure of the UPS. If the failure events are not rectified within a certain pre-defined timeperiod, the UPS will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Delta UPS.

3.3 The UPS Service Layer

To evaluate the performance of the input lines and output lines to the UPS, and to measure the I/O activity handled by these lines, use the tests associated with the **UPS Service** layer.

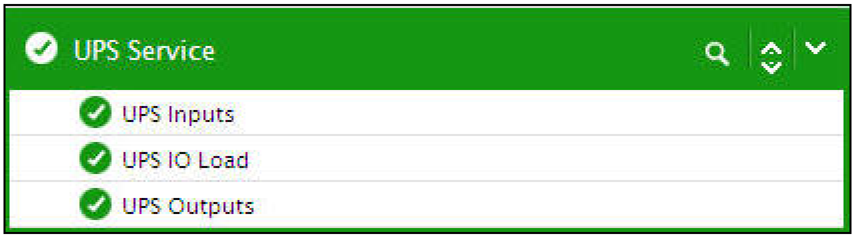


Figure 3.4: The tests mapped to the UPS Service layer

3.3.1 Delta UPS Inputs Test

This test monitors the inputs to the UPS via input lines, and reveals the level of activity on the UPS. Any drop in the level (i.e., a sudden voltage drop) could indicate an imminent power failure at the source.

Target of the test : A Delta UPS

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Delta UPS device that is to be monitored.

Configurable parameters for the test

Parameter	**Description**
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the host listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen

Parameter	Description
	is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:

Parameter	Description
	- **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Input line1 frequency	Indicates the current input frequency of phase 1 in this UPS.	Hz	Comparing the value of these measures with each other helps you to identify the phase with the maximum input frequency.
Input line2 frequency	Indicates the current input frequency of phase 2 in this UPS.	Hz	
Input line3 frequency	Indicates the current input frequency of phase 3 in this UPS.	Hz	
Input line1 voltage	Indicates the current input voltage of phase 1 in this UPS.	Volts	Comparing the value of these measures across each other will help you identify the phase with the maximum input voltage.
Input line2 voltage	Indicates the current input voltage of phase 2 in this UPS.	Volts	
Input line3 voltage	Indicates the current input voltage of phase 3 in this	Volts	

Measurement	Description	Measurement Unit	Interpretation
	UPS.		
Input line1 current	Indicates the input current presently handled by phase 1 in this UPS.	Amps	Comparing the value of these measures across each other will help you identify the phase that handles the maximum input current.
Input line2 current	Indicates the input current presently handled by phase 2 in this UPS.	Amps	
Input line3 current	Indicates the input current presently handled by phase 3 in this UPS.	Amps	

3.3.2 UPS IO Load Test

This test monitors the power capacity used by each output phase of the UPS. Any discrepancy in the level of activity on the output phase could be indicative of a problem with the UPS.

Target of the test : A Delta UPS

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Delta UPS that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the host listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen

Parameter	Description
	is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:

Parameter	Description
	- **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Output line1 load	Indicates the percentage of the UPS power capacity presently being used on output phase 1.	Percent	Comparing the value of this measure with Output line2 load and Output line3 load will reveal which output line is utilizing the maximum power.
Output line2 load	Indicates the percentage of the UPS power capacity presently being used on output phase 2.	Percent	Comparing the value of this measure with Output line3 load and Output line1 load will reveal which output line is utilizing the maximum power.
Output line3 load	Indicates the percentage of the UPS power capacity presently being used on output phase 3.	Percent	Comparing the value of this measure with Output line1 load and Output line2 load will reveal which output line is utilizing the maximum power.

3.3.3 UPS Outputs Test

This test monitors the outputs sent by the UPS via its output phase to the loads. Any discrepancy in the level of activity on the output phase could be indicative of a problem with the UPS.

Target of the test : A Delta UPS

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Delta UPS device that is to be monitored.

Configurable parameters for the test

Parameter	**Description**
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the host listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a 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*.

Parameter	Description
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Output lines	Indicates the number of output lines currently utilized by this UPS.	Number	A high value is indicative of high activity on the UPS.
Output frequency	Indicates the current output frequency.	Hz	
Output line1 voltage	Indicates the current output voltage of phase 1 in this UPS.	Volts	Comparing the value of these measures with each other will help you identify the phase with the maximum output voltage.
Output line2 voltage	Indicates the current output voltage of phase 2 in this UPS.	Volts	
Output line3 voltage	Indicates the current output voltage of phase 3 in this UPS.	Volts	
Output line1 current	Indicates the output current presently handled by phase 1 in this UPS.	Amps	Comparing the value of these measures with each other will help you identify the phase with the maximum output current.
Output line2 current	Indicates the output current presently handled by phase 2 in this UPS.	Amps	
Output line3 current	Indicates the output current presently handled by phase 3 in this UPS.	Amps	
Output line1 power	Indicates the real output power of phase 1 in this UPS.	Watts	Comparing the value of these measures with each other will help you identify the phase with the maximum output power.
Output line2 power	Indicates the real output power of phase 1 in this UPS.	Watts	
Output line3 power	Indicates the real output power of phase 1 in this UPS.	Watts	

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.