Monitoring Delta UPS

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

1

Monitoring Delta UPS

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 .

eG Enterprise provides a specialized Delta *UPS* monitoring model (see Figure 1) to monitor the external availability and internal health of a Delta UPS and its core components.

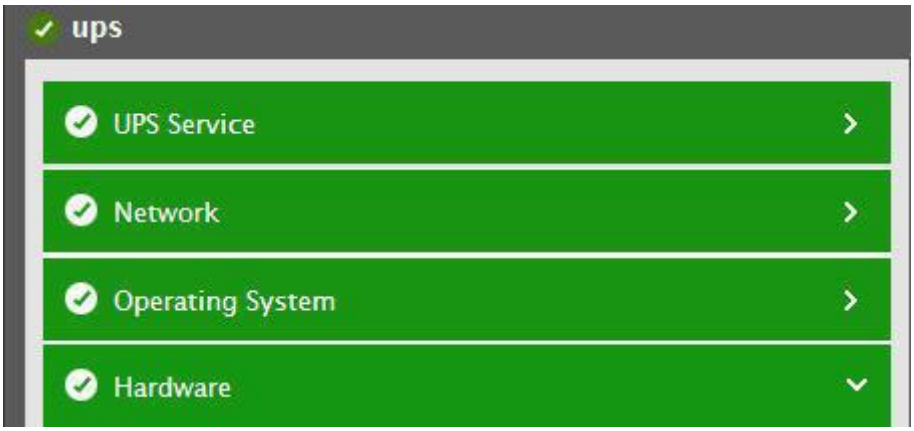

Figure 1: The layer model of a Delta UPS

Every layer of Figure 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 Web Servers document, the sections to come will discuss the remaining layers of Figure 1.

1.1 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 2: The tests mapped to the Hardware layer

1.1.1 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.

Purpose	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
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Delta UPS 3. **SNMPPORT** – The SNMP Port number of the Delta UPS (161 typically) 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. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **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. 15. **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 Delta UPS over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for the Delta UPS monitored

<table>
<tr><th>Measurements made by the test</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td rowspan="3"></td><td>Battery status:
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>
Note:
This measure reports the Measure Values 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>
<tr><td>Battery usage time:
Indicates the battery discharge time.</td><td>Secs</td><td>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.</td></tr>
<tr><td>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.</td><td>Mins</td><td>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.</td></tr>
</table>

<table>
<tr><td></td><td>Charge remaining:
Indicates the percentage of charge currently remaining in the battery.</td><td>Percent</td><td>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.</td></tr>
<tr><td></td><td>Battery voltage:
Indicates the current battery voltage.</td><td>Volts</td><td></td></tr>
<tr><td></td><td>Battery current:
Indicates the amount of current presently conducted by the battery.</td><td>Amps</td><td>A high value is indicative of excessive usage of the UPS.</td></tr>
<tr><td></td><td>Battery temperature:
Indicates the current ambient temperature at or near the UPS battery.</td><td>Celcius</td><td>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 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></td><td>Battery condition:
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>Note:
This measure reports the Measure Values 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>

1.1.2 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.

Purpose	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
Target of the test	A Delta UPS
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **SOURCEADDRESS** - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. 4. **OIDVALUE** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

	In this case the **OIDVALUE** parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface. An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**. Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be *HOST* and not *Host_*system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be: *Trap5: .1.3.6.1.4.1.9156.1.1.5-any*.**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. 6. **TRAPOIDS** – By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified **SOURCEADDRESS**es. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the **TRAPOIDS** text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, **94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces. 7. **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**.		
Outputs of the test	One set of results for each type of failure event that occurred on the target Delta UPS		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**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.

1.2 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.

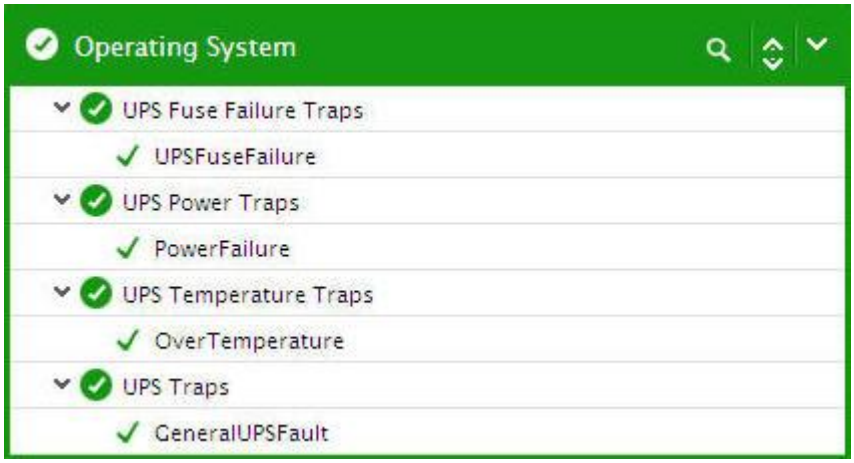

Figure 3: The tests mapped to the Operating System layer

1.2.1 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.

Purpose	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

<table>
<tr>
<td>Configurable parameters for the test</td>
<td>
1. TESTPERIOD - How often should the test be executed
2. HOST - The host for which the test is to be configured.
3. SOURCEADDRESS - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
4. OIDVALUE - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:
<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>
</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 *HOST* and not *Host_*system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be: *Trap5: .1.3.6.1.4.1.9156.1.1.5-any*.**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. 6. **TRAPOIDS** – By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified **SOURCEADDRESS**es. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the **TRAPOIDS** text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, **94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces. 7. **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**.		
Outputs of the test	One set of results for each type of failure event that occurred on the target Delta UPS		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**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.

1.2.2 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.

Purpose	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
Target of the test	A Delta UPS
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **SOURCEADDRESS** - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. 4. **OIDVALUE** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

	In this case the **OIDVALUE** parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface. An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**. Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be *HOST* and not *Host_*system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be: *Trap5: .1.3.6.1.4.1.9156.1.1.5-any*.**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. 6. **TRAPOIDS** – By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified **SOURCEADDRESS**es. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the **TRAPOIDS** text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, **94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces. 7. **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**.		
Outputs of the test	One set of results for each type of failure event that occurred on the target Delta UPS		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**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.

1.2.3 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.

Purpose	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
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **SOURCEADDRESS** - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. 4. **OIDVALUE** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

	In this case the **OIDVALUE** parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface. An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**. Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be *HOST* and not *Host_*system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be: *Trap5: .1.3.6.1.4.1.9156.1.1.5-any*.**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. 6. **TRAPOIDS** – By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified **SOURCEADDRESS**es. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the **TRAPOIDS** text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, **94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces. 7. **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**.		
Outputs of the test	One set of results for each type of failure event that occurred on the target Delta UPS		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**Temperature 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 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.

1.2.4 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.

Purpose	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
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **SOURCEADDRESS** - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. 4. **OIDVALUE** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

	In this case the **OIDVALUE** parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface. An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**. Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be *HOST* and not *Host_*system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be: *Trap5: .1.3.6.1.4.1.9156.1.1.5-any*.**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. 6. **TRAPOIDS** – By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified **SOURCEADDRESS**es. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the **TRAPOIDS** text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, **94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces. 7. **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**.		
Outputs of the test	One set of results for each type of failure event that occurred on the target Delta UPS		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**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.

1.3 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 4: The tests mapped to the UPS Service layer

1.3.1 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.

Purpose	Monitors the inputs to the UPS via input lines, and reveals the level of activity on the UPS
Target of the test	A Delta UPS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Delta UPS 3. **SNMPPORT** – The SNMP Port number of the Delta UPS (161 typically) 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. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **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.

	15. **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 Delta UPS over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Delta UPS device that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Input lines: Indicates the number of input lines i.e., phase currently utilized by this UPS.	Number	A high value is indicative of high activity on the UPS.
	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 UPS.	Volts	

	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	

1.3.2 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.

Purpose	Monitors the power capacity used by each output phase of the UPS
Target of the test	A Delta UPS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Delta UPS 3. **SNMPPORT** – The SNMP Port number of the Delta UPS (161 typically) 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. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **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.

	15. **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 Delta UPS over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Delta UPS that is to be monitored		
Measurements made by the test	**Measurement**	**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.

1.3.3 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.

Purpose	Monitors the outputs sent by the UPS via its output phase to the loads
Target of the test	A Delta UPS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Delta UPS 3. **SNMPPORT** – The SNMP Port number of the Delta UPS (161 typically) 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. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **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.

	15. **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 Delta UPS over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Delta UPS device that is to be monitored		
Measurements made by the test	**Measurement**	**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	

2 Conclusion

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

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