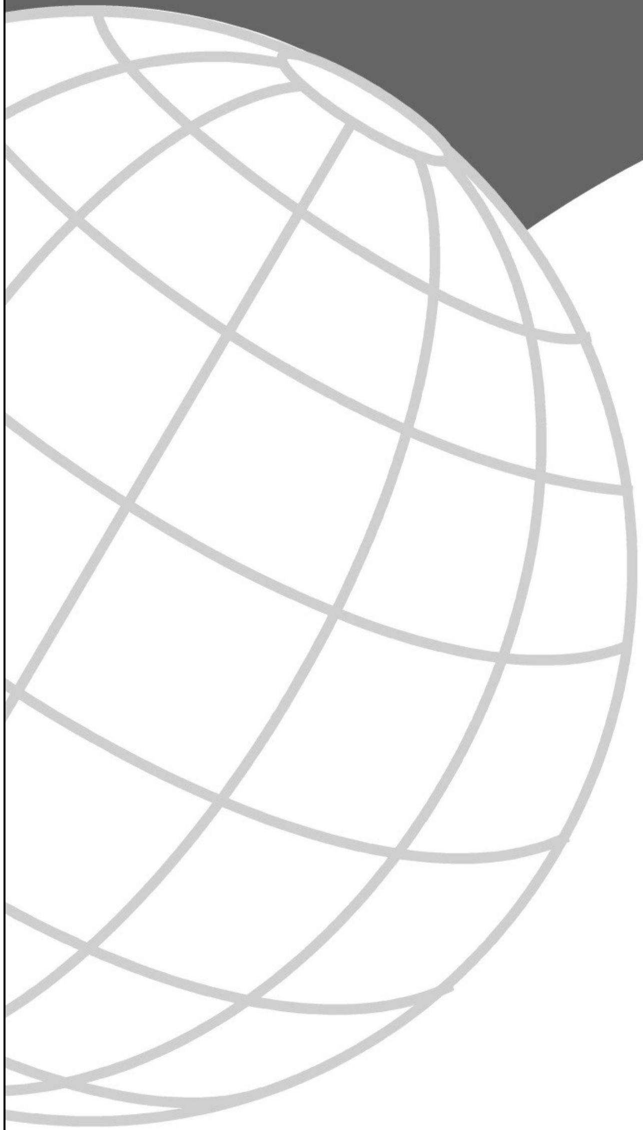


Monitoring Dell Switch M-Series

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 2008, Windows 7, Windows 8, Windows 10, Windows 2012 and Windows 2016 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

©2016 eG Innovations Inc. All rights reserved.

Table of contents

Table of Figures

1

Introduction

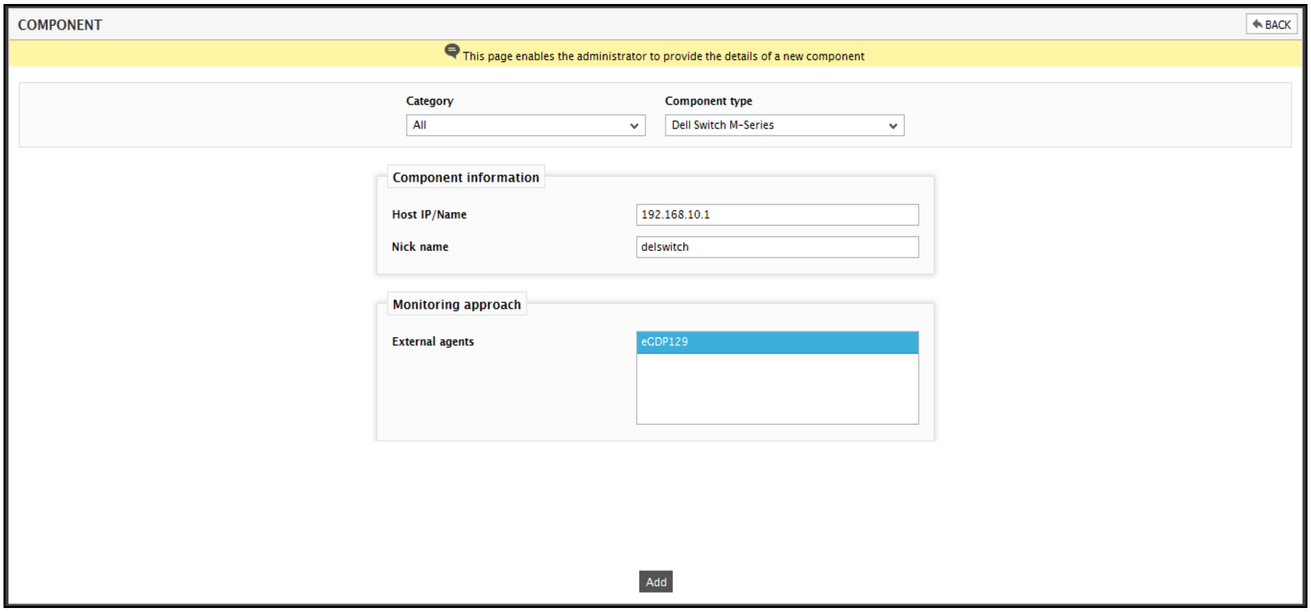
The Dell™ PowerEdge™ M-series blade solution is a breakthrough in enterprise server architecture. Built from the ground up using Dell's Energy Smart and FlexIO technologies, the M-series is designed to combat data center sprawl and IT complexity. The M-series delivers one of the most energy efficient, flexible, and manageable blade server products on the market.

The MXL 10/40GbE Switch is a layer 2/ 3 blade switch with two fixed 40GbE ports on the base module and support for two optional plug-in modules. The switch operates in a PowerEdge M1000e Enclosure, which can support up to 32 servers and six MXL 10/40GbE Switches. This switch runs the Dell Networking operating system (OS), providing switching, bridging, and routing functionality for transmitting data, storage, and server traffic. The switch also supports data center bridging (DCB) features, and optimizes connectivity between servers and storage devices over Fiber Channel over Ethernet (FCoE) and internet small computer system interface (iSCSI) links. For a smooth data transmission in data centers, most administrators of large infrastructures rely on these MXL 10/40GbE switches. If the switches malfunction or do not respond, then, data may not be transmitted from the data centers at a faster pace which would directly have an impact on the end users. Administrators should therefore monitor the switches in their environment 24*7. Let us now deep-dive into the procedure to monitor the Dell Switch M-Series monitoring model in the forthcoming chapters.

2

Administering the eG Manager to monitor a Dell Switch M-Series

1. Log into the eG administrative interface.
2. eG Enterprise cannot automatically discover Dell Switch M-Series. You need to manually add the server using the **COMPONENTS** page (see) that appears when the Infrastructure -> Components -> Add/Modify menu sequence is followed. Remember that components manually added are managed automatically.



COMPONENT

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

Category: All

Component type: Dell Switch M-Series

Component information

Host IP/Name: 192.168.10.1

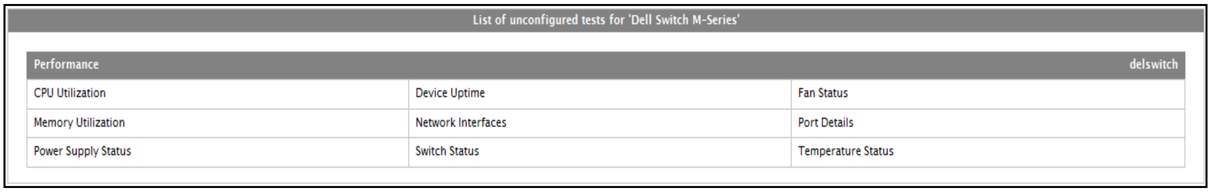
Nick name: delswitch

Monitoring approach

External agents: eGDP129

Figure 2.1: Adding the Dell Switch M-Series

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



List of unconfigured tests for 'Dell Switch M-Series'

Performance		delswitch
CPU Utilization	Device Uptime	Fan Status
Memory Utilization	Network Interfaces	Port Details
Power Supply Status	Switch Status	Temperature Status

Figure 2.2: List of tests to be configured for Dell Switch M-Series

4. Click on the **CPU Utilization** test to configure it. To know how to configure the test, click here. All other tests will be configured automatically.
5. Finally, signout of the eG administrative interface.

3

Monitoring the Dell Switch M-Series

eG Enterprise has developed a dedicated *Dell Switch M-Series* monitoring model which periodically checks the data traffic to and from each port of the switch, the temperature of each stack unit of the switch, the memory utilization etc, so that abnormalities can be detected and rectified before any irreparable damage occurs.

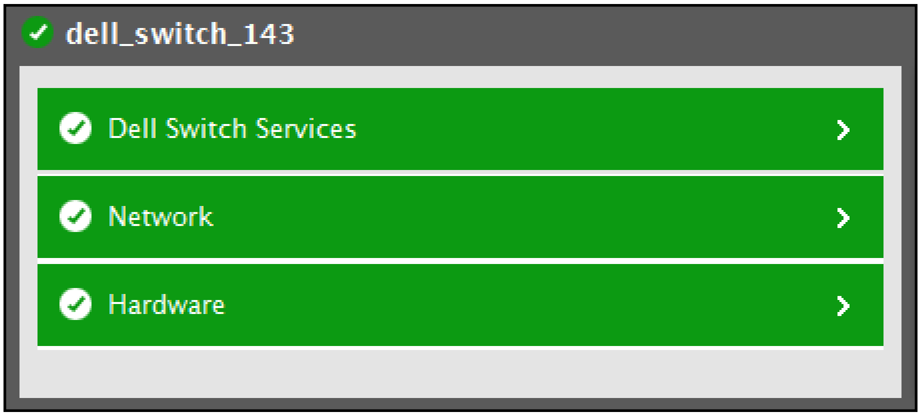


Figure 3.1: The layer model of the Dell Switch M-Series

Every layer of Figure 1 is mapped to a variety of tests which connect to the SNMP MIBs of the target Dell Switch M-Series to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- What is the CPU utilization during the last second?
- What is the CPU utilization during the last minute?
- How well the CPU is utilized during the last 5 minutes?
- What is the current status of the fan available in each stack unit?
- How well the memory of each stack unit is utilized?
- What is the current status of the power supply unit within each stack unit?
- What is the current temperature of each stack unit?
- What is the current status of the switch available in each stack unit?
- How well each port transmits / receives power signals?
- What is the administrative and operational status of each port?

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

3.1 The Hardware layer

Using this layer administrators can track the CPU utilization and memory utilization of each stack unit available in the Dell Switch M-series. In addition, administrators can also track the current temperature of each stack unit and determine the stack units that are not operating within the admissible temperature range.

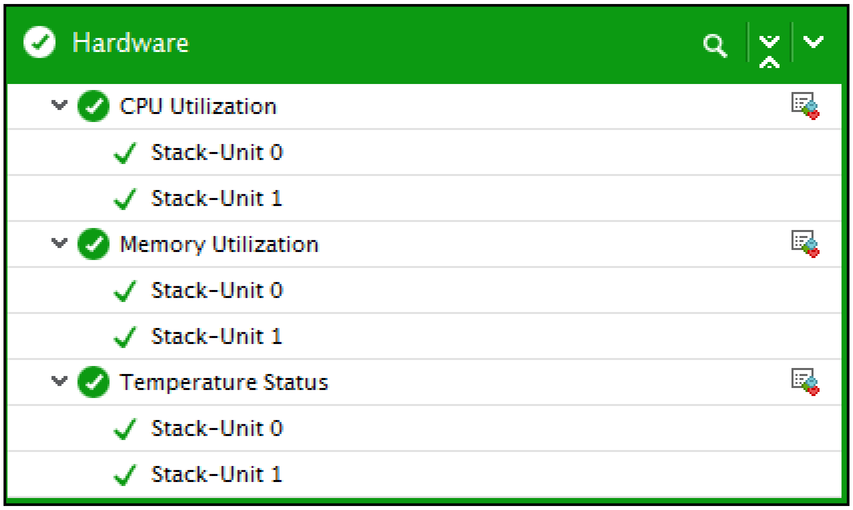


Figure 3.2: The tests associated with the Hardware layer

The sections that follow discusses each test of this layer in detail.

3.1.1 CPU Utilization Test

This test auto-discovers the stack units of the Dell Switch M-Series, and monitors the current CPU utilization of each stack unit. If the stack unit is found to consume CPU resources excessively, then, this test will help administrators to determine when exactly did the CPU utilization peak - during the last 5 sec? or 1 minute? or 5 minutes? This revelation helps administrators troubleshoot the CPU spikes better.

Target of the test : Dell Switch M-Series

Agent deploying the test : An external Agent

Outputs of the test : One set of results for every stack unit in the Dell Switch M-Series monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the monitored target exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.

6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.

7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.

8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.

9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.

10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm

11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.

12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:

    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard

13. **ENCRYPTPASSWORD**– Specify the encryption password here.

14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.

15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU usage in last 5sec:	Indicates the percentage of CPU utilization of this stack unit during last 5 seconds.	Percent	By comparing the values of these measures, you can quickly figure out when exactly was the CPU usage maximum. Using this analysis, administrators can further investigate the real reason behind the sudden spike in the CPU usage.
CPU usage in last 1min:	Indicates the percentage of CPU utilization of this stack unit during last 1 minute.	Percent	
CPU usage in last 5min:	Indicates the percentage of CPU utilization of this stack unit during last 5 minutes.	Percent	

3.1.2 Fan Status Test

This test reports the current operational state of the fan available in each stack unit of the Dell Switch M-Series. Using this test, administrators can identify the fan that is down and rectify the same well before the stack unit starts malfunctioning.

Target of the test : Dell Switch M-Series

Agent deploying the test : An external Agent

Outputs of the test : One set of results for every stack unit in the Dell Switch M-Series monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection

in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.

15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td><b>Fan status:</b></td><td>Indicates the current status of the fan available in this stack unit.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Up</td><td>1</td></tr>
<tr><td>Down</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b> s listed in the table above to indicate the current status of the fan in each stack unit. The graph of this measure however, represents the status of the fan using the numeric equivalents only - 1 to 2.</td></tr>
</table>

3.1.3 Temperature Status Test

This test auto-discovers the stack units of the Dell Switch M-Series and reports the current temperature of each stack unit. By carefully analyzing the temperature of the stack units, administrators can figure out the stack units that are malfunctioning due to the temperature being out of the admissible range.

Target of the test : Dell Switch M-Series

Agent deploying the test : An external Agent

Outputs of the test : One set of results for every stack unit in the Dell Switch M-Series monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.

12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Temperature:	Indicates the current temperature of this stack unit.	Celsius	Ideally, the temperature should be well within admissible range. A sudden / gradual increase /decrease in the temperature is a cause of concern and warrants the immediate attention of the administrator.

3.1.4 Memory Utilization Test

This test auto-discovers the stack units of the Dell Switch M-Series and reports the memory utilization of each stack unit. By comparing the memory usage statistics across the stack units, administrators can quickly identify the stack unit that is currently running out of space.

Target of the test : Dell Switch M-Series

Agent deploying the test : An External Agent

Outputs of the test : One set of results for every stack unit in the Dell Switch M-Series monitored

Configurable parameters for the test

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

2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:

- **DES** – Data Encryption Standard
- **AES** – Advanced Encryption Standard

13. **ENCRYPTPASSWORD**– Specify the encryption password here.

14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.

15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total memory:	Indicates the total amount of memory allocated for this stack unit.	MB	
Utilized memory:	Indicates the amount of memory that is utilized by this stack unit.	MB	A low value is desired for this measure. A value close to the *Total memory* measure indicates that the memory resources are depleting rapidly.
Available free memory:	Indicates the amount of memory that is currently available for use in this stack unit.	MB	A high value is desired for this measure.
Memory utilization:	Indicates the percentage of memory utilized by this stack unit.	Percent	A low value is desired for this measure. A high value or a consistently increasing value is a cause of concern, as it could indicate a gradual erosion of memory in the stack unit. In such cases, you may want to resize the stack unit or investigate the cause of memory erosion and find a way to arrest the memory erosion.

3.1.5 Power Supply Status Test

This test reveals the current status of the power supply unit available in each stack unit of the Dell Switch M-Series.

Target of the test : Dell Switch M-Series

Agent deploying the test : An external Agent

Outputs of the test : One set of results for every stack unit in the Dell Switch M-Series monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.

10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm

11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.

12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:

    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard

13. **ENCRYPTPASSWORD**– Specify the encryption password here.

14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.

15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

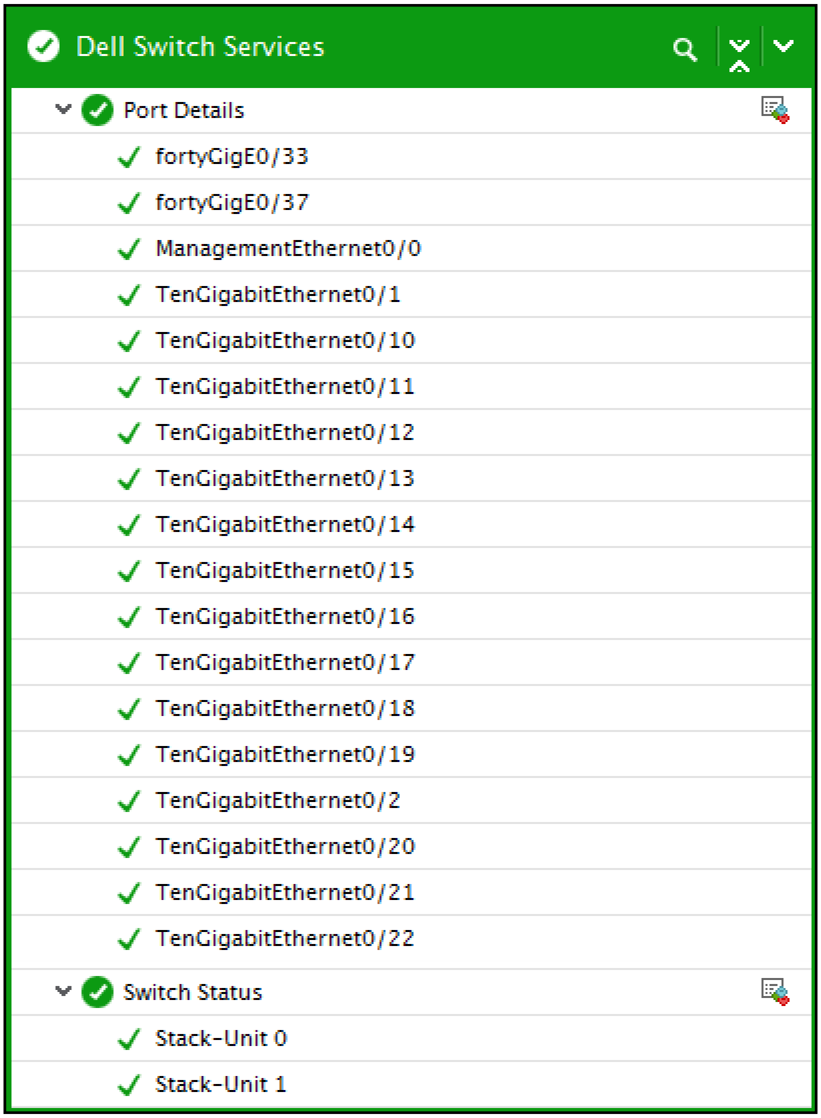
Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td><b>PS Status:</b></td><td>Indicates the current status of the power supply unit available in this stack unit.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Warning</td><td>2</td></tr>
<tr><td>Critical</td><td>3</td></tr>
<tr><td>Shutdown</td><td>4</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Not present</td><td>5</td></tr>
<tr><td>Not functioning</td><td>6</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b> s listed in the table above to indicate the current status of the power supply unit in this stack unit. The graph of this measure however, represents the status of the power supply using the numeric equivalents only - 1 to 6.
</td></tr>
</table>

3.2 The Dell Switch Services layer

This layer helps administrators to track the current administrative and operational status of each port available in the Dell Switch M-series. Also, administrators can determine the current status of the switch in each stack unit.



Dell Switch Services

Port Details

- ✓ fortyGigE0/33
- ✓ fortyGigE0/37
- ✓ ManagementEthernet0/0
- ✓ TenGigabitEthernet0/1
- ✓ TenGigabitEthernet0/10
- ✓ TenGigabitEthernet0/11
- ✓ TenGigabitEthernet0/12
- ✓ TenGigabitEthernet0/13
- ✓ TenGigabitEthernet0/14
- ✓ TenGigabitEthernet0/15
- ✓ TenGigabitEthernet0/16
- ✓ TenGigabitEthernet0/17
- ✓ TenGigabitEthernet0/18
- ✓ TenGigabitEthernet0/19
- ✓ TenGigabitEthernet0/2
- ✓ TenGigabitEthernet0/20
- ✓ TenGigabitEthernet0/21
- ✓ TenGigabitEthernet0/22

Switch Status

- ✓ Stack-Unit 0
- ✓ Stack-Unit 1

Figure 3.3: The tests associated with the Dell Switch Services layer

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

3.2.1 Switch Status Test

The Dell Switch M-series allows connecting up to six Dell Force10 MXL switches using QSFP+ (40Gb) ports to create a single stack unit. In the stack unit so created, a single switch acts as a Master and controls other switches thereby allowing users to manage and configure the member switches and ports using a single IP address. This IP address is copied from the Master to the Standby when the Standby is created. If for any reason the Master fails and the Standby takes over as the Master, the IP address of the stack unit will remain the same, thus allowing continuous management of the stack unit. Fatal failure of the switches due to erratic power fluctuations or physical damage can render the stack unit unavailable/inoperable which in turn causes difficulties in managing the network connections. To avoid such issues, administrators should monitor the stack units at regular intervals. This is where the **Switch Status** test aids administrators!

Using this test, administrators are able to determine the current switch status of each stack unit in the Dell Switch M-Series.

Target of the test : Dell Switch M-Series

Agent deploying the test : An external Agent

Outputs of the test : One set of results for every stack unit in the Dell Switch M-Series monitored.

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose

between the following options:

- **MD5** – Message Digest Algorithm
- **SHA** – Secure Hash Algorithm

11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td><b>Status:</b></td><td>Indicates the current switch status of this stack unit.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Ok</td><td>1</td></tr>
<tr><td>Not Supported</td><td>2</td></tr>
<tr><td>Code mismatch</td><td>3</td></tr>
<tr><td>Config mismatch</td><td>4</td></tr>
<tr><td>Unit down</td><td>5</td></tr>
<tr><td>Not present</td><td>6</td></tr>
</table>
</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Note: By default, this measure reports the **Measure Value** s listed in the table above to indicate the current switch status of the stack unit. The graph of this measure however, represents the status of the fan using the numeric equivalents only - 1 to 6.

3.2.2 Port Details Test

The Dell Switch M-Series comprises of multiple ports through which multiple network connections are established. This test auto discovers the ports on the Dell Switch M-Series, and reports the current administrative state and operational state of each port. In addition, this test also reveals the strength of the power signals that are received and transmitted through each port. This way, administrators can be proactively alerted to transmission / reception of weak signals, and in the process, they can initiate remedial measures before connection failures occur.

Target of the test : Dell Switch M-Series

Agent deploying the test : An external Agent

Outputs of the test : One set of results for every port on the Dell Switch M-Series being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG

agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.

7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.

8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.

9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.

10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm

11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.

12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:

    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard

13. **ENCRYPTPASSWORD**– Specify the encryption password here.

14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.

15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td><b>Administrative status:</b></td><td>Indicates the current administrative status of this port.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Up</td><td>1</td></tr>
<tr><td>Down</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current administrative status of the port. The graph of this measure however, represents the status of the fan using the numeric equivalents only - 1 and 2.</td></tr>
<tr><td><b>Operational status:</b></td><td>Indicates the current operational status of this port.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Ready</td><td>1</td></tr>
<tr><td>Port down</td><td>2</td></tr>
<tr><td>Port problem</td><td>3</td></tr>
<tr><td>Card problem</td><td>4</td></tr>
<tr><td>Card down</td><td>5</td></tr>
<tr><td>Not present</td><td>6</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current switch status of the stack unit. The graph of this measure however, represents the current operation status of the port using the numeric equivalents only - 1 to 6.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Received power signal:	Indicates the strength of the power signal received through this port.	dB	
Transmitted power signal:	Indicates the strength of the power signal transmitted through this port.	dB	
Received temperature:	Indicates the current temperature reading of this port.	Celsius	Ideally, the temperature of the port should be well within admissible limits.

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 **Dell Switch M-Series**. 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.