Monitoring Dlink DGS Switch

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Dlink DGS-3100 series switches are managed Layer 2 Gigabit stackable that support up to 6 stack units. These switches provide wide-ranging port densities and up to 20Gbps physical stacking. A stack can consist of 10/100/1000Mbps switches, 10/100/1000Mbps PoE switches, or a combination of both types, with up to 96 SFP fibre links.DGS-3100 stack provides the D-Link Safeguard Engine function to increase the switch's reliability and availability. Jumbo Frame support is designed to enhance Ethernet networking throughput and significantly reduce the CPU utilization of large file transfers like large multimedia files or large data files by enabling more efficient larger payloads per packets.

If the switches malfunction or do not respond due to overutlization/failure of core components, 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 Dlink DGS Switch using the dedicated monitoring offered by eG Enterprise.

Chapter 1: How to Monitor Dlink DGS Switch Using eG Enterprise?

eG Enterprise monitors the Dlink DGS Switch using an eG external agent. This agent can be deployed on any remote host in the environment. This agent is capable of monitoring the performance of the switch by polling the SNMP-MIB of the switch at regular intervals. Ensure that the Dlink DGS Switch is SNMP-enabled before you start monitoring the target switch.

1.1 Managing the Dlink DGS Switch

eG Enterprise can automatically discover the Dlink DGS Switch, and also lets to manually add the component for monitoring using eG admin interface. To manage a Dlink DGS Switch component, do the following:

1. Log into the eG admin interface.
2. If the Dlink DGS Switch is already discovered, then directly proceed towards managing the broker using the **COMPONENTS – MANAGE/UNMANAGE** page.
3. However, if you are yet to discover the Dlink DGS Switch, then run discovery (Infrastructure -> Components -> Discover) or follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu to manually add the component using the **Components** page.
4. Click on the **Add new Component** button after choosing the *Dlink DGS Switch* from the **Component Type** drop down list in the **Components** page. This will lead you to the **Add Component** page (Figure 1.1). Remember that components manually added are managed automatically.

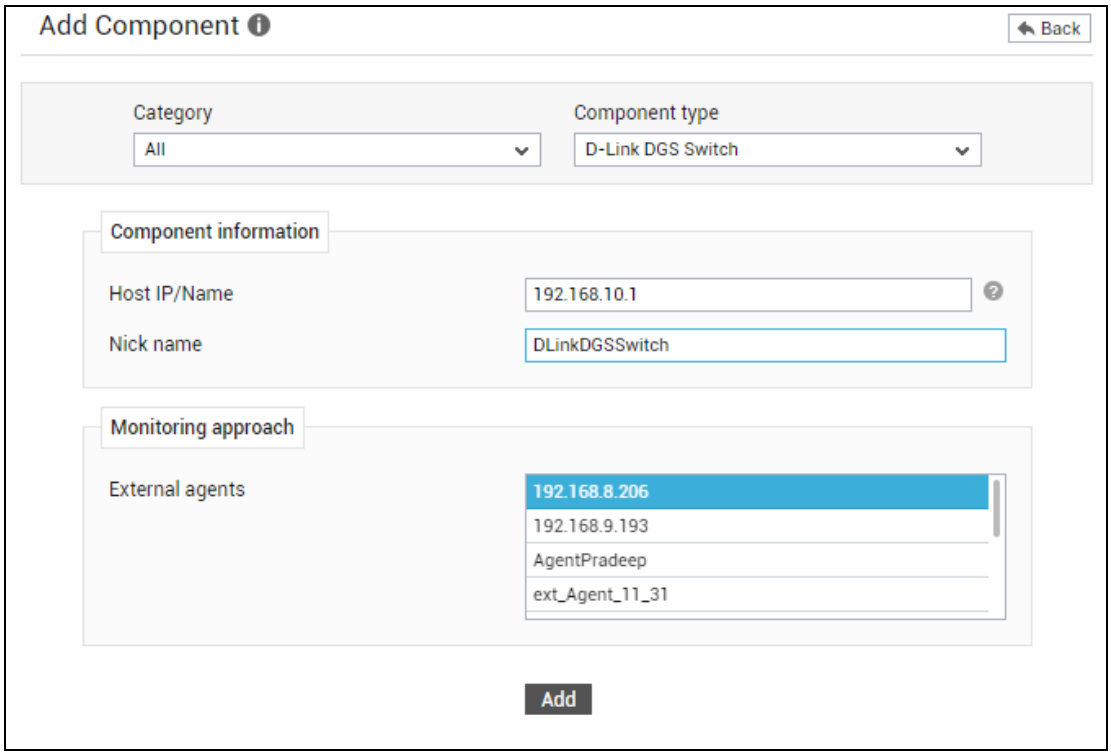
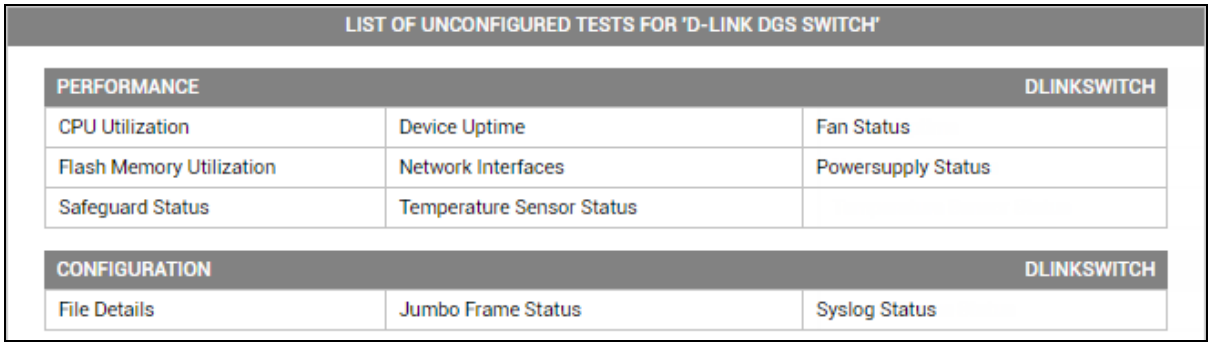


Figure 1.1: Adding a Dlink DGS Switch component

5. Specify the **Host IP/Name** and the **Nick name** of the Dlink DGS Switch in Figure 1.1.
6. Then, pick an external agent from the **External agents** list box and click the **Add** button to add the component for monitoring.
7. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 1.2.



LIST OF UNCONFIGURED TESTS FOR 'D-LINK DGS SWITCH'

PERFORMANCE		DLINKSWITCH
CPU Utilization	Device Uptime	Fan Status
Flash Memory Utilization	Network Interfaces	Powersupply Status
Safeguard Status	Temperature Sensor Status	

CONFIGURATION		DLINKSWITCH
File Details	Jumbo Frame Status	Syslog Status

Figure 1.2: List of Unconfigured tests to be configured for the Dlink DGS Switch

8. To configure the tests, click on the CPU Utilization test in Figure 1.2. To know how to configure the test, refer to Section **1.1.1**.

9. Once the tests are configured, signout of the eG admin interface.

Chapter 1: Monitoring Dlink DGS Switch

eG Enterprise has developed a dedicated *Dlink DGS Switch* monitoring model. This model periodically checks the flash memory utilization, the CPU utilization and the status of Safeguard Engine, fan and temperature sensor on each stack unit of the target switch. This way, abnormalities can be detected and rectified before any irreparable damage occurs.

Figure 1.1: The layer model of the Dlink DGS Switch

Every layer of Figure 1.1 is mapped to a variety of tests which connect to the SNMP MIBs of the target switch 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 at various time intervals?
- What is the current status of each fan available in each stack unit?
- How well the flash memory is being utilized on each stack unit?
- What is the current status of the power supply unit within each stack unit?
- What is the current status of the temperature sensor in each stack unit?
- Is the Safeguard Engine enabled on the stack unit?
- Is the Safeguard Engine in idle state?
- What is the current status of each stack unit?

1.1 Operating System Layer

Using this layer administrators can track the CPU utilization and flash memory utilization of each stack unit available in the Dlink DGS Switch. In addition, administrators can also track the status of the fan, temperature sensor and Safeguard Engine (if enabled) in each stack unit.

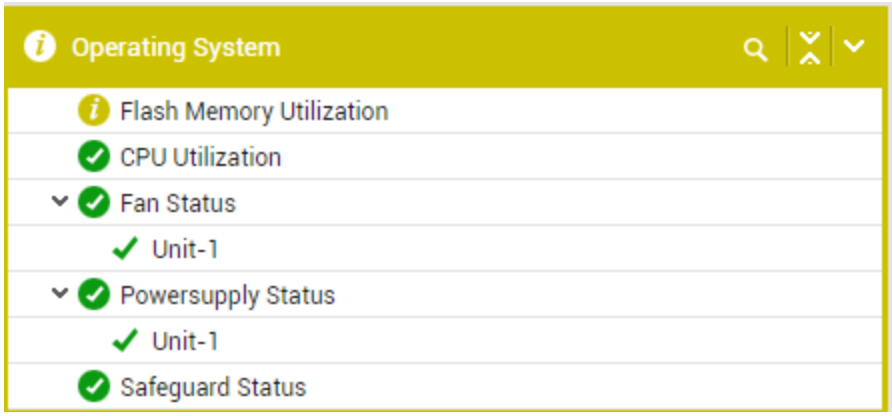


Figure 1.2: The tests associated with the Operating System layer

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

1.1.1 CPU Utilization Test

This test auto-discovers the stack units of the Dlink DGS switch, and monitors the current CPU utilization of each stack unit if the CPU utilization monitoring is enabled for the 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 1 sec? or 1 minute? or 5 minutes? This revelation helps administrators troubleshoot the CPU spikes better.

Target of the test : A Dlink DGS Switch

Agent deploying the test : An external Agent

Outputs of the test : One set of results for each *stack unit* in the Dlink DGS Switch to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection

Parameter	Description
	in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Is CPU utilization enabled ?	Indicates whether/not CPU utilization monitoring is enabled for this stack unit.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** Yes / 1 No / 2 **Note:** By default, this measure reports the **Measure Value**s listed in the table

Measurement	Description	Measurement Unit	Interpretation
			above to indicate whether the CPU utilization monitoring is enabled for each stack unit. The graph of this measure however, represents the status of the fan using the numeric equivalents only - 1 to 2.
CPU utilization for last 1 second	Indicates the percentage of CPU utilization of this stack unit during last 1 second.	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 utilization for last 1 minute	Indicates the percentage of CPU utilization of this stack unit during last 1 minute.	Percent	
CPU utilization for last 5 minutes	Indicates the percentage of CPU utilization of this stack unit during last 5 minutes.	Percent	

1.1.2 Fan Status Test

This test reports the current operational state of each fan available in each stack unit of the Dlink DGS switch. 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 : A Dlink DGS Switch

Agent deploying the test : An external Agent

Outputs of the test : One set of results for each *stack unit* in the Dlink DGS Switch monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.

Parameter	Description
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Fan 1 status	Indicates the current status of fan 1 in this stack unit.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** Normal / 1

<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>Shutdown</td><td>4</td></tr>
<tr><td>Not present</td><td>5</td></tr>
<tr><td>Not functioning</td><td>6</td></tr>
<tr><td>Warning</td><td>7</td></tr>
<tr><td>Critical</td><td>8</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of fan 1 in each stack unit. The graph of this measure however, represents the status of the fan using the numeric equivalents only.
</td></tr>
<tr><td>Fan 2 status</td><td>Indicates the current status of fan 2 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>Shutdown</td><td>4</td></tr>
<tr><td>Not present</td><td>5</td></tr>
<tr><td>Not functioning</td><td>6</td></tr>
<tr><td>Warning</td><td>7</td></tr>
<tr><td>Critical</td><td>8</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of
</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>fan 2 in each stack unit. The graph of this measure however, represents the status of the fan using the numeric equivalents only.</td></tr>
<tr><td>Fan 3 status</td><td>Indicates the current status of fan 3 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>Shutdown</td><td>4</td></tr><tr><td>Not present</td><td>5</td></tr><tr><td>Not functioning</td><td>6</td></tr><tr><td>Warning</td><td>7</td></tr><tr><td>Critical</td><td>8</td></tr></table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of fan 3 in each stack unit. The graph of this measure however, represents the status of the fan using the numeric equivalents only.</td></tr>
<tr><td>Fan 4 status</td><td>Indicates the current status of fan 1 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></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>Shutdown</td><td>4</td></tr>
<tr><td>Not present</td><td>5</td></tr>
<tr><td>Not functioning</td><td>6</td></tr>
<tr><td>Warning</td><td>7</td></tr>
<tr><td>Critical</td><td>8</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of fan 4 in each stack unit. The graph of this measure however, represents the status of the fan using the numeric equivalents only.
</td></tr>
<tr><td>Fan 5 status</td><td>Indicates the current status of fan 5 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>Shutdown</td><td>4</td></tr>
<tr><td>Not present</td><td>5</td></tr>
<tr><td>Not functioning</td><td>6</td></tr>
<tr><td>Warning</td><td>7</td></tr>
<tr><td>Critical</td><td>8</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of
</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			fan 5 in each stack unit. The graph of this measure however, represents the status of the fan using the numeric equivalents only.

1.1.3 Flash Memory Utilization Test

This test auto-discovers the stack units of the Dlink DGS Switch and reports the flash 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 : A Dlink DGS Switch

Agent deploying the test : An external Agent

Outputs of the test : One set of results for each *stack unit* in the Dlink DGS Switch to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total flash memory	Indicates the total amount of flash memory allocated for this stack unit.	MB	
Used flash memory	Indicates the amount of flash memory that is utilized by this stack unit.	MB	A low value is desired for this measure. A value close to the *Total flash memory* measure indicates that the memory resources are depleting rapidly.
Free flash memory	Indicates the amount of flash memory that is currently available for use in this stack unit.	MB	A high value is desired for this measure.
Flash memory utilization	Indicates the percentage of flash 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 flash 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.

1.1.4 Powersupply Status Test

This test reveals the current status of the power supply unit available in each stack unit of the Dlink DGC Switch.

Target of the test : A Dlink DGS Switch

Agent deploying the test : An external Agent

Outputs of the test : One set of results for each *stack unit* in the Dlink DGS Switch monitored.

Configurable parameters for the test

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

Parameter	Description
	contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related

Parameter	Description
	to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of the power supply unit in this stack unit.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** Normal – 1 Shutdown – 4 Not present – 5 Not functioning – 6 Warning – 7 Critical – 8 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current status of the power supply in each stack unit. The graph of this measure however, represents the measure values using the numeric equivalents only.

1.1.5 Safeguard Status Test

Safeguard Engine is a feature designed to enhance the robustness of switches, and increase overall network reliability and availability by identifying bulk traffics, throttling unwanted interruption, and protecting switch operation. Safeguard Engine effectively protects switches against abnormal bulks of traffic caused by virus infection or worm scanning. With Safeguard Engine, D-Link DGS Switch can identify and prioritize CPU-intensive applications traffic, throttle interruption, and protect switch

operation. When CPU utilization is exceed the set threshold, the Safeguard Engine will take action to prevent the over-use of switch resources by stop receiving the ARP packets or by minimizing the bandwidth for ARP packets. This way, the Safeguard Engine not only ensures the stability of the target switch, but also provides high availability of network. If the Safeguard Engine is not enabled on the switch or in idle state, then the resource utilization on the switch may become uncontrollable when the switch is processing intensive application traffic. To avoid such eventualities, it is necessary for administrators to continuously track the status of the Safeguard Engine on the stack unit of the target switch. This can be easily achieved using the **Safeguard Status** test!

This test continuously monitors the stack units of the target switch and reveals whether the Safeguard Engine is enabled on each stack unit. In the process, this test also reports the current status of the Safeguard Engine if it is enabled.

Target of the test : A Dlink DGS Switch

Agent deploying the test : An external Agent

Outputs of the test : One set of results for each *stack unit* in the Dlink DGS Switch monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Is safeguard engine enabled?	Indicates whether/not the Safeguard Engine is enabled for this stack unit.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** Yes – 1 No – 2 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate whether the Safeguard Engine is enabled for each stack unit. The graph of this measure however, represents the measure values using the numeric equivalents only.
Status	Indicates the current status of the Safeguard Engine.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Idle</td><td>0</td></tr><tr><td>Attack</td><td>1</td></tr></table> **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current status of the Safeguard Engine in each stack unit. The graph of this measure however, represents the measure values using the numeric equivalents only.

1.1.6 Temperature Sensor Status Test

This test auto-discovers the temperature sensor in each stack unit of the target Dlink DGS Switch and reports the current status of the temperature sensor. 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 : A Dlink DGS Switch

Agent deploying the test : An external Agent

Outputs of the test : One set of results for each *stack unit* in the Dlink DGS Switch monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.

Parameter	Description
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by

Parameter	Description
	default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current operational status of the temperature sensor in this stack unit.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** Ok – 1 Unavailable – 2 Not operational – 3 **Note:**

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure reports the **Measure Value**s listed in the table above to indicate the current operational status of the temperature sensor in each stack unit. The graph of this measure however, represents the measure values using the numeric equivalents only.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.