Monitoring XUPS Server

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The XUPs Series provides UPS backup with line-interactive automatic voltage regulation (AVR), over/under-voltage protection, surge protection with heavy duty noise filtering and communications capability.

Since this UPS plays a crucial role in protecting computers, data centers, telecommunication equipment or other electrical equipment, issues in its performance – eg., the depletion of the battery charge - can cause injuries, fatalities, serious business disruption or data loss. It is therefore imperative that the UPS is monitored periodically, and its 24 x 7 availability ensured.

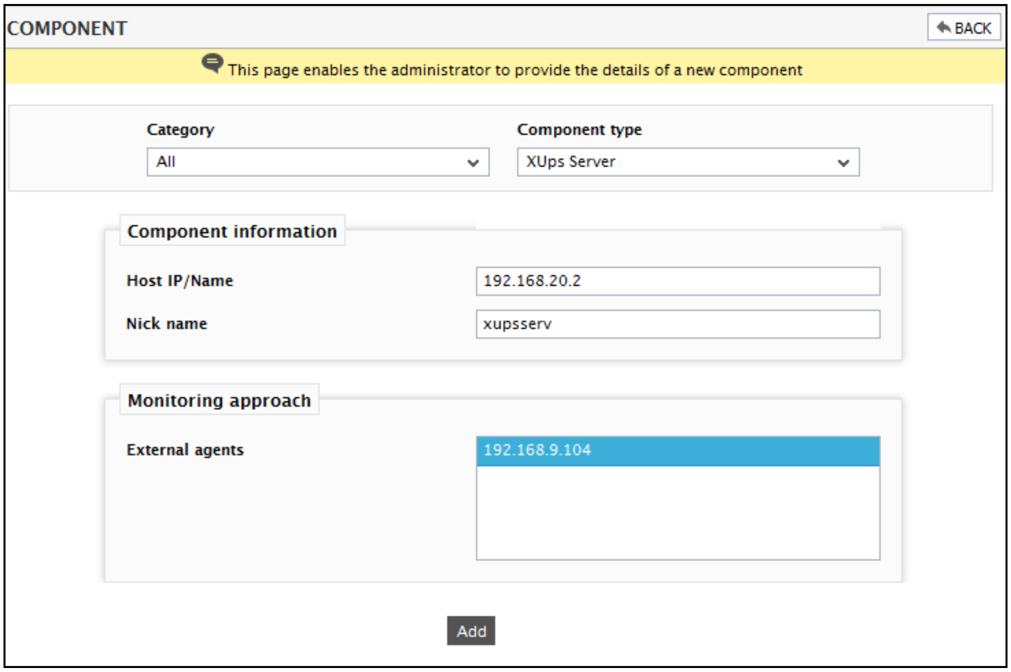
Chapter 2: How to Monitor XUPS Using eG Enterprise ?

eG Enterprise monitors the XUPS in an agentless manner. All that is required for this is a single eG agent on any remote Windows host in the environment. This agent periodically polls the SNMP MIB of the XUps server and gathers statistics related to its performance. To enable the eG agent to collect metrics, you should enable SNMP on the XUPS server.

2.1 Managing the XUps Server

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

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select XUps Server as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.



COMPONENT

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

Category: All

Component type: XUps Server

Component information

Host IP/Name: 192.168.20.2

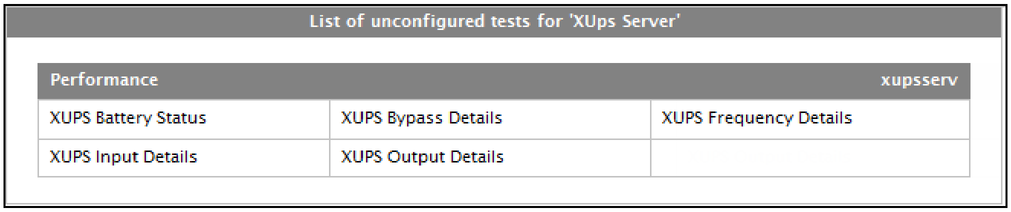
Nick name: xupsserv

Monitoring approach

External agents: 192.168.9.104

Figure 2.1: Adding a new XUps Server

4. Specify the **Host IP/Name** and the **Nick name** of the XUps Server in Figure 2.1. Then, click the **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests appears .

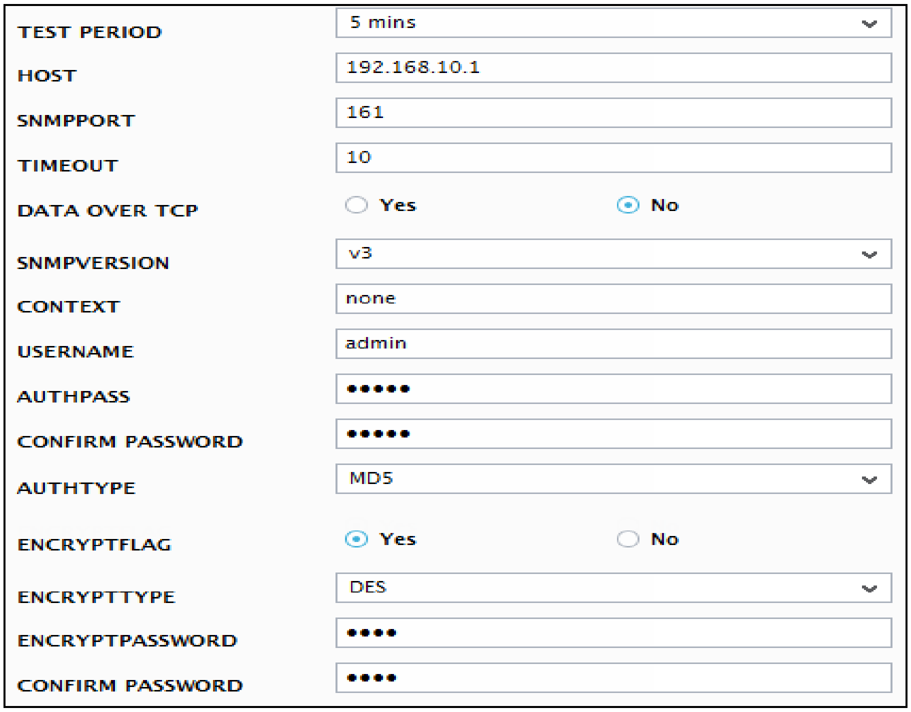


List of unconfigured tests for 'XUps Server'

Performance		xupsserv
XUPS Battery Status	XUPS Bypass Details	XUPS Frequency Details
XUPS Input Details	XUPS Output Details	

Figure 2.2: List of Unconfigured tests to be configured for the XUps Server

6. Click on any test in the list of unconfigured tests. For instance, click on the **XUPS Battery Status** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.



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

Figure 2.3: Configuring the XUPS Battery Status test

7. To know how to configure parameters, refer to **Monitoring the XUps**.
8. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the XUps

For this purpose, eG Enterprise provides a dedicated XUps Server monitoring model. By periodically polling the SNMP MIB of the XUps, the eG external agent collects a wealth of performance information pertaining to the device, and proactively reveals abnormalities (if any).

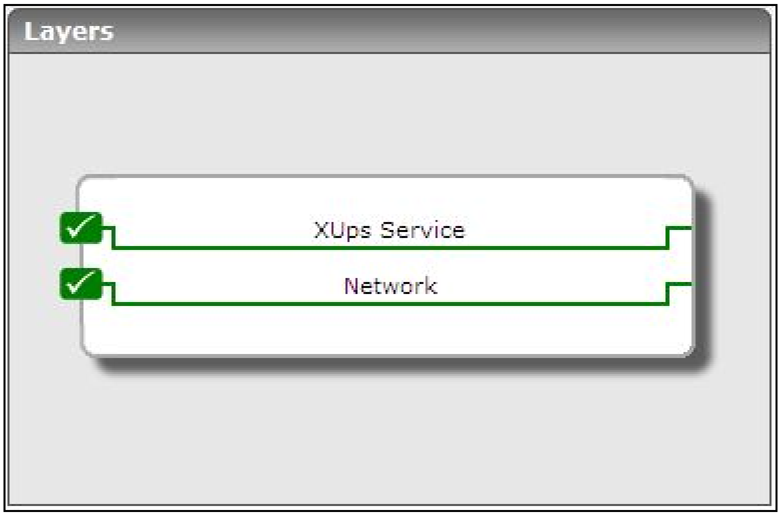


Figure 3.1: The XUps server monitoring model

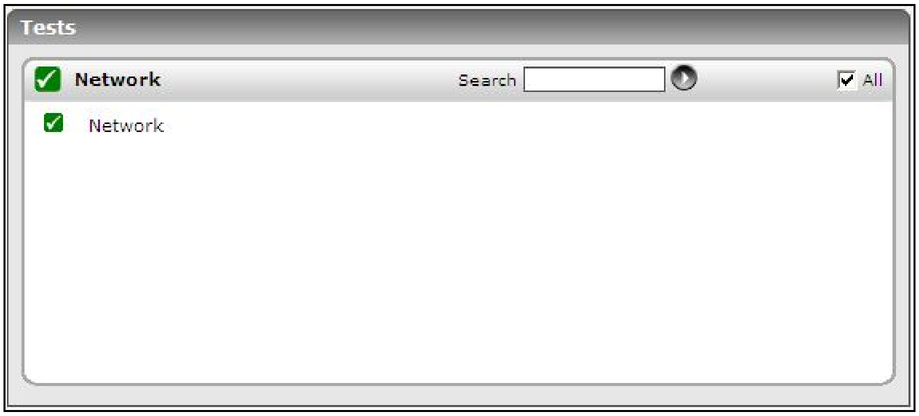
Each layer of Figure 4.1 above is mapped to a variety of tests, each of which periodically polls the SNMP MIB of the UPS to retrieve a plethora of statistics revealing the overall health of the device. These statistics enable administrators to figure out the following:

- What is the current status of the UPS battery?
- How long would it be before the UPS runs out of battery?
- How much charge is left on battery?
- What is the bypass voltage of the UPS?
- What is the current external source of input power and source of output power?
- Did input power exceed tolerance level more than once?
- Is the output load of the UPS too high?
- Is the input voltage and current within prescribed limits?
- Is the output voltage and current within prescribed limits?

The sections that follow will discuss each layer of the monitoring model in detail.

3.1 The Network Layer

To determine the health of network connections leading to and from the XUps, use the **Network** test mapped to this layer.


Tests

☑ Network Search ☑ All

☑ Network

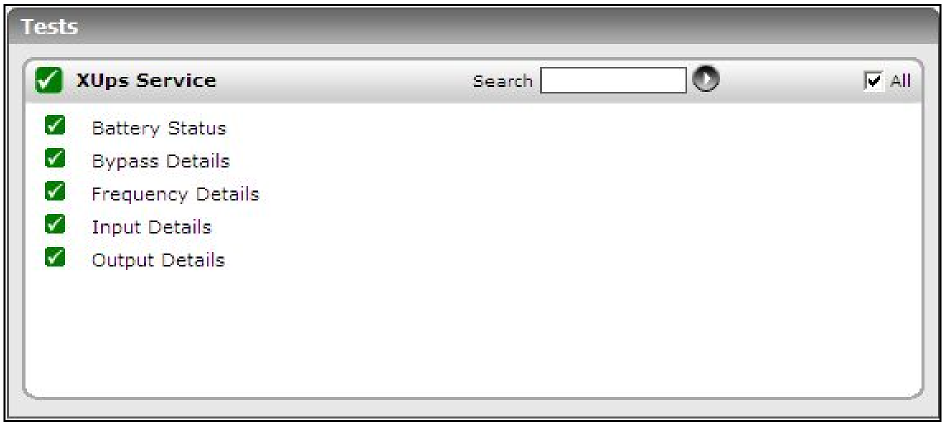
Figure 3.2: The test mapped to the Network layer

The **Network** test has been discussed in the *Monitoring Cisco Router* document, let us proceed to the next layer.

3.2 The XUps Service Layer

Using this layer, you can monitor the following:

- The status of the battery;
- The battery charge;
- The input and output frequency of the battery;
- The input and output voltage, current, and real power of the battery



Tests

☑ XUps Service   Search ____   ☑ All

- ☑ Battery Status
- ☑ Bypass Details
- ☑ Frequency Details
- ☑ Input Details
- ☑ Output Details

Figure 3.3: The tests mapped to the Battery Status layer

3.2.1 Battery Status Test

This test reports the status of the UPS battery, and also indicates whether or not the batter needs to be recharged.

Target of the test : An XUPS

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version

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

Parameter	Description
	- **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
Remaining battery time	Indicates the battery run time in seconds before UPS turns off due to low battery.	Status	A very low value for this measure could indicate that the UPS battery is fast running out of charge and may have to be recharged.
Battery voltage	Indicates the battery voltage.	Volts	
Battery current	Indicates the amount of power that is being conducted by the battery.	Amps	The status of the current is positive when discharging the battery and the status of the current is negative when recharging the battery.
Battery capacity	Indicates the charge of the battery in percentage.	Percent	A high value is typically desired for this measure. A very low value could indicate that the UPS battery is fast running out of charge and may have to be recharged.
Advanced battery mgmt status	Indicates the status of the Advanced Battery Management.	Number	This measure can take any of the following values:

<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>Description</th></tr>
<tr><td>1</td><td>Battery Charging</td></tr>
<tr><td>2</td><td>Battery Discharging</td></tr>
<tr><td>3</td><td>Battery Floating</td></tr>
<tr><td>4</td><td>Battery Resting</td></tr>
<tr><td>5</td><td>unknown</td></tr>
</table>
<b>Note:</b>
Typically, this measure will report one of the <b>Measure Values</b> listed in the table above to indicate the status of the Advanced Battery Management. The graph of this measure will be drawn using the measure values.
</td></tr>
</table>

3.2.2 Bypass Details Test

This test measures the bypass voltage of the UPS.

Target of the test : An XUPS

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
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 firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
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
Bypass voltage	Indicates the measured UPS bypass voltage in volts.	Volts	

3.2.3 Frequency Details Test

This test reports the input and output frequency, and provides the load details of the XUps.

Target of the test : An XUPS

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Input frequency	Indicates the utility line frequency in tenths of Hz.	Hz	
Bad input lines	Indicates the number of times the Input was out of tolerance.	Number	

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Output source</td><td>Indicates the current external source of input power.</td><td>Number</td><td>This measure can take any of the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>1</td><td>Other</td></tr>
<tr><td>2</td><td>None</td></tr>
<tr><td>3</td><td>PrimaryUtility</td></tr>
<tr><td>4</td><td>BypassFeed</td></tr>
<tr><td>5</td><td>SecondaryUtility</td></tr>
<tr><td>6</td><td>generator</td></tr>
<tr><td>7</td><td>flywheel</td></tr>
<tr><td>8</td><td>fuelcell</td></tr>
</table></td></tr>
<tr><td>Output frequency</td><td>Indicates the UPS output frequency in tenths of Hz.</td><td>Hz</td><td></td></tr>
<tr><td>Output load</td><td>Indicates the UPS output load in percent of rated capacity.</td><td>Percent</td><td></td></tr>
<tr><td>Output source</td><td>Indicates the current source of output power.</td><td>Number</td><td>This measure can take any of the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>1</td><td>Other</td></tr>
<tr><td>2</td><td>None</td></tr>
<tr><td>3</td><td>Normal</td></tr>
<tr><td>4</td><td>Bypass</td></tr>
<tr><td>5</td><td>Battery</td></tr>
<tr><td>6</td><td>Booster</td></tr>
<tr><td>7</td><td>Reducer</td></tr>
<tr><td>8</td><td>ParallelCapacity</td></tr>
<tr><td>9</td><td>ParallelRedundant</td></tr>
<tr><td>10</td><td>HighEfficiencyMode</td></tr>
</table></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Bypass frequency	Indicates the bypass frequency in tenths of Hz.	Hz	

3.2.4 Input Details Test

This test reports the input voltage and input current of the XUps.

arget of the test : An XUPS

Agent deploying the test : An external agent

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

Configurable parameters for the test

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

Parameter	Description
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.
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.

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Input voltage	Indicates the input voltage of the UPS.	Volts	
Input current	Indicates the input current of the UPS.	Amps	

3.2.5 Output Details Test

This test reports the output voltage, output current, and output watts of the UPS.

Target of the test : An XUPS

Agent deploying the test : An external agent

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

Configurable parameters for the test

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

Parameter	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Output voltage	Indicates the output voltage of the UPS.	Volts	
Output current	Indicates the output current of the UPS.	Amps	
Output watts	Indicates the real output power.	Watts	

About eG Innovations

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

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

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

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