



Monitoring Printers

eG Innovations Product Documentation

www.eginnovations.com



Table of Contents

CHAPTER 1: INTRODUCTION	1
CHAPTER 2: HOW TO MONITOR PRINTER USING EG ENTERPRISE?	2
2.1 Managing the Printer	2
CHAPTER 3: MONITORING PRINTERS	4
3.1 The Printer Service Layer	4
3.1.1 Printer Cover Test	5
3.1.2 Printer Inputs Test	7
3.1.3 Printer Outputs Test	10
3.2 The Printer Details Layer	12
3.2.1 Printer Errors Test	13
3.2.2 Printer PageCount Test	16
3.2.3 Printer Test	18
ABOUT EG INNOVATIONS	22

Table of Figures

Figure 2.1: Adding an Printer	3
Figure 3.1: The layer model of a Printer	4
Figure 3.2: Tests that run on the Printer Service layer	5
Figure 3.3: Tests executing on the Printer Details layer	13

Chapter 1: Introduction

Of all peripheral devices that can be used in an IT infrastructure, printers are the most frequently used, and hence, the most important. If a printer goes offline, then critical reports and documents cannot be printed until such time that it is switched back online. Since network printers are typically placed in a central location and shared by users across multiple locations, it would be impractical for some users and a bit time-consuming for others, to manually check the printer status time and again. Instead, if the current status of the printer and its core components such as the tray, cover, output bins etc., is automatically reported to a centralized console at pre-configured intervals, then administrators will come to know of abnormalities in printer operations as soon as they occur, and can initiate corrective measures soon after. This is possible only if a monitoring solution is employed to monitor the printer status at pre-set frequencies. This is where eG Enterprise helps administrators.

Chapter 2: How to Monitor printer Using eG Enterprise?

eG Enterprise monitors the Printer 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 is capable of polling the SNMP MIB Of the Printer at regular intervals and fetching the useful statistics related its performance.

2.1 Managing the Printer

The eG Enterprise cannot automatically discover the Printer. This indicates 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 Printer 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 *Printer* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

The screenshot shows the 'COMPONENT' page in the eG Enterprise interface. At the top, there is a 'COMPONENT' header and a 'BACK' button. Below this is a yellow banner with a speech bubble icon and the text: 'This page enables the administrator to provide the details of a new component'. The main form area contains two dropdown menus: 'Category' (set to 'All') and 'Component type' (set to 'Printer'). Below these are two sections: 'Component information' and 'Monitoring approach'. The 'Component information' section has two input fields: 'Host IP/Name' (containing '192.168.10.1') and 'Nick name' (containing 'print'). The 'Monitoring approach' section has an 'External agents' input field (containing '192.168.9.104'). At the bottom center of the form is an 'Add' button.

Figure 2.1: Adding an Printer

4. Specify the **Host IP/Name** and **Nick name** of the Printer as shown in Figure 2.1. Then, click on the **Add** button to register the changes.
5. Next, try to sign out of the eG administrative interface. Now, you will be prompted to configure the **Device Uptime** test. To know how to configure this test, refer to Monitoring Cisco Router document.
6. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring Printers

eG Enterprise has designed a specialized Printer monitoring model (see Figure 3.1) that periodically runs status checks on the printer to determine its availability, monitors its key parts such as the printer cover, the tray, the output bin, the toner, the door, etc., for faults, and proactively alerts administrators to printer-related problems.

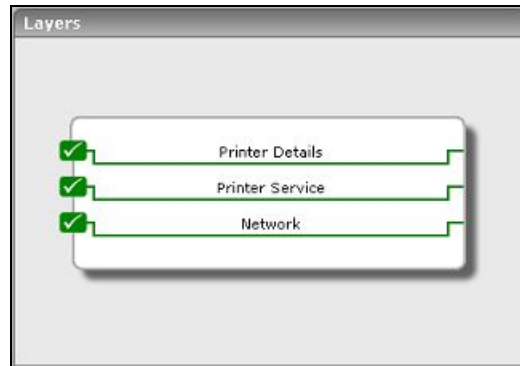


Figure 3.1: The layer model of a Printer

The **Network** layer depicted by Figure 3.1 has been discussed in the *Monitoring Unix and Windows Servers* document. The sections to come therefore, will discuss only the top 2 layers of Figure 3.1.

3.1 The Printer Service Layer

Using the tests associated with this layer, administrators can determine the following (see Figure 3.2):

- Is the printer cover closed?
- Are the input trays available?
- Has paper been fed into the input trays?
- Are the output bins available?



Figure 3.2: Tests that run on the Printer Service layer

3.1.1 Printer Cover Test

This test provides the status of every cover available in the printer.

Target of the test : A Printer

Agent deploying the test : An external agent

Outputs of the test : One set of results for the printer being 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

Parameter	Description
	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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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 cover closed (Critical Warning)	Indicates whether a particular cover is closed	Boolean	A value of 0 indicates that the cover is open. If the value is 1, it means that the cover is closed.

Note:

This measure is available only for printers with covers.

3.1.2 Printer Inputs Test

This test reports statistics relating to a printer's input trays.

Target of the test : A Printer

Agent deploying the test : An external agent

Outputs of the test : One set of results for the printer being 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.

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 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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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	Measurement
Input device availability (Critical warning)	Indicates whether a particular tray is available for printing	Boolean	<p>A value of 0 indicates that the tray is not available for printing and the value 1 indicates that the tray is available for printing.</p> <p>Availability problems can be caused by various factors including paper unavailability, paper jam, etc.</p>	
Is tray idle (Non Critical warning)	Indicates whether the tray is idle or	Boolean	While a value of 1 indicates that the tray is idle, value of 0 denotes that the tray is busy with some printing job	

Measurement	Description	Measurement Unit	Interpretation	Measurement
	busy			
Is paper available in tray (Critical warning)	Indicates whether the tray has paper or not	Boolean	A value of 0 indicates that the tray does not have paper to print. A value of 1, suggests that the tray has paper to print.	

3.1.3 Printer Outputs Test

This test reports statistics relating to each of the output bins of a printer.

Target of the test : A Printer

Agent deploying the test : An external agent

Outputs of the test : One set of results for the printer being 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

Parameter	Description
	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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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

Parameter	Description
	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		Measurement Unit	Interpretation
Output device availability (Non-critical warning)	Indicates whether the output bin is available or not.	Boolean	A value of 0 indicates that the output bin is not available and a value of 1 indicates that it is available.
Is output bin idle (Non-critical warning)	Indicates whether the output bin is busy or idle	Boolean	A value of 0 indicates that the bin is busy and a value of 1 indicates that it is idle.

Note:

These measures are available only for printers that support output bins.

3.2 The Printer Details Layer

This layer promptly notifies administrators when printer errors occur, or when the printer suddenly goes offline. The layer also helps administrators judge how effectively the printer was utilized by reporting the number of pages that have been printed using the printer.



Figure 3.3: Tests executing on the Printer Details layer

3.2.1 Printer Errors Test

This test indicates whether a particular measure generates a Critical warning or a Non-critical warning. A Critical warning is indicative of a problem so severe, that the printer is rendered unavailable until the warning is attended to. A Non-critical warning is one wherein the printer will continue to remain available despite the warning.

Target of the test : A Printer

Agent deploying the test : An external agent

Outputs of the test : One set of results for the printer being 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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • DES – Data Encryption Standard

Parameter	Description
	<ul style="list-style-type: none"> • 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 paper available (Critical warning)	Indicates the availability of papers in all trays	Boolean	A value of 0 indicates that there are no papers in any of the trays. If the value is 1, it means that papers are available in at least one tray.
Toner capacity (Non-critical warning)	Indicates the status of the toner with respect to its capacity	Boolean	A value of 0 indicates that the toner capacity is low. However, if the value is 1 it indicates that there is adequate toner in the printer.
Is toner available (Critical warning)	Indicates whether a toner is available for printing or not	Boolean	<p>A value of 0 is indicative of either of the following scenarios:</p> <ul style="list-style-type: none"> • The toner cartridge is not physically present in the printer • The printer is out of toner <p>A value of 1, on the other hand, confirms the physical presence of the toner cartridge and its availability for printing.</p>

Measurement	Description	Measurement Unit	Interpretation
Paper flow status (Critical warning)	Indicates whether the flow of paper into and out of the printer is smooth	Boolean	A value of 0 indicates that there is a paper jam and a value of 1 indicates that the paper flow is smooth
Is online (Critical warning)	Indicates whether the printer is on line or off line.	Boolean	A value of 0 indicates that the printer is off line. If the value is 1, it denotes that the printer is on line
Is door closed (Critical warning)	Indicates the overall status of the doors/covers present in the printer Note: This measure is available only for printers with doors / covers.	Boolean	While a value of 0 indicates that the door is open, 1 indicates that it is closed.

3.2.2 Printer PageCount Test

This test monitors the usage of a printer.

Target of the test : A Printer

Agent deploying the test : An external agent

Outputs of the test : One set of results for the printer being 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	Description
	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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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

Parameter	Description
	<p>encryption types:</p> <ul style="list-style-type: none"> • 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
Pages printed	<p>Indicates the number of pages printed during the set test frequency</p> <p>For example, assume that the PrinterPageCount is set to execute every 60 seconds. During this time interval, if 3 pages are printed, then the Pages printed measure will return 3.</p>	Pages	The value "–1" indicates that the test is not able to generate measures. Any other value indicates the number of pages printed during the pre-defined time interval.

3.2.3 Printer Test

This test monitors the availability of a network printer.

Target of the test : A Printer

Agent deploying the test : An external agent

Outputs of the test : One set of results for the printer being 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 <i>none</i> .
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.

Parameter	Description
AuthType	<p>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:</p> <ul style="list-style-type: none"> • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
EncryptFlag	<p>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.</p>
EncryptType	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Is the printer service available	This shows whether the printer is available for	Boolean	A value of 0 indicates that the printer is not available for printing. A value of 1

Measurement	Description	Measurement Unit	Interpretation
	printing or not		<p>indicates that the printer is available for printing.</p> <p>A printer could be rendered unavailable if its off the network. This could be due to the following reasons:</p> <ul style="list-style-type: none">• A Power shut-down• Failure of the network connection <p>Similarly, a printer on the network can also become unavailable for printing. This could be owing to either of the following reasons:</p> <ul style="list-style-type: none">• The printer does not support snmp• The printer is in an "unknown" state

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.

Copyright © 2018 eG Innovations Inc. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations 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. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.