Monitoring BlackBerry Server

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The BlackBerry® Enterprise solution is a complete wireless platform that extends the benefits of data messaging and collaboration environments and other tools to mobile environments. The BlackBerry Enterprise solution provides push-based access to email; calendar, contacts, tasks and notes; instant messaging; web-based applications and services and enterprise applications. Many enterprises use the BlackBerry Enterprise server to provide their employees with mobile access to email and other enterprise applications. Figure 1.1 depicts the architecture of the BlackBerry Enterprise Server.

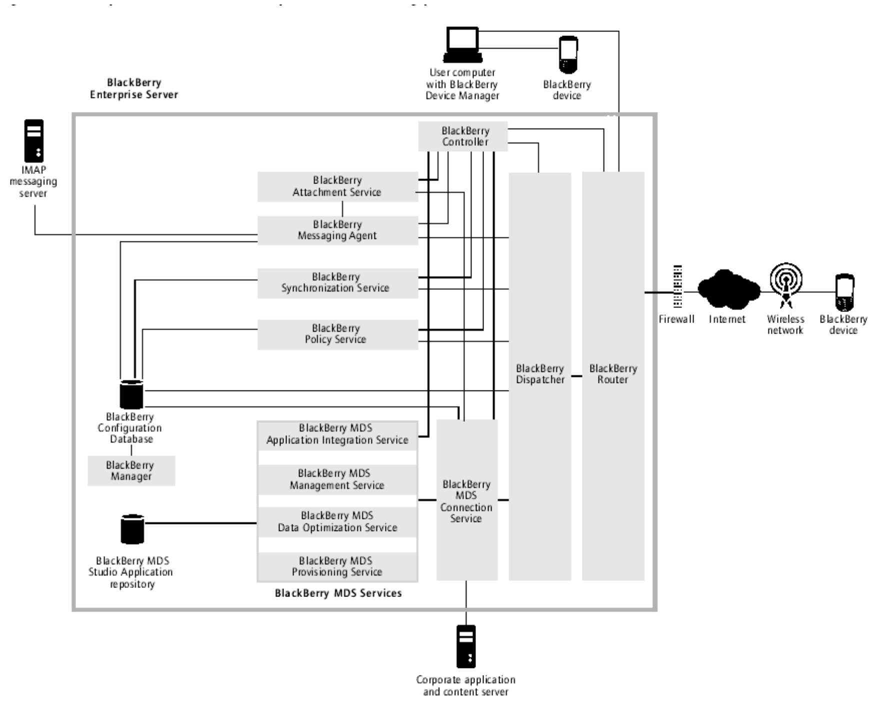
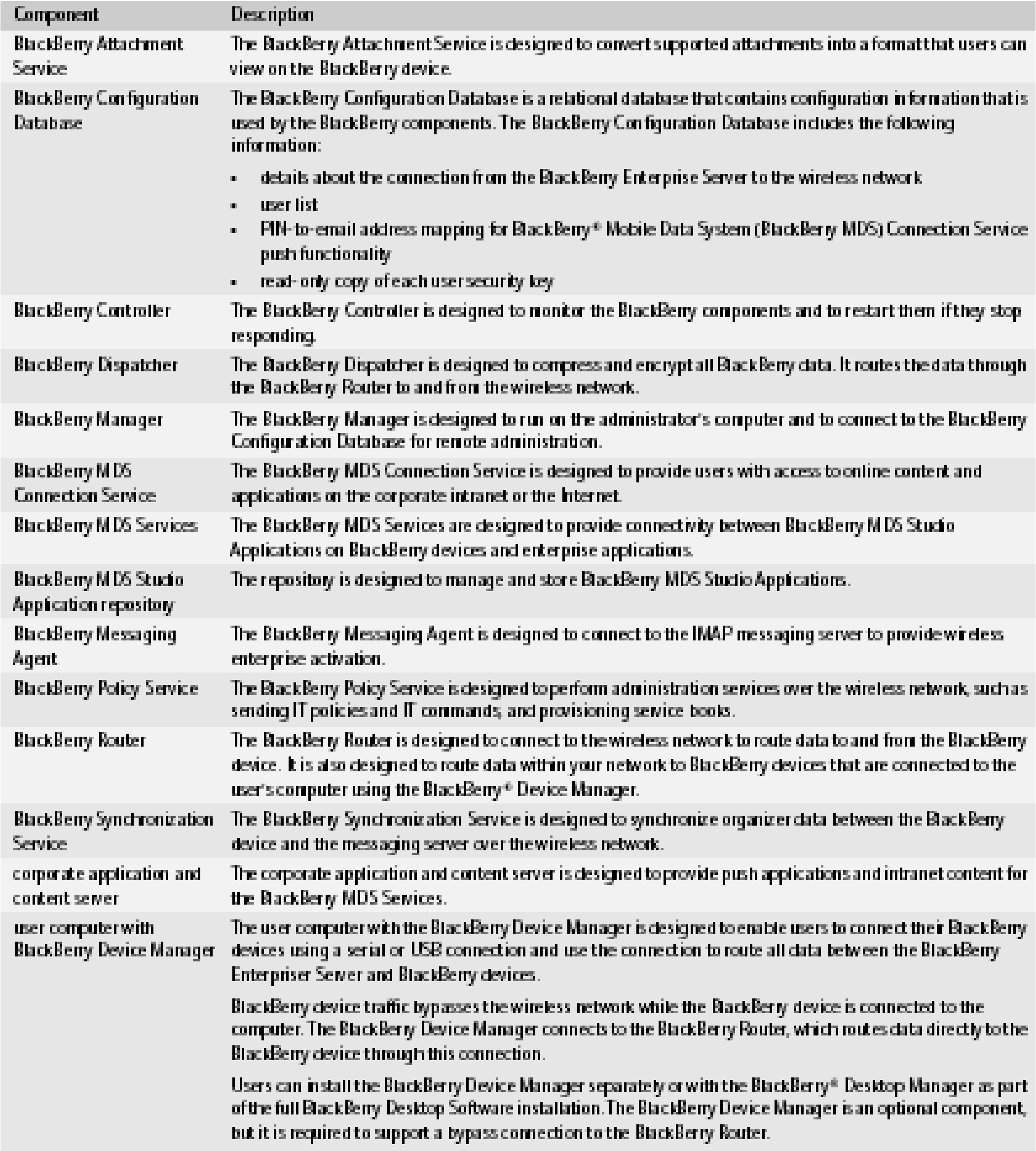

User computer with BlackBerry Device Manager
BlackBerry device
BlackBerry Enterprise Server
IMAP messaging server
BlackBerry Controller
BlackBerry Attachment Service
BlackBerry Messaging Agent
BlackBerry Synchronization Service
BlackBerry Policy Service
Firewall
Internet
Wireless network
BlackBerry device
BlackBerry Dispatcher
BlackBerry Router
BlackBerry Configuration Database
BlackBerry Manager
BlackBerry MDS Application Integration Service
BlackBerry MDS Management Service
BlackBerry MDS Data Optimization Service
BlackBerry MDS Provisioning Service
BlackBerry MDS Connection Service
BlackBerry MDS Studio Application repository
BlackBerry MDS Services
Corporate application and content server

Figure 1.1: Architecture of the BlackBerry Enterprise Server

As can be inferred from Figure 1.1, the BlackBerry® Enterprise Server consists of various services and components. The BlackBerry services are designed to provide data from enterprise applications to mobile users.The BlackBerry components are designed to monitor BlackBerry services, process, route, compress, and encrypt data, and communicate with the wireless network. The table below briefly describes some of the key components of the BES architecture.



Component	Description
BlackBerry Attachment Service	The BlackBerry Attachment Service is designed to convert supported attachments into a format that users can view on the BlackBerry device.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains configuration information that is used by the BlackBerry components. The BlackBerry Configuration Database includes the following information: ▪ details about the connection from the BlackBerry Enterprise Server to the wireless network ▪ user list ▪ PIN-to-email address mapping for BlackBerry® Mobile Data System (BlackBerry MDS) Connection Service push functionality ▪ read-only copy of each user security key
BlackBerry Controller	The BlackBerry Controller is designed to monitor the BlackBerry components and to restart them if they stop responding.
BlackBerry Dispatcher	The BlackBerry Dispatcher is designed to compress and encrypt all BlackBerry data. It routes the data through the BlackBerry Router to and from the wireless network.
BlackBerry Manager	The BlackBerry Manager is designed to run on the administrator's computer and to connect to the BlackBerry Configuration Database for remote administration.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service is designed to provide users with access to online content and applications on the corporate intranet or the Internet.
BlackBerry MDS Services	The BlackBerry MDS Services are designed to provide connectivity between BlackBerry MDS Studio Applications on BlackBerry devices and enterprise applications.
BlackBerry MDS Studio Application repository	The repository is designed to manage and store BlackBerry MDS Studio Applications.
BlackBerry Messaging Agent	The BlackBerry Messaging Agent is designed to connect to the IMAP messaging server to provide wireless enterprise activation.
BlackBerry Policy Service	The BlackBerry Policy Service is designed to perform administration services over the wireless network, such as sending IT policies and IT commands, and provisioning service books.
BlackBerry Router	The BlackBerry Router is designed to connect to the wireless network to route data to and from the BlackBerry device. It is also designed to route data within your network to BlackBerry devices that are connected to the user's computer using the BlackBerry® Device Manager.
BlackBerry Synchronization Service	The BlackBerry Synchronization Service is designed to synchronize organizer data between the BlackBerry device and the messaging server over the wireless network.
corporate application and content server	The corporate application and content server is designed to provide push applications and intranet content for the BlackBerry MDS Services.
user computer with BlackBerry Device Manager	The user computer with the BlackBerry Device Manager is designed to enable users to connect their BlackBerry devices using a serial or USB connection and use the connection to route all data between the BlackBerry Enterpriser Server and BlackBerry devices. BlackBerry device traffic bypasses the wireless network while the BlackBerry device is connected to the computer. The BlackBerry Device Manager connects to the BlackBerry Router, which routes data directly to the BlackBerry device through this connection. Users can install the BlackBerry Device Manager separately or with the BlackBerry® Desktop Manager as part of the full BlackBerry Desktop Software installation. The BlackBerry Device Manager is an optional component, but it is required to support a bypass connection to the BlackBerry Router.

Many enterprises use the BlackBerry Enterprise server to provide their employees with mobile access to email and other enterprise applications. Monitoring and management of the BlackBerry Enterprise server (BES) is important, since any failure with the mobile access system will result in hundreds of users losing access to critical enterprise applications. This is where eG Enterprise lends hands to administrators for continuously monitoring the BlackBerry Enterprise servers.

eG Enterprise offers two specialized models for monitoring the different versions of the BlackBerry Enterprise Server - while the *BlackBerry* model enables the monitoring of BlackBerry servers of versions less than 5 (i.e., v4.1 and lesser), the *BlackBerry 5x* model facilitates the monitoring of BlackBerry servers of version 5 (or its variants).

This document discusses both these models at length.

Chapter 2: How to Monitor the Blackberry Server using eG Enterprise?

The eG agent connects to the SNMP MIB of the BlackBerry server and extracts metrics of interest from it. For this, you need to make sure that the following requirements are done before attempting to monitor the Blackberry server;

- SNMP service should be installed and started on the BlackBerry server.
- You need to configure the SNMP Service of the BlackBerry host to accept SNMP packets from the BlackBerry application.

The procedure to install, start and configure the SNMP service on the Blackberry server is explained in the upcoming sections.

2.1 Install the SNMP Service and SNMP Management Tool

1. On the computer on which the BlackBerry server is installed, on the taskbar, click Control Panel -> Add/Remove Programs -> Add/Remove WindowsComponents -> Management and Monitoring Tools -> Details.
2. Install the SNMP service. See the Windows or Microsoft Windows Server™ documentation for more information.
3. To verify that the SNMP service was installed, perform one of the following actions:
4. Windows Server 2003: In Windows Services, verify that the SNMP service appears.
5. Windows 2000: On the taskbar, click Control Panel -> Add/Remove Programs -> Add/Remove Windows Components -> Management and Monitoring Tools -> Details. Verify that the SNMP service appears.
6. On the computer on which the BlackBerry server is installed, install the **SNMP management tool.**
7. Start the **SNMP** service and the **BlackBerry** Enterprise Server services.

2.2 Register the SNMP Agent

1. Verify that the correct SNMP registry keys were installed in the registry when you installed the BlackBerry Enterprise Server. If the keys were not installed automatically, create them manually.
2. If the version of the BlackBerry enterprise server is 3.5 or 3.6 then do the following to enable SNMP:

Registry Key	Value Type	Value Name	Value Data
HKEY_ LOCAL_ MACHINE\SOFTWARE\Research In Motion\ BlackBerry Enterprise Server\SNMPAgent\CurrentVersion	String Value	PathName	C:\Program Files\Research In Motion\BlackBerry Enterprise Server\BlackBerryServerSNMPAgent.dll
HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\SNMP\Parameters\ ExtensionAgents	String Value	Server	SOFTWARE\Research In Motion\BlackBerry Enterprise Server\SNMPAgent\CurrentVersion

3. Start the **SNMP** Service and the BlackBerry Enterprise Server.
4. Check the Event Viewer System Log for **SNMP** Service startup failures.
5. The BlackBerry Enterprise Server Management Information Base (MIB) is located in the BlackBerryServer.mib file in C:\Program Files\Research In Motion\BlackBerry Enterprise Server
6. Use a third-party SNMP browser (for example, Cisco Systems® Works 2000) to compile the MIB file.
7. If you created the SNMP registry keys manually, restart the **SNMP** service.

If the version of the BlackBerry enterprise server is 4.1 then do the following to enable SNMP:

1. Open the Registry Editor and go to **HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server**.
2. Right-click BlackBerry Enterprise Server, select New -> Key, and name it **SNMPAgent**.
3. Right-click **SNMPAgent**, select **New** -> **Key**, and name it **CurrentVersion**.
4. Right-click **CurrentVersion**, select **New** -> **String Value**, and name it **PathName**.
5. Right-click **PathName** and select **Modify**.
6. Under Value data, type C:\Program Files\Research In Motion\BlackBerry Enterprise Server\BlackBerryServerSNMPAgent.dll or point to the path where the **BlackBerryServerSNMPAgent.dll** file exists.
7. In the Microsoft Windows Control Panel, open **Administrative Tools > Services**.
8. Right-click **SNMP Service** and select **Restart**.

2.3 Set up the SNMP Service

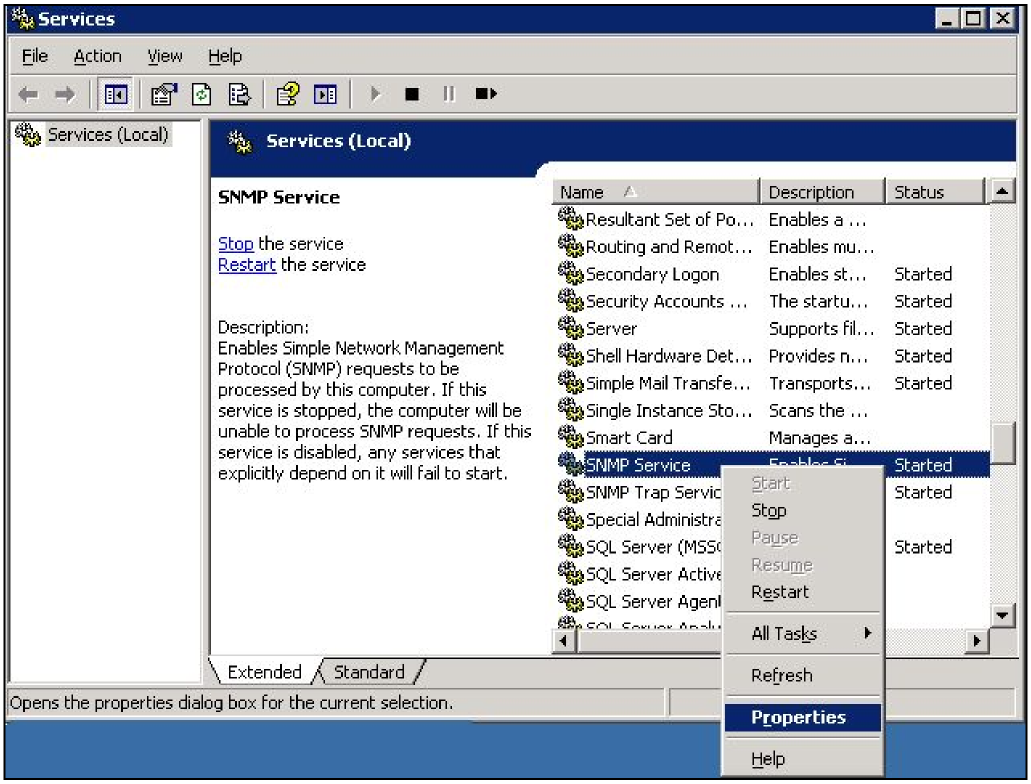
You must create a community name and assign permissions to the community name to view SNMP events. At a minimum, Research In Motion (RIM) requires that you to assign read-only permissions to the community name.

1. Right-click the **SNMP** service. Click **Properties**.
2. On the **Security** tab, in the Accepted Community Names section, click **Add**.
3. In the Community rights drop-down list, click the desired permission.
4. In the Community name field, type **public**.
5. Select the desired hosts to accept SNMP packets from.
6. Click **OK**.

2.4 Configuring the SNMP Service of the BlackBerry Host

To explicitly configure the SNMP Service of the BlackBerry host to receive SNMP packets from itself, follow the steps given below:

1. Open the **Services** window on the BlackBerry host.
2. Select the **SNMP Service**, right-click on it, and pick the **Properties** option from the shortcut menu that appears.



SNMP Service

Stop the service
Restart the service

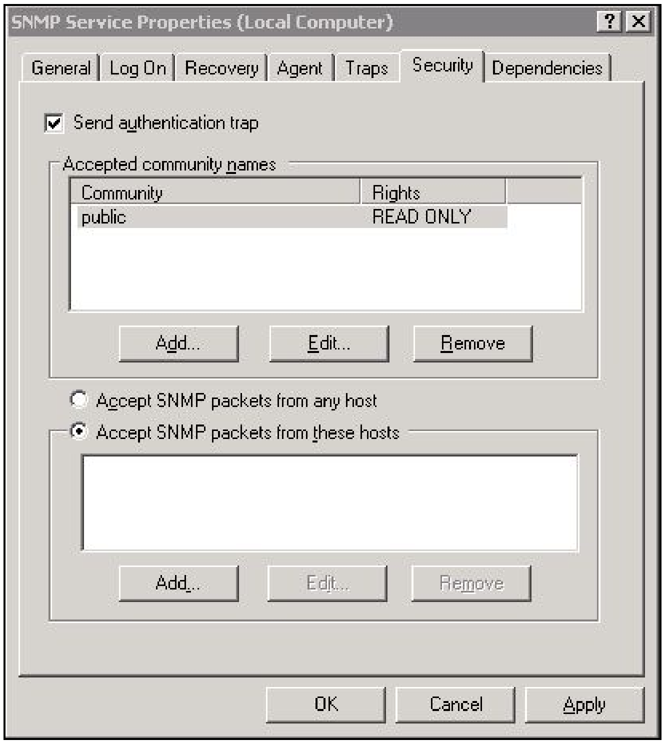
Description:
Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer. If this service is stopped, the computer will be unable to process SNMP requests. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status
Resultant Set of Po...	Enables a ...	
Routing and Remot...	Enables mu...	
Secondary Logon	Enables st...	Started
Security Accounts ...	The startu...	Started
Server	Supports fil...	Started
Shell Hardware Det...	Provides n...	Started
Simple Mail Transfe...	Transports...	Started
Single Instance Sto...	Scans the ...	
Smart Card	Manages a...	
SNMP Service	Enables Si...	Started
SNMP Trap Servic		Started
Special Administra		
SQL Server (MSSC		Started
SQL Server Active		
SQL Server Agent		

Opens the properties dialog box for the current selection.

Figure 2.1: Selecting the Properties option

3. Click on the **Security** tab page in the **SNMP Service Properties** dialog box that appears, select the **Accept SNMP packets from these hosts** option in the dialog box, and click the **Add** button therein.



☑ Send authentication trap

Accepted community names

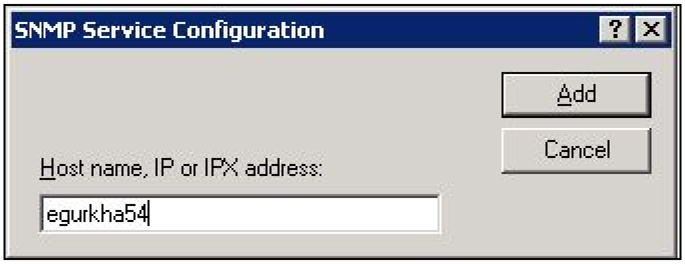
Community	Rights
public	READ ONLY

○ Accept SNMP packets from any host

● Accept SNMP packets from these hosts

Figure 2.2: The SNMP Service Properties dialog box

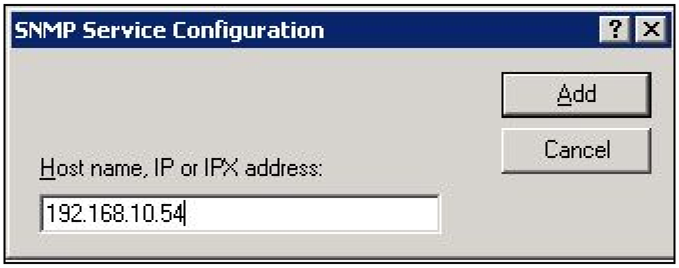
4. In Figure 2.3 that appears next, specify the host name of the BlackBerry host and click the **Add** button.



Host name, IP or IPX address: egurkha54

Figure 2.3: Configuring the host name of the BlackBerry host

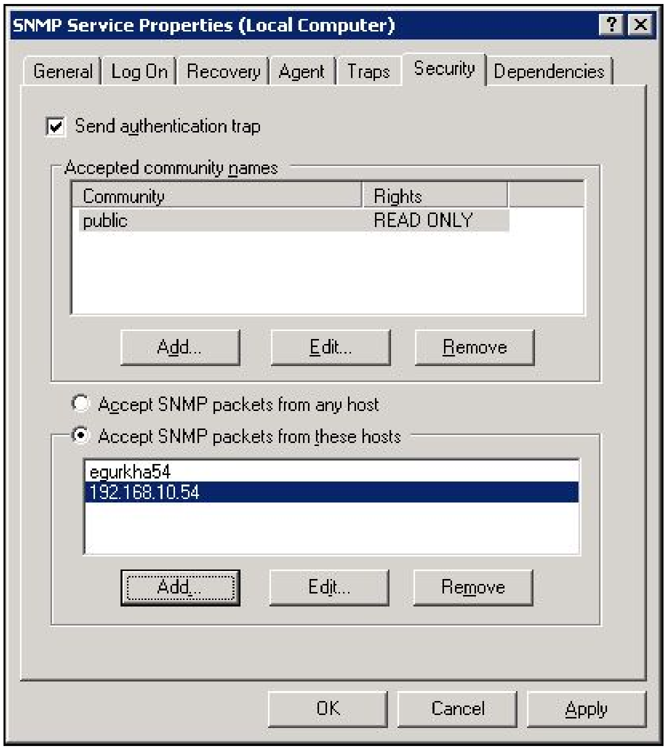
5. Upon returning to Figure 2.2, click on the **Add** button again. When Figure 2.4 appears, provide the IP address of the BlackBerry host and click the **Add** button.



Host name, IP or IPX address: 192.168.10.54

Figure 2.4: Specifying the IP address of the BlackBerry host

6. When Figure 2.5 appears, you will find that both the IP address and host name of the BlackBerry host are displayed therein. Finally, click the **Apply** and **OK** buttons in Figure 2.5.



☑ Send authentication trap

Accepted community names

Community	Rights
public	READ ONLY

○ Accept SNMP packets from any host

● Accept SNMP packets from these hosts

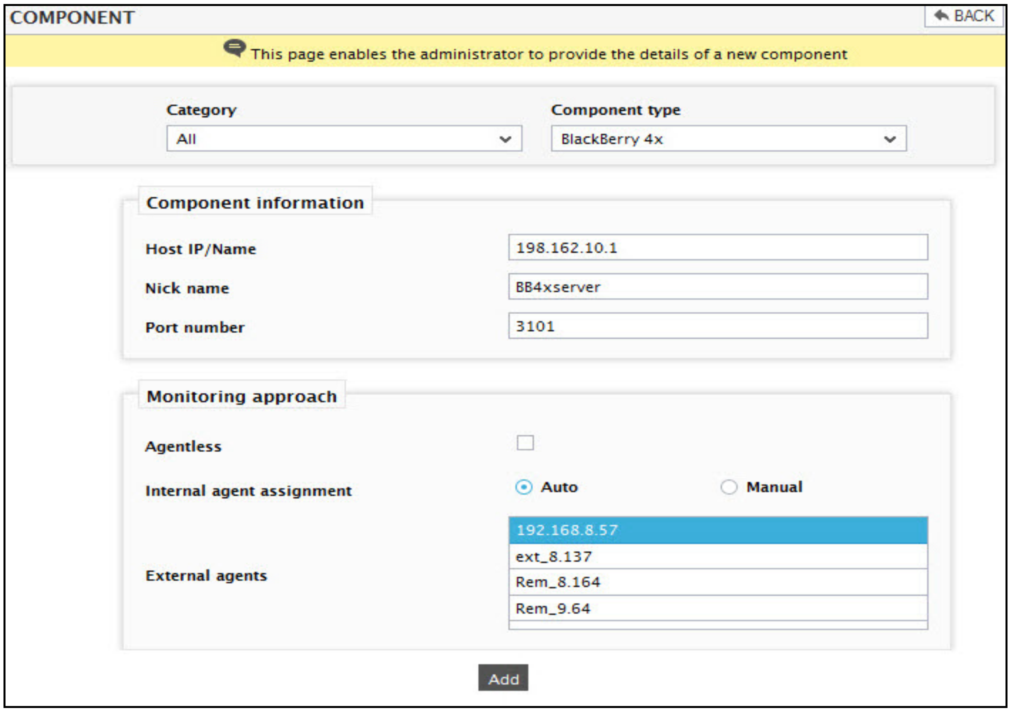
egurkha54
192.168.10.54

Figure 2.5: The IP address and host name of the BlackBerry host

2.5 Managing the BlackBerry 4x Server

The eG Enterprise cannot automatically discover the BlackBerry server so that you need to manually add the component for monitoring. To manage a BlackBerry 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 *BlackBerry 4x* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.6.



COMPONENT

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

Category: All

Component type: BlackBerry 4x

Component information

Host IP/Name: 198.162.10.1

Nick name: BB4xserver

Port number: 3101

Monitoring approach

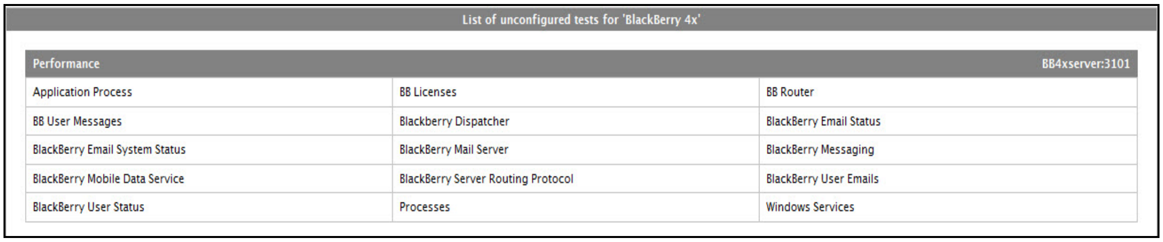
Agentless: □

Internal agent assignment: ● Auto ○ Manual

External agents: 192.168.8.57, ext_8.137, Rem_8.164, Rem_9.64

Figure 2.6: Figure 6: Adding the BlackBerry 4x server

4. Specify **Host IP/Name** and **Nick name** of the BlackBerry 4x server in Figure 2.6. Then, click on the **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests pertaining to the BlackBerry 4x server appears (see Figure 2.7).

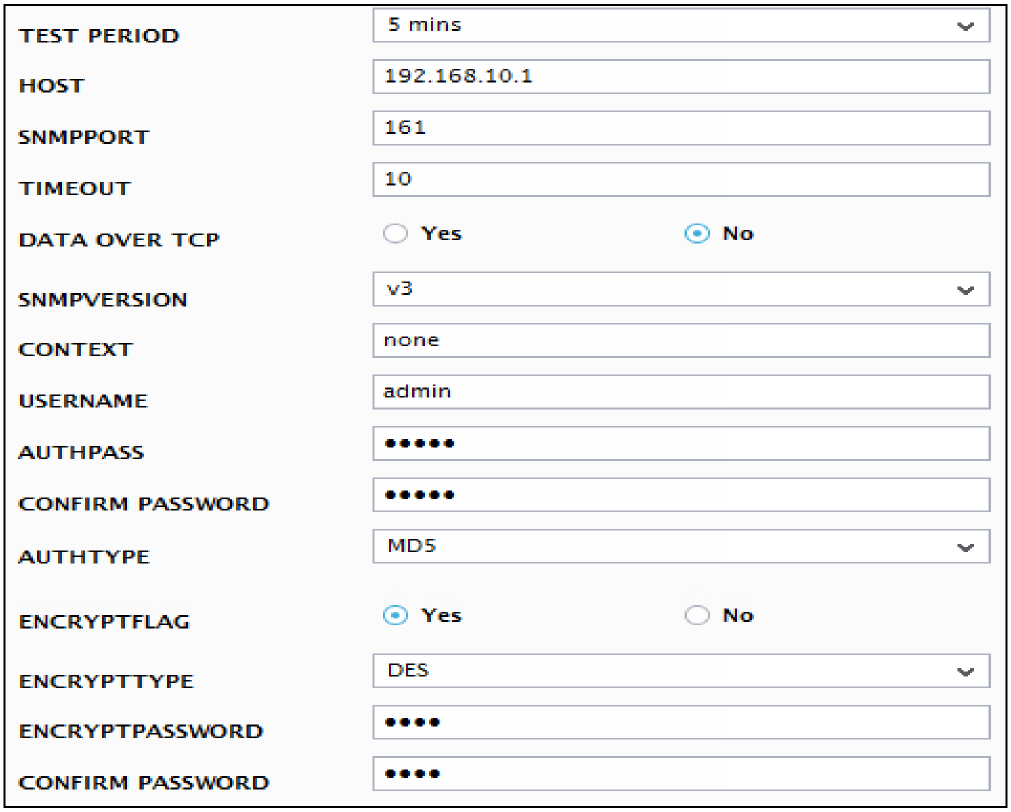


List of unconfigured tests for 'BlackBerry 4x'

Performance		BB4xserver:3101
Application Process	BB Licenses	BB Router
BB User Messages	Blackberry Dispatcher	BlackBerry Email Status
BlackBerry Email System Status	BlackBerry Mail Server	BlackBerry Messaging
BlackBerry Mobile Data Service	BlackBerry Server Routing Protocol	BlackBerry User Emails
BlackBerry User Status	Processes	Windows Services

Figure 2.7: List of Unconfigured tests for the BlackBerry 4x servers

6. Click on any test in the list of unconfigured tests. For instance, click on the **BlackBerry Dispatcher** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.8.



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 2.8: Configuring the BlackBerry Dispatcher test

7. To know how to configure parameters, refer to **Monitoring the BlackBerry Enterprise Server v4.1 (and lesser)**.

8. Finally, signout of the eG administrative interface.

You can follow the procedure explained above to configure the BlackBerry Enterprise Server v5 (or its variants) to work with the eG agent.

Chapter 3: Monitoring the BlackBerry Enterprise Server v4.1 (and lesser)

eG Enterprise offers a specialized BlackBerry 4x model that enables administrators to monitor the BlackBerry Enterprise Server v4.1 (and lesser), and report the status of critical services offered by the server.

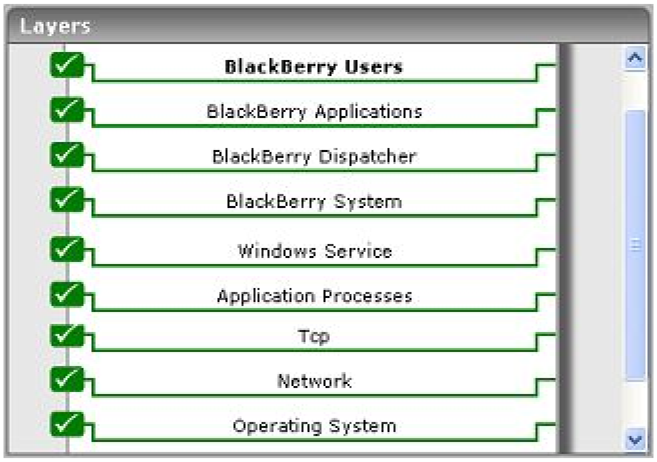


Figure 3.1: The layer model of the BlackBerry Enterprise Server

Each layer of Figure 2.1 above is mapped to a wide variety of tests, each of which reports a plethora of interesting statistics related to the performance of the BES.

The eG agent collects these metrics by contacting the SNMP MIB of the BlackBerry server. To enable this communication, **SNMP should be enabled on the BlackBerry server**. For this, refer to **How to Monitor the Blackberry Server using eG Enterprise?**.

These metrics, when analyzed, help administrators find accurate answers to the following performance queries:

- What is the workload on BES in terms of the number of push server connections?
- How healthy is the BlackBerry MDS (Mobile Data Services)? Did any connection initiated by the MDS fail?
- Did the SRP (Server Routing Protocol) host reject any data packets sent by MDS?
- Is BES currently connected to the SRP (Server Routing Protocol) host? If not, how long has it been disconnected?

- On an average, how many times do connections to SRP host fail?
- Is the dispatcher server currently connected to the SRP host? If not, how long has it been disconnected?
- How frequently does the dispatcher server fail to connect to the SRP host?
- Are enough CAL (Client Access License) keys installed on BES?
- How quickly does the BlackBerry messaging agent perform operations on a mail server?
- How is the network connectivity between the messaging agent and the mail server?
- Is WER (Wireless Email Reconciliation) enabled on BES? How many users have WER enabled? Who are they?
- Are there any inactive user accounts on BES?
- Is any user's handheld not connected to the Desktop Software currently?
- Are too many messages pending delivery to user's handheld?
- How many messages were not delivered owing to errors? Is the count very high?
- Is the Windows system hosting the BlackBerry server adequately sized in terms of CPU, memory, and disk space?
- Are any resource-intensive processes executing on the BES host?
- Are the critical BlackBerry services up and running?
- Is the BES available over the network? If so, how quickly does it respond to user requests?

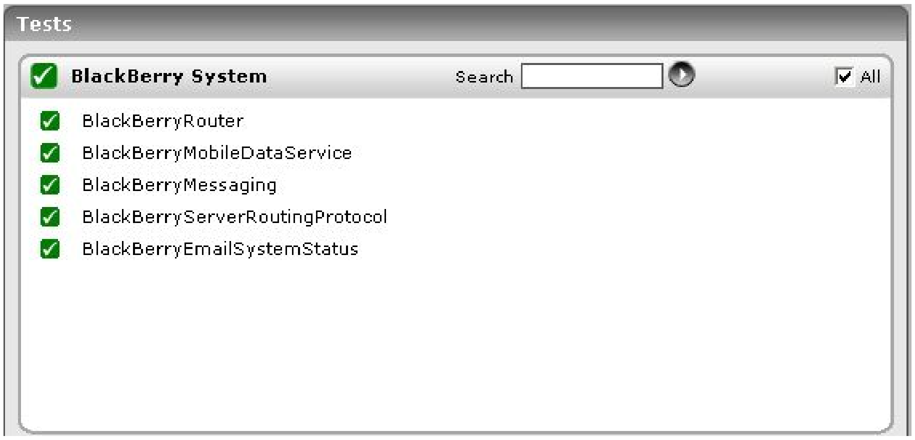
The sections to come discuss the top 4 layers of Figure 1, as the remaining layers have been elaborately dealt with in the *Monitoring Unix and Windows Servers* document.

3.1 The BlackBerry System Layer

The tests mapped to this layer report the overall health of each of the following BES components/services:

- The BlackBerry Router, which transmits all data to handheld
- The BlackBerry MDS, which provides connectivity between BlackBerry SmartPhones and enterprise applications
- The BlackBerry message-handling services, which handle the mail traffic to and from the handheld device

- The BlackBerry SRP (Server Routing Protocol) host, which provides BES with information related to the location of handheld devices
- The BlackBerry Email System, which ensures that the status of messages on the user desktop and on the user handheld are in sync



☑ BlackBerryRouter
☑ BlackBerryMobileDataService
☑ BlackBerryMessaging
☑ BlackBerryServerRoutingProtocol
☑ BlackBerryEmailSystemStatus

Figure 3.2: The tests mapped to the BlackBerry System layer

3.1.1 BB Router Test

The BlackBerry Router performs the following functions:

- Routes all data to wireless device
- Links BES to the SRP (Server Routing Protocol) host; while transmitting messages from within a corporate network to a handheld device, BES contacts the SRP host to know where the handheld is located

This test monitors the router and reports the number of devices and services currently connected to the router.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results the BlackBerry router being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.

Parameter	Description
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 transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm

Parameter	Description
	• **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
Services connected to router	This measure indicates the number of services currently connected to the router.	Number	
Devices connected to router	This measure indicates the number of devices currently connected to the router.	Number	

3.1.2 BlackBerry Mobile Data Service Test

BlackBerry® Mobile Data System (BlackBerry MDS) v4.1 is an optimized application development framework for the BlackBerry® Enterprise Solution. It can dramatically reduce the amount of time and resources required to develop and deploy wireless applications for mobile workers. BlackBerry MDS allows organizations to deliver corporate data wirelessly, leveraging the same proven push delivery model and advanced security features used for BlackBerry email.

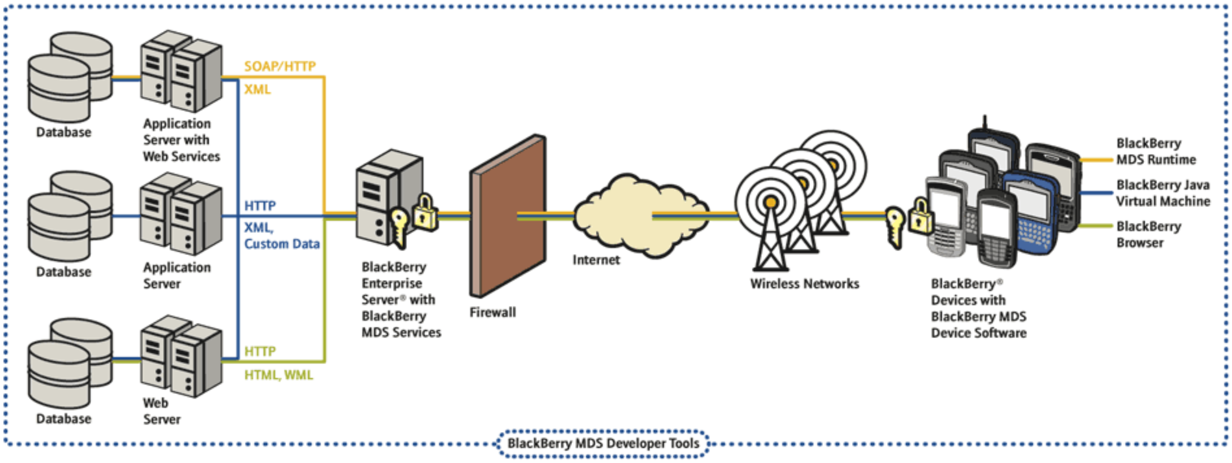

Database
Application Server with Web Services
SOAP/HTTP
XML
Database
Application Server
HTTP
XML, Custom Data
Database
Web Server
HTTP
HTML, WML
BlackBerry Enterprise Server® with BlackBerry MDS Services
Firewall
Internet
Wireless Networks
BlackBerry® Devices with BlackBerry MDS Device Software
BlackBerry MDS Runtime
BlackBerry Java Virtual Machine
BlackBerry Browser
BlackBerry MDS Developer Tools

Figure 3.3: BlackBerry Moble Data System architecture

BlackBerry MDS provides the essentials for creating, deploying and managing applications for the BlackBerry Enterprise Solution. Its three main components are:

- **BlackBerry MDS Services** : BlackBerry MDS Services are the next generation of the BlackBerry® Mobile Data Service. As part of the BlackBerry® Enterprise Server, they are responsible for managing interactions and requests between BlackBerry smartphones and enterprise applications that sit behind the corporate firewall.
- **BlackBerry MDS Developer Tools** : Use BlackBerry MDS Developer Tools to create wireless applications for BlackBerry smartphones.
- **BlackBerry MDS Device Software** : BlackBerry MDS Device Software allows applications built with BlackBerry MDS Developer Tools to run on BlackBerry smartphones.

This test monitors the efficiency of the **BlackBerry MDS Services** component of the BlackBerry MDS.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every server 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 *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

Parameter	Description
	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 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
Handheld initiated connections	Represents the number of handheld-initiated MDS connections initiated	Number	This is a good indicator of the workload on the BlackBerry MDS.

Measurement	Description	Measurement Unit	Interpretation
	during the last measurement period.		
Push server connections	Indicates the number of connections the BlackBerry MDS Connection Service central push server has established with BlackBerry devices during the last measurement period.	Number	‘Push’ technology is a data distribution technology in which selected data is automatically delivered into a mobile phone/computer at prescribed intervals or based on some event that occurs. Using the BlackBerry Manager, you designate one BlackBerry MDS Connection Service in a BlackBerry Domain as the central push server. The central push server receives push requests from applications. It establishes a connection to the BlackBerry device through which applications send data.
Average packet data size from device	Indicates the average data packet size received from handheld devices during the last measurement period.	MB	
Average packet data size from push	Indicates the average packet size of push data sent from the MDS to handhelds during the last measurement period.	MB	Typically, the enterprise application residing behind a corporate firewall sends an HTTP POST request to the BlackBerry MDS Connection Service central push server over the web server listen port (default 8080). The central BlackBerry Connection Service push server checks the central BlackBerry Configuration Database for information about the recipients who are defined in the push application. The BlackBerry MDS Connection Service responds to the push application to acknowledge that it is processing the request, and then closes the connection.

Measurement	Description	Measurement Unit	Interpretation
			The central BlackBerry MDS Connection Service push server routes the content to the push server connection listen port (default 8080). The BlackBerry MDS Connection Service converts the content for viewing on the BlackBerry device and sends the content to the BlackBerry Dispatcher. The value of this measure indicates the amount of data traffic that is handled by the BlackBerry MDS Services component while routing, converting, and eventually pushing the content to the handheld device.
Packets refused by SRP Host	Indicates the number of packets sent by MDS that were refused by the wireless network during the last measurement period.	Number	Server Routing Protocol (SRP) is a unique identifier used to communicate and authenticate the BlackBerry Enterprise Server with the BlackBerry relay. The BlackBerry relay is a key component of the BlackBerry system. It receives messages from within a corporate network, translates the messages, and routes them to the wireless network for delivery to the handheld device. SRP needs to be allowed through your company firewall. Therefore, if the value of this measure is very high, it could indicate that your firewall rules might have to be fine-tuned to allow bi-directional traffic from and to the SRP host. Also, check whether the SRP status is disconnected, as this could also obstruct the movement of data packets into an SRP host.
Invalid packets received by MDS	Indicates the number of invalid packets received	Number	A very high value of this measure could indicate a problem.

Measurement	Description	Measurement Unit	Interpretation
	by the MDS during the last measurement period.		
Successful connections from MDS	Indicates the number of successful connections initiated by MDS with another address or service during the last measurement period.	Number	
Failed connections from MDS	Indicates the number of connections the MDS attempted with another address or service, but failed currently.	Number	Ideally, the value of this measure should be low.
Truncated connections encountered by MDS	Indicates the number of truncated connections that the MDS encountered during the last measurement period.	Number	Ideally, the value of this measure should be low.

3.1.3 BlackBerry Messaging Test

This test reveals how effectively BES handles mails sent to and received from handheld devices.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for each server 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.

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
Messages processed	Indicates the number of messages processed by the BES during the last measurement period.	Number	This value includes messages to handheld devices, from handheld devices, and filtered messages.
Messages sent to handheld	Indicates the current number of messages that passed the filter criteria and were sent to handheld devices.	Number	This value does not include calendar items.
Messages sent from	Indicates the number of	Number	This value does not include calendar

Measurement	Description	Measurement Unit	Interpretation
handheld	messages currently sent from handhelds during the last measurement period.		items.
Messages pending delivery	Indicates the number of messages that are currently awaiting delivery to the handhelds.	Number	If the value of this measure is high or is increasing steadily, it could be a cause for concern, as it indicates a bottleneck in message delivery. This, in turn, could cause an increase in the size of the incoming message queue.
Messages expired	Indicates the total number of messages that timed out without being forwarded to the handheld during the last measurement period.	Number	Typically, messages time out after 7 days of non-delivery to the handheld. Messages can also time out if a user is not in a wireless network coverage area.
Undeliverable messages	Indicates the current number of messages that could not be delivered due to errors.	Number	Ideally, the value of this measure should be low. A high value for this measure would require an investigation.
Messages filtered	Indicates the number of messages to which the BlackBerry Enterprise Server applied filters and therefore did not forward to handhelds during the last measurement period.	Number	You can create email message filters to define which messages the BlackBerry® Enterprise Server forwards from email applications to BlackBerry devices. When users receive messages in the incoming message queue, the BlackBerry Enterprise Server applies email message filters to determine how to direct the messages: forward, forward with priority, or do not forward to the BlackBerry devices. If messages were not forwarded to handhelds because of a ‘do not forward’ filter, then such messages will be included in this count.

3.1.4 BlackBerryServerRoutingProtocol Test

Server Routing Protocol (SRP) is a unique identifier used to communicate and authenticate the BlackBerry Enterprise Server with the BlackBerry relay. The BlackBerry relay is a key component of the BlackBerry system. It receives messages from within a corporate network, translates the messages, and routes them to the wireless network for delivery to the handheld device.

In order to facilitate this transaction, the BlackBerry Enterprise Server maintains a constant connection with the SRP host, so that it knows where the handheld devices are located.

This test monitors the SRP host and reports the status of the BES server's connections with the SRP host.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every server 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 *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

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	Description	Measurement Unit	Interpretation
Is BlackBerry server connected to SRP host?	Indicates whether BES is currently connected to the SRP host or not	Boolean	The value 1 indicates that BES is connected to the SRP host. The value 0 indicates that BES is not connected to the SRP host. If the BES-SRP host connection fails, it would result in crucial lapses in delivery of messages to handheld devices. Therefore, if the value of this measure is 0, you are advised to perform additional prognosis to identify the cause of the connection failure, and attend to the cause quickly.
Successful reconnection to SRP host	Indicates the number of times the blackberry server has successfully reconnected to the SRP host during the last measurement period.	Number	The BlackBerry Enterprise Server may disconnect the Server Routing Protocol (SRP) connection to the BlackBerry Infrastructure. This disconnection may be due to the following network conditions: • Packet loss • Latency • Other symptoms of poor network conditions Immediately following the SRP disconnection, the BlackBerry

Measurement	Description	Measurement Unit	Interpretation
			Enterprise Server attempts to reconnect to the BlackBerry Infrastructure. However, if poor network conditions persist during this time, the SRP connection may be repeatedly disconnected and reconnected by the BlackBerry Enterprise Server. This is what a high value of the Failed reconnections to SRP host measure would typically imply.
Failed reconnections to SRP host	Indicates the number of times the blackberry server has failed to reconnect to the SRP host during the last measurement period.	Number	
Time connection to SRP host has been lost	Indicates the number of seconds for which BES has not been connected to the SRP host during the last measurement period.	Secs	If the BES remains disconnected from the SRP host for too long a time, it would disrupt the interaction between BES and the BlackBerry handheld devices within a wireless network. Such disconnections could be caused due to any of the following practical reasons: • Pathetic network conditions causing reconnections to SRP hosts to fail repeatedly • The BlackBerry Infrastructure is configured to disable SRP identification (IDs) that establish and exceed five connections within one minute. This configuration can be changed. • If the BlackBerry Enterprise Server is connected to the BlackBerry Infrastructure and another client attempts to connect using the same SRP ID and Authentication Key, the

Measurement	Description	Measurement Unit	Interpretation
			BlackBerry Infrastructure drops the connection to the BlackBerry Enterprise Server. Improper configuration of BES can also affect the BES-SRP host connectivity. Such configuration issues include: • Firewall configurations disallowing BES - SRP host connections • The Network Access Node key is set to an IP address or NetBIOS name other than localhost. • The Server Routing Protocol (SRP) Address is blank or set to local host. • The SRP identifier or SRP authentication key are specified incorrectly. • On the Server tab of BlackBerry Server Configuration, the router host is not set to localhost. • The BlackBerry Router service cannot start.

3.1.5 BlackBerry Email System Status Test

The Wireless Email Reconciliation (WER) feature, if enabled on BES, helps manage emails better, as it enables automatic, wireless synchronization of device and desktop mailboxes. Messages that have been read or deleted on the device are automatically updated on the desktop and vice versa.

This test reports the number of WER requests received and sent by BES.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every server 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 *none*.

Parameter	Description
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 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
Users enabled for wireless email reconciliation - WER	Indicates the current number of users for whom WER is enabled.	Number	
WER requests to handheld	Indicates the current number of WER requests sent to handheld devices.	Number	
WER requests from handheld	Indicates the current number of reconciliation requests that BES received from handheld devices.	Number	

3.2 The BlackBerry Dispatcher Layer

The tests associated with the **BlackBerry Dispatcher** layer reports on the overall health of the BlackBerry Dispatcher and also reveals whether or not BES is utilizing licenses optimally.

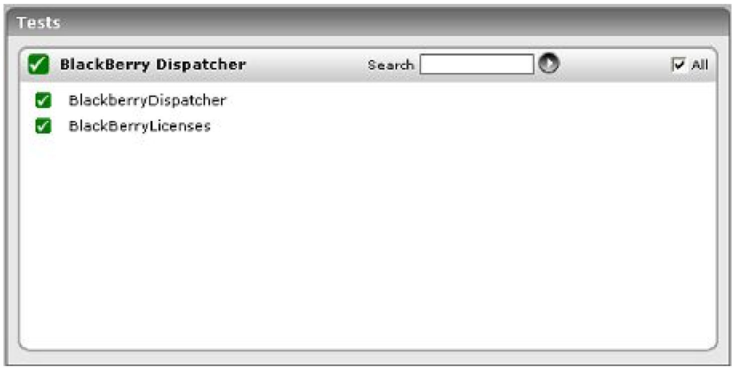


Figure 3.4: The tests associated with the Network layer

3.2.1 BlackBerryDispatcher Test

The BlackBerry Dispatcher is designed to compress and encrypt all information sent to the BlackBerry device. The BlackBerry Dispatcher is also designed to decompress and decrypt all information that users send from the BlackBerry device, and to send that information to other BlackBerry services and components.

To receive or send information to BES, the BlackBerry Dispatcher must first connect to the SRP host to determine which BES to communicate with. This test monitors the health of the interactions between the BlackBerry Dispatcher and the SRP host.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every server 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

Parameter	Description
	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 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 dispatcher server connected to SRP?	Indicates whether/not the BlackBerry Dispatcher is currently connected to SRP.	Boolean	The value 1 indicates that the dispatcher is connected to the SRP server. The value 0 indicates that the dispatcher is not connected to the SRP server. Without establishing a connection with the SRP server, the dispatcher will not know which BES to communicate with, and therefore will not be able to send/receive information from the BES.
Successful reconnections to SRP	Indicates the number of times the dispatcher server has successfully reconnected to the SRP host during the last measurement period.	Number	The BlackBerry Dispatcher may disconnect the Server Routing Protocol (SRP) connection to the BlackBerry Infrastructure due to the following network conditions: • Packet loss • Latency • Other symptoms of poor network conditions Immediately following the SRP disconnection, the BlackBerry Dispatcher attempts to reconnect to the BlackBerry Infrastructure. However, if poor network conditions persist during this time, the SRP connection may be repeatedly disconnected and reconnected by the BlackBerry Dispatcher. This is what a high value of the Failed reconnections to SRP host measure would typically imply.
Failed reconnections to SRP	Indicates the number of number of failed reconnections to SRP during the last measurement period.	Number	
Time dispatcher is not connected to SRP	Indicates the duration for which the dispatcher could not connect to SRP during the last	Secs	If the dispatcher remains disconnected from the SRP host for too long a time, it would disrupt the

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		interaction between BlackBerry infrastructure and the wireless network. Such disconnections could be caused due to any of the following practical reasons: • Pathetic network conditions causing reconnections to SRP hosts to fail repeatedly • The BlackBerry Infrastructure is configured to disable SRP identification (IDs) that establish and exceed five connections within one minute. This configuration can be changed. • If the BlackBerry Enterprise Server is connected to the BlackBerry Infrastructure and another client attempts to connect using the same SRP ID and Authentication Key, the BlackBerry Infrastructure drops the connection to the BlackBerry Enterprise Server. Improper configuration of BES can also affect the Dispatcher-SRP host connectivity. Such configuration issues include: • Firewall configurations disallowing Dispatcher - SRP host connections • The Network Access Node key

Measurement	Description	Measurement Unit	Interpretation
			is set to an IP address or NetBIOS name other than localhost. • The Server Routing Protocol (SRP) Address is blank or set to local host. • The SRP identifier or SRP authentication key are specified incorrectly. • On the Server tab of BlackBerry Server Configuration, the router host is not set to localhost. • The BlackBerry Router service cannot start.

3.2.2 BB Licenses Test

CAL (Client access license) keys control how many user accounts can exist on a BlackBerry® Enterprise Server at the same time. To ensure the continued use of the BlackBerry infrastructure, adequate licenses or CAL keys need to be available on BES. This test monitors the license usage on BES, and reveals if more licenses are required.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every server 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 *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**.

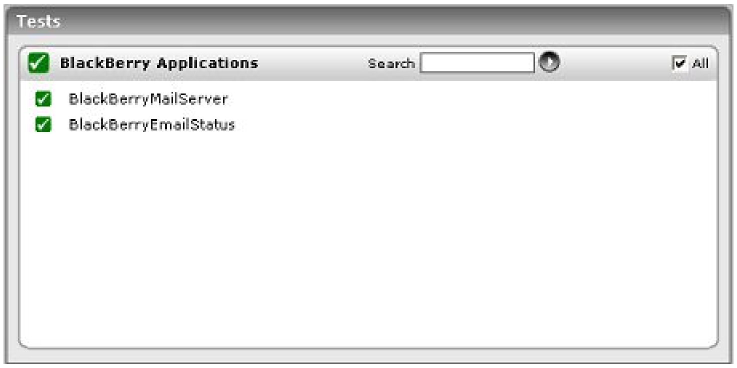
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Licenses installed	Indicates the number of license keys installed on BES, currently.	Number	
Licenses in use currently	Indicates the number of licenses currently in use on the BES.	Number	
Licenses remaining for use	Indicates the number of licenses yet to be used.	Number	Ideally, the value of this measure should be high. A zero value or a value close to zero indicates that the

Measurement	Description	Measurement Unit	Interpretation
			BlackBerry Enterprise server has exhausted all installed CAL keys, or is excessively consuming CAL keys (as the case may be). When you exceed the number of licensed user accounts, the BlackBerry Manager informs you that you require more CAL keys. You will not be able to continue using BES until additional CAL keys are installed on BES.
Excess license usage	Indicates the number of licenses used over and above the installed licenses.	Number	This measure will appear only if the sum of the value of the Licenses in use currently and the Licenses remaining for use measures is greater than the value of the Licenses installed measure. In other words, this measure will appear only if the total license usage is greater than the number of licenses that are installed. If not, this measure will not appear. If the measure appears, it is indicative of excessive license usage.

3.3 The BlackBerry Applications Layer

Using the tests mapped to the **BlackBerry Applications** layer, you can determine the status of mail exchanges between the BlackBerry Messaging Agent and the external mail servers.



Tests

☑ BlackBerry Applications   Search   ☑ All

☑ BlackBerryMailServer

☑ BlackBerryEmailStatus

Figure 3.5: The test associated with the BlackBerry Applications layer

3.3.1 BlackBerry Mail Server Test

The BlackBerry® Messaging Agent connects to an organization's messaging server and provides messaging services, calendar management, address lookups, attachment viewing, attachment downloading, and encryption key generation. This test monitors the activities of the BlackBerry Messaging Agent on each mail server in the target environment, and reports how quickly it performs the operations.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every mail server that the BES is configured to use.

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.

Parameter	Description
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 selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:

Parameter	Description
	- **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
Current users	Indicates the number of users currently homed on this mail server.	Number	
Avg response time for operations	Indicates the time the messaging agent takes currently to perform operations for users on this mail server.	Secs	A low value indicates that the messaging agent is able to process user requests to this mail server, rather quickly. A high value or a value that steadily increases could indicate a sudden/gradual deterioration in responsiveness. This would require further investigation.
Failed connection attempts	Indicates the number of times the BlackBerry messaging agent failed currently to connect to this mail server.	Number	A low value is desired for this measure. A high value indicates persistent issues in connectivity. This could be owing to a poor network connection or improper configuration.

3.3.2 BlackBerry Email Status Test

The Wireless Email Reconciliation (WER) feature, if enabled on BES, helps manage emails better, as it enables automatic, wireless synchronization of device and desktop mailboxes. Messages that have been read or deleted on the device are automatically updated on the desktop and vice versa.

This test reports the current status of the WER capability of the BES messaging agent.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BES server 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

Parameter	Description
	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.
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

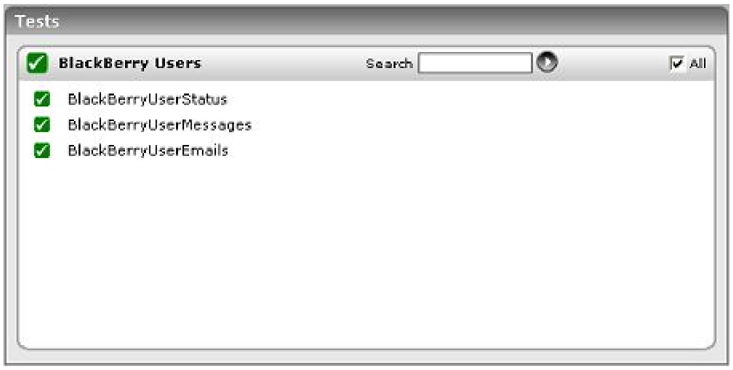
Parameter	Description
	components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Wireless email reconciliation status	Indicates whether WER is currently enabled or not on BES.	Boolean	If the value of this measure is 1, it indicates that WER is enabled. The value 0 for this measure, on the other hand, denotes that WER is disabled.

3.4 The BlackBerry Users Layer

The tests mapped to this layer reveal the current status and overall health of the user accounts registered with the BlackBerry Enterprise server.



☑ BlackBerryUserStatus
☑ BlackBerryUserMessages
☑ BlackBerryUserEmails

Figure 3.6: The tests associated with the BlackBerry Users layer

3.4.1 BlackBerry User Status Test

This test reports the status of the user account on the BES, and also the status of the user's handheld.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every user account registered with the BES 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 *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.

Parameter	Description
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 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 the device in cradle?	Indicates whether this user's handheld is	Boolean	The cradle is used for charging a build-in battery in a handheld electronic

Measurement	Description	Measurement Unit	Interpretation
	currently in the cradle or not.		device and connecting the handheld electronic device to a host computer so that the handheld electronic device can exchange information with the host computer. If the value of this measure is 1, it indicates that the device is in the cradle. This means that the user's handheld is connected to the Desktop Software. The value 0 on the other hand, denotes that the user's device is not in the cradle. This implies that the device is not currently connected to the Desktop software.
Is the user currently enabled?	Indicates whether this user's account is currently enabled on BES or not.	Boolean	While the value 1 for this measure indicates that the user account is enabled, the value 0 indicates that the user account is inactive or disabled on BES.

3.4.2 BB User Messages Test

This test reports key statistics revealing the BlackBerry Enterprise Server's message processing capabilities.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every user account registered with the BES 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 *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
Messages processed	Indicates the number of messages processed by the BES for this user during the last measurement period	Number	This value includes messages to handheld devices, from handheld devices, and filtered messages.
Messages sent to handheld	Indicates the number of messages that currently passed the filter criteria and were sent to this user's handheld.	Number	This value does not include calendar items.

Measurement	Description	Measurement Unit	Interpretation
Messages sent from handheld	Indicates the number of messages sent from this user's handheld during the last measurement period.	Number	This value does not include calendar items.
Messages pending delivery	Indicates the number of messages currently awaiting delivery to the this user's handheld.	Number	If the value of this measure is high or is increasing steadily, it could be a cause for concern, as it indicates a bottleneck in message delivery. This, in turn, could cause an increase in the size of the incoming message queue.
Messages expired	Indicates the total number of messages that timed out without being forwarded to this user's handheld during the last measurement period.	Number	Typically, messages time out after 7 days of non-delivery to the handheld. Messages can also time out if a user is not in a wireless network coverage area.
Undeliverable messages	Indicates the number of messages that could not be delivered currently due to errors.	Number	Ideally, the value of this measure should be low. A high value for this measure would require an investigation.
Messages filtered by user filter settings	Indicates the number of messages to which the BlackBerry Enterprise Server applied filters, and therefore did not forward to the user's handheld during the last measurement period.	Number	You can create email message filters to define which messages the BlackBerry® Enterprise Server forwards from email applications to BlackBerry devices. When users receive messages in the incoming message queue, the BlackBerry Enterprise Server applies email message filters to determine how to direct the messages: forward, forward with priority, or do not forward to the BlackBerry devices. If messages were not forwarded to handhelds because of a 'do not forward' filter, then such messages will be included in this count.
Messages forwarded	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
from device	messages that the user currently forwarded from his/her handheld.		
Avg size of messages forwarded from device	Indicates the average size of messages that the user currently forwarded from his/her handheld.	Kbytes	
Avg size of messages reply with text	Indicates the average size of messages that the user currently replied to with text from his/her handheld.	Kbytes	

3.4.3 BlackBerry User Emails Test

The Wireless Email Reconciliation (WER) feature, if enabled on BES, helps manage emails better, as it enables automatic, wireless synchronization of device and desktop mailboxes. Messages that have been read or deleted on the device are automatically updated on the desktop and vice versa.

This test reveals the WER status for every user registered with BES, and also reports metrics related to the reconciliation activity per user.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every user registered with BES 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.

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
Is the user enabled for wireless reconciliation?	Indicates whether/not WER is enabled for this user currently	Boolean	The value 1 indicates that WER is enabled, and the value 0 indicates that it is not. If disabled, then status synchronization will not occur for emails pertaining to this user.
Wireless email requests to handheld	Indicates the number of WER requests sent to the user's handheld currently.	Number	
Wireless email requests from handheld	Indicates the number of reconciliation requests that BES received from this user's handheld currently.	Number	

Chapter 4: Monitoring the BlackBerry Enterprise Server v5 (or its variants)

BlackBerry Enterprise Server v5.0 differs from its predecessors in its built-in high availability architecture which enables fast recovery from unplanned downtime of core BlackBerry Enterprise Server components. The new high availability option is designed to automatically use the standby core components if the need arises and has the flexibility of being deployed on physical and virtual servers (specifically VMware®).

With the component level architecture, health metrics are continually monitored by the BlackBerry Enterprise Server. BlackBerry administrators can set failover thresholds, which when exceeded, trigger the BlackBerry Enterprise Server to automatically switch over to the standby server. For example, if the primary server loses its connection to the mail server, automatic failover would occur to the standby server, minimizing the delay of switching over manually. The administrator acknowledges when an automatic failover has occurred, fixes the problem on the originating server, and then manually sets the systems back, ensuring that failover loops are avoided.

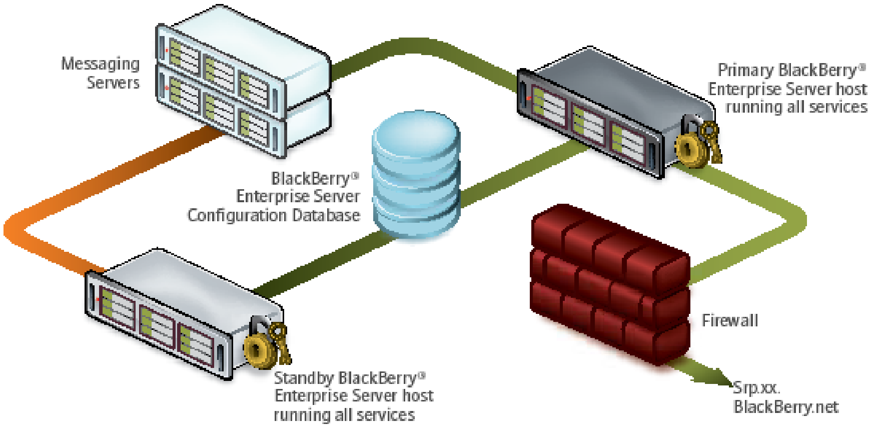

Messaging Servers
Primary BlackBerry® Enterprise Server host running all services
BlackBerry® Enterprise Server Configuration Database
Firewall
Standby BlackBerry® Enterprise Server host running all services
Srp.xx. BlackBerry.net

Figure 4.1: The high availability architecture of the BES v5

To monitor BES v5, eG Enterprise provides a dedicated *BlackBerry 5x* model.

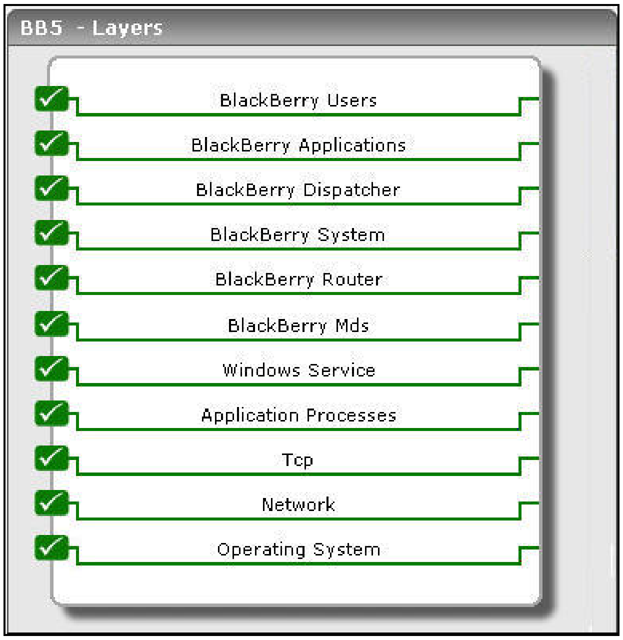


Figure 4.2: The layer model of the BlackBerry Enterprise Server v5

Each layer of Figure 4.2 is mapped to a wide variety of tests which report a wealth of performance metrics related to the BlackBerry Enterprise Server v5. Using the metrics reported by these tests, administrators can find quick and accurate answers to the following performance queries:

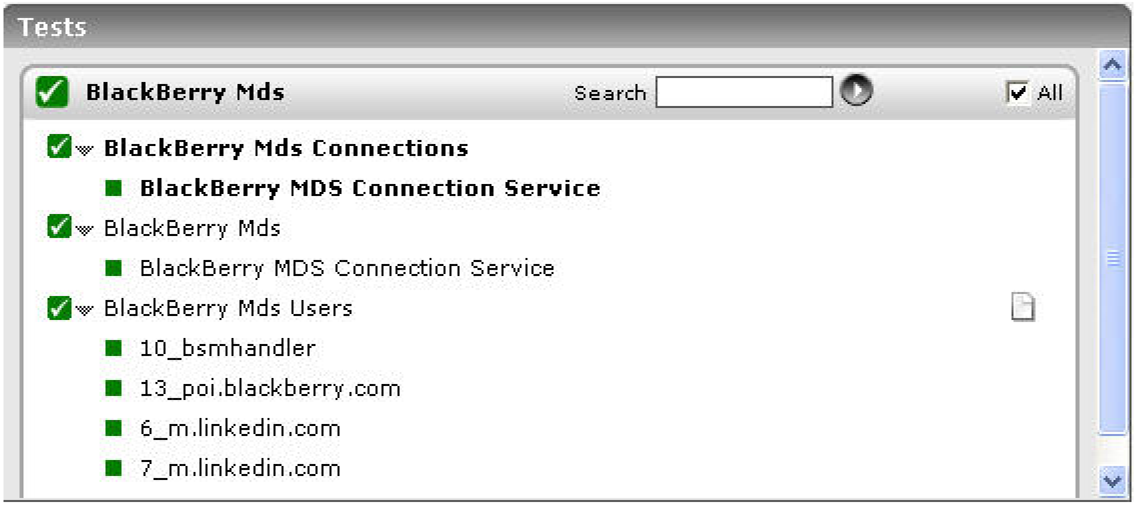
- How many users have MDS enabled on their devices?
- Are data transmissions on MDS connections heavy?
- Has the MDS Connection Service refused any data packets?
- Were invalid packets received by the MDS Connection Service?
- Have too many SRP connections to the BlackBerry Infrastructure failed?
- Is any user connected to the MDS for an unreasonably long time? Which user is this?
- Is too much data transmitted from the MDS to any user's handheld device? Which user is this?
- Is the router configured with adequate device connections?
- How is the load on the router?
- Are there too many undelivered messages on the BlackBerry Enterprise Server?
- Have too many messages expired?
- Are there too many pending requests to the BlackBerry Policy Service?
- Did any request to the Policy Service fail?

- Were any hung threads detected on the BlackBerry Enterprise Server?
- Is the BlackBerry Dispatcher connected to the handheld device? If so, how quickly was the connection established?
- Does the BES have adequate licenses?
- What is the user load on the BlackBerry Messaging Agent? Which users are currently connected to the agent?
- Did any connection attempt to the messaging agent fail in the last 10 minutes?
- Are devices taking too long to connect to the messaging agent?
- Is the messaging agent able to process messages quickly or are too many messages pending on the agent?
- Has any user failed to initialize with BES?

The sections that follow will discuss the top 6 layers of Figure 3.2. For remaining layers, refer to *Monitoring Unix and Windows Servers* document.

4.1 BlackBerry Mds Layer

The BlackBerry MDS Connection Service is designed to provide users with access to online content and applications in the corporate internet and intranet. The tests mapped to the **BlackBerry Mds** layer monitors the load on the MDS Connction Service, and reveals how well the service handles the load.



☑ **BlackBerry Mds Connections**
- **BlackBerry MDS Connection Service**

☑ BlackBerry Mds
- BlackBerry MDS Connection Service

☑ BlackBerry Mds Users
- 10_bsmhandler
- 13_poi.blackberry.com
- 6_m.linkedin.com
- 7_m.linkedin.com

Figure 4.3: The tests mapped to the BlackBerry Mds layer

4.1.1 BlackBerry Mds Connections Test

Application developers can use the BlackBerry® MDS Connection Service component of the BlackBerry® Enterprise Server to proactively deliver data or web content directly to BlackBerry devices that are activated on an organization’s BlackBerry Enterprise Server. Users do not need to request or download data; the push application, in conjunction with the BlackBerry MDS Connection Service, delivers it as soon as it is available. This way, BlackBerry device users gain access to web content. It also permits applications on devices to receive application data and updates from your organization's application servers or content servers.

By monitoring the MDS communication between the MDS-enabled devices and the BlackBerry Enterprise server, you can determine the number of handheld device users to whom data will be pushed by the MDS, and thus infer the load imposed by such users on the BES. In the process, you can also monitor how MDS controls the flow of data packets to the BlackBerry device, and regulate the flow (if need be) based on your findings. This test enables you to achieve all of the above.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every server 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

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
Mds connection enabled users	Indicates the number of users who have enabled the BlackBerry MDS Connection Service on their handheld devices.	Number	
Total push connections	Indicates the total number of push connections that were initiated by the BlackBerry MDS Connection Service.	Number	Using the BlackBerry® MDS Connection Service, you can push content to the BlackBerry handheld device using any of the following push methods: • Pushing content to a browser channel: This method delivers content to the browser cache and adds an icon on the Home screen as an entry point to the content. Clicking the icon opens the pushed content in the browser.

Measurement	Description	Measurement Unit	Interpretation
			- Pushing content to the message list: This method delivers content to the message list, where it appears as an item in the list. Clicking the item in the message list displays the pushed content in the browser. - Pushing content to the browser cache: This method delivers content to the cache, but provides no notification to the user. The next time the user accesses the content, the updated cached content is displayed.
Total cached push connections	Indicates the number of push connections that pushed content directly to the BlackBerry Browser cache.	Number	Browser cache push content helps to ensure that users can access pages from a local cache at any time, even when they are outside a wireless coverage area. An application that pushes data to the browser cache can include an expiry time that defines the length of time that the data remains in the cache before it is removed. The default length of time that push content is stored in cache memory varies with the BlackBerry Browser software version used. In BlackBerry Browser version 3.8 and later, pushed content is removed from the cache after 12 hours. In preceding versions, pushed content expired and was removed from the cache after 29 days.
Data received on	Indicates the amount of	KB	

Measurement	Description	Measurement Unit	Interpretation
MDS connections	data received by all the MDS-enabled BlackBerry devices on MDS connections that they initiated.		
Data transmitted on MDS connections	Indicates the amount of data transmitted by all the MDS-enabled BlackBerry devices on MDS connections that they initiated.	KB	The BlackBerry® MDS Connection Service controls the flow of data that is sent to the BlackBerry device. This flow control allows the BlackBerry MDS Connection Service to minimize the amount of data that is sent over the wireless network, and can help to reduce the impact of pushing data to BlackBerry devices that are out of network coverage, turned off, or otherwise unavailable. The BlackBerry MDS Connection Service sends data to each BlackBerry device specified in the push request as a series of packets. To control the flow of pushed data, the BlackBerry MDS Connection Service initially sends a maximum of five packets. The BlackBerry MDS Connection Service does not send additional packets until the BlackBerry device returns an acknowledgment that the initial packets were received. By default, the BlackBerry MDS Connection Service limits the size of packets to 29 KB for BlackBerry® Enterprise Server 4.0, or 1 KB for BlackBerry Enterprise Server 4.1 or later.

4.1.2 BlackBerry Mds Test

The BlackBerry MDS receives push requests from applications; these requests typically contain the data to be delivered. The MDS then pushes the data to the BlackBerry devices. Using this test, you can monitor the data received by the MDS (from applications) and the connections established by the MDS with BlackBerry devices for transmitting data to them. With the help of the metrics reported by this test, you can ascertain the following:

- Whether any data packets were refused or declared invalid by the MDS;
- Whether any connectivity issues exist between the MDS and the devices; if so, you can also figure out whether it is owing to failed SRP (Server Routing Protocol) connections

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BES 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 *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

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	Description	Measurement Unit	Interpretation
Refused packets	Indicates the number of data packets that were refused by the BlackBerry MDS Connection Service during the last measurement period.	Number	The BlackBerry MDS may reject a data packet if it does not recognize the format of a data packet or does not recognize the device transport key that protects the data packet.
Invalid packets	Indicates the total number of invalid data packets that were received by this BlackBerry MDS Connection service during the last meaurement period.	Number	One of the reasons why a push request may have been declared invalid by the MDS is if the request contains a reliability specification, but does not include a notification URL. In your push request, you can specify that you want the BlackBerry® device to return a result notification when the pushed data is successfully delivered. The BlackBerry® MDS Connection Service receives notifications from each destination BlackBerry device that successfully receives the pushed data and forwards those notifications to the push originator. Similarly, the BlackBerry MDS Connection Service sends a notification to the push originator if a push request is not

Measurement	Description	Measurement Unit	Interpretation
			successfully delivered to one or more destination BlackBerry devices within the allotted time. If you do not specify a reliability level for your push method, the BlackBerry MDS Connection Service does not provide the push originator with any notification regarding the outcome of the push request. You must also specify a notification URL to which the BlackBerry MDS Connection Service will send result notifications, with every push request that specifies a reliability option. A push request that requests some level of reliability but does not provide a notification URL is considered invalid and is rejected by the BlackBerry MDS Connection Service.
Truncated connections	Indicates the number of truncated connections that were encountered by the BlackBerry MDS Connection service during the last measurement period.	Number	Ideally, the value of this measure should be low.
Invalid connections	Indicates the number of invalid connections encountered by this Blackberry MDS Connection Service during the last measurement period.	Number	
Successful SRP connections	Indicates the number of successful SRP connections to the BlackBerry Infrastructure.	Number	The BlackBerry Dispatcher handles traffic to the BlackBerry Infrastructure. It compresses/decompresses and encrypts/decrypts wireless data. The BlackBerry Dispatcher handles all Server Routing Protocol (SRP) connections from the BlackBerry MDS

Measurement	Description	Measurement Unit	Interpretation
			Connection Service and many other components of the BlackBerry Infrastructure. The MDS Connection Service (on the BlackBerry Enterprise Server) connects to the BlackBerry Dispatcher through specific ports and communicates with the BlackBerry Infrastructure through the BlackBerry Router using a unique SRP identifier that the BlackBerry Dispatcher establishes. Once the SRP identifier is established, the BlackBerry MDS sends a basic information packet to the BlackBerry Infrastructure via the BlackBerry Router; this packet includes version information, the SRP identifier established by the BlackBerry dispatcher, and other information that is required to open an SRP connection. If the packets so received are valid, then the BlackBerry infrastructure will send basic information packets to the BlackBerry MDS, therey successfully opening the SRP connection. On the other hand, if the BlackBerry Infrastructure receives unrecognized packets from the BlackBerry MDS, then the SRP is connection is closed. Also, if a BlackBerry MDS uses the same SRP authentication key and SRP identifier to connect to (and then disconnect from) the BlackBerry Infrastructure 5 times in 1 minute, the BlackBerry Infrastructure deactivates the SRP identifier to help prevent a potentially malicious user from using the SRP identifier to create conditions for a DoS attack.
Failed SRP connections	Indicates the number of failed SRP connections to the BlackBerry Infrastructure.	Number	

4.1.3 BlackBerry Mds Users Test

Upon the receipt of push requests from applications, the MDS Connection Service pushes application data to each user's handheld device. By monitoring the communication between MDS and every user's BlackBerry device, you can isolate communication bottlenecks and connections on which a large amount of data is transmitted. This test enables you to do just that. With the help of the metrics reported by this test, you can instantly identify the user (i.e., the device) to whom the BlackBerry MDS takes too long to deliver data, and the user (i.e., the device) to whom an unreasonably large amount of data is being transmitted. Network links to such devices can then be investigated for congestions and the flow of data via such links can be regulated, so as to optimize performance.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every server 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 *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

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	Description	Measurement Unit	Interpretation
Connection duration	Indicates the duration for which this user was connected to MDS.	Secs	A very high value for this measure indicates that the user has remained connected to the MDS for a very long time. This could be because of a delay in delivering data to the user's handheld, which in turn can be caused by a network congestion or a poor network link.
Transmitted packets size	Indicates the size of packets that were transmitted from the BlackBerry MDS Connection Service to this user's handheld during the last measurement period.	KB	The BlackBerry® MDS Connection Service controls the flow of data that is sent to the BlackBerry device. This flow control allows the BlackBerry MDS Connection Service to minimize the amount of data that is sent over the wireless network, and can help to reduce the impact of pushing data to BlackBerry devices that are out of network coverage, turned off, or otherwise unavailable. The BlackBerry MDS Connection Service sends data to each BlackBerry device specified in the push request as a series of packets. To control the flow of pushed data, the

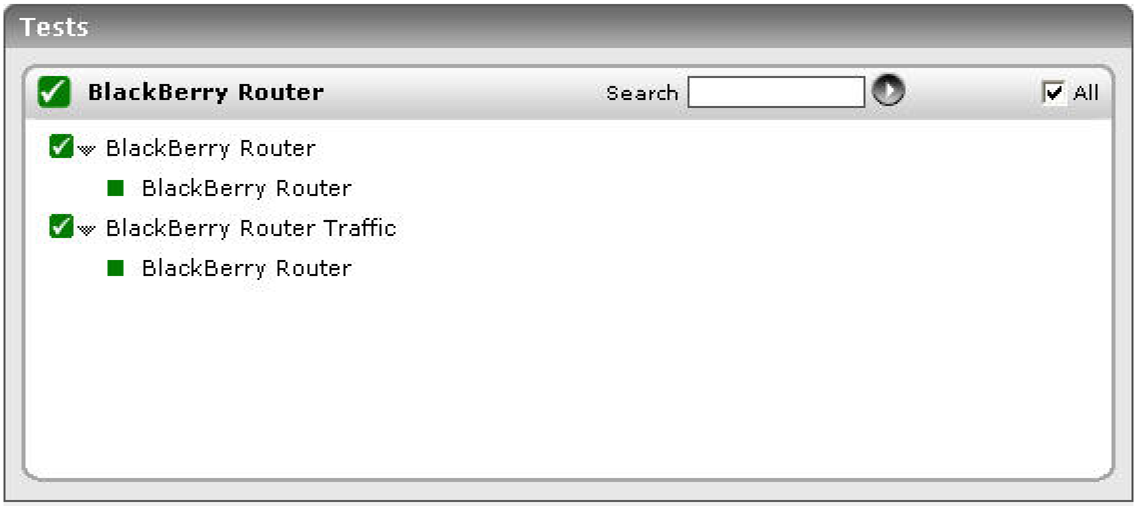
Measurement	Description	Measurement Unit	Interpretation
			BlackBerry MDS Connection Service initially sends a maximum of five packets. The BlackBerry MDS Connection Service does not send additional packets until the BlackBerry device returns an acknowledgment that the initial packets were received. By default, the BlackBerry MDS Connection Service limits the size of packets to 29 KB for BlackBerry® Enterprise Server 4.0, or 1 KB for BlackBerry Enterprise Server 4.1 or later.
Packets transmitted	Indicates the total number of packets that were transmitted from the BlackBerry MDS Connection Service to this user's BlackBerry handheld device during the last measurement period.	Number	
Received packets size	Indicates the size of the packets that were received by the Blackberry MDS Connection Service from this user's BlackBerry handheld device during the last measurement period.	KB	
Packets received	Indicates the total number of packets that were received by the BlackBerry MDS Connection service from this user's BlackBerry handheld device during the last measurement period.	Number	

4.2 BlackBerry Router Layer

The BlackBerry Router performs the following functions:

- Routes all data to wireless device
- Links BES to the SRP (Server Routing Protocol) host; while transmitting messages from within a corporate network to a handheld device, BES contacts the SRP host to know where the handheld device is located

With the help of the tests mapped to it, the **BlackBerry Router** layer monitors the usage of router connections by the BlackBerry handheld devices and the transaction traffic on the router.



- ☑ BlackBerry Router
  - 🟩 BlackBerry Router
- ☑ BlackBerry Router Traffic
  - 🟩 BlackBerry Router

Figure 4.4: The tests mapped to the BlackBerry Router layer

4.2.1 BlackBerry Router Test

The router is typically configured with the maximum number of connections that services and devices can establish with it. You need to monitor the usage of these connections at frequent intervals, so as to ensure that the configured limit is not exceeded.

This test reports the configured connection limits for devices and services, and also indicates how many connections have been utilized and how many are free; this way, the test promptly alerts you if the services and devices are about to run out of connections.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Router configured for the BlackBerry Enterprise Server 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 *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
Total service connections to router	Indicates the maximum number of connections that services can establish with the router.	Number	
Total device connections to router	Indicates the maximum number of connections that devices can establish with the router.	Number	
Used service connections to router	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
	connections that services are currently utilizing for connecting to the router.		
Used device connections to router	Indicates the number of connections that the devices are currently utilizing for connecting to the router.	Number	
Free service connections to router	Indicates the percentage of total service connections to router that are unused.	Percent	Ideally, these values should be high. If these measures record very low values, it could indicate that services and devices are already utilizing router connections excessively, and may soon run out of connections to the router. Under such circumstances, try releasing a few service/device connections or try increasing the maximum number of router connections that services and devices are permitted to use.
Free device connections to router	Indicates the percentage of total device connections to router that are unused.	Percent	

4.2.2 BlackBerry Router Traffic Test

This test reveals the load on the BlackBerry router by reporting the number of transactions sent and received by the router.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Router configured for the BlackBerry Enterprise Server being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed

Parameter	Description
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 transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm

Parameter	Description
	- **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	Descripton	Measurement Unit	Interpretation
Transactions received	Indicates the number of transactions that were sent from the BlackBerry router to the BlackBerry devices.	Number	These measures serve as good indicators of the load on the router.
Transactions sent	Indicates the total number of transactions that were sent from the BlackBerry	Number	

Measurement	Descripton	Measurement Unit	Interpretation
	devices to the BlackBerry router.		

4.3 BlackBerry System Layer

The tests mapped to this layer reveal the following:

- Message processing bottlenecks on the BES;
- The load on the BlackBerry Policy Service and how well the service handles the load;
- The status of threads assigned by the BlackBerry Enterprise Server

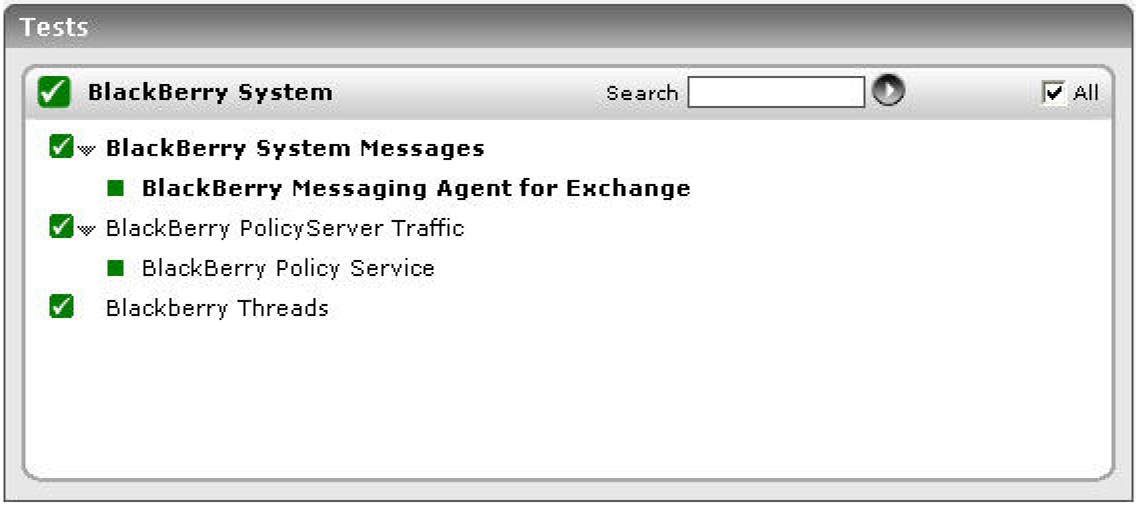

Tests
BlackBerry System
Search
All
BlackBerry System Messages
BlackBerry Messaging Agent for Exchange
BlackBerry PolicyServer Traffic
BlackBerry Policy Service
Blackberry Threads

Figure 4.5: The tests mapped to the BlackBerry System layer

4.3.1 BlackBerry System Messages Test

The BlackBerry Messaging Agent is a BlackBerry Enterprise Server component that connects to your organization's messaging server to provide messaging services, calendar management, contact lookups, attachment viewing, and attachment downloading. The BlackBerry Messaging Agent also generates device transport keys and acts as a gateway for the BlackBerry Synchronization Service to access organizer data on the messaging server.

A good indicator of the health of the messaging agent is its ability to process and deliver all messages it receives to user handhelds promptly. If too many messages remain undelivered, then, you may want to investigate the reasons for the same and plug the holes quickly, so that the messages are delivered to the device without delay. With the help of this test, you can not only determine the message load on the messaging agent at any given point in time, but can also assess how well the messaging agent handles this load.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Messaging Agent 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

Parameter	Description
	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 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
Pending messages	Indicates the number of messages that have been recognized for delivery to the BlackBerry handheld devices from the BlackBerry Enterprise Server.	Number	When the BlackBerry Enterprise Server is unable to deliver a message to a BlackBerry handheld device, the pending count on the BlackBerry Enterprise Server for that BlackBerry handheld device user will increase by one. Messages cannot be delivered to the BlackBerry handheld device if it is outside an area of wireless network coverage or is turned off. Once the BlackBerry handheld device is turned on, or returns to an area with wireless network coverage, the pending messages will be delivered. The pending count on the server will then decrease on the BlackBerry Enterprise Server.
Sent messages	Indicates the number of messages that were sent from the BlackBerry Enterprise Server to the BlackBerry handheld device during the last measurement period.	Number	
Received messages	Indicates the number of messages that were received from the BlackBerry handheld device by the BlackBerry Enterprise Server during the last measurement period.	Number	
Expired messages	Indicates the number of messages that were not delivered to the BlackBerry	Number	Ten minutes after the connection between the BlackBerry® Enterprise Server and the BlackBerry®

Measurement	Description	Measurement Unit	Interpretation
	handheld device and are subsequently purged by the Blackberry Enterprise Server during the last measurement period.		Infrastructure closes, the BlackBerry Infrastructure notifies the sender's BlackBerry handheld device and deletes the message that is not delivered. The wireless network can queue up to 5 undelivered messages for up to 7 days. If more than 5 undelivered messages exist in the queue, the BlackBerry Enterprise Server stores the messages in the BlackBerry Configuration Database. The BlackBerry Infrastructure does not store data to send to BlackBerry devices. If the BlackBerry Infrastructure is not responding and the connection closes unexpectedly, the wireless network deletes the undelivered messages. The BlackBerry device does not receive the messages and it does not send acknowledgment packets to the BlackBerry Enterprise Server. When the BlackBerry Infrastructure becomes available again, the BlackBerry Enterprise Server resends messages that it did not receive acknowledgment packets for.
Filtered messages	Indicates the number of messages that have been received by the BlackBerry Enterprise Server but not delivered to the BlackBerry handheld device during the last measurement period.	Number	These type of messages occur when you have set certain specification for messages that needs to be delivered to your BlackBerry device. Once you choose to set a filter, the messages will not be delivered to your BlackBerry device.
Used licenses	Indicates the number of users who possess valid	Number	

Measurement	Description	Measurement Unit	Interpretation
	licenses to access this BlackBerry Enterprise Server.		

4.3.2 BlackBerry PolicyServer Traffic Test

An IT policy consists of rules that define BlackBerry device security, settings for synchronizing data over the wireless network, and other behaviors for the individual groups or user accounts that you define. You can configure IT policies using the BlackBerry Administration Service.

The BlackBerry® Policy Service sends IT policies and IT administration commands to BlackBerry devices and provisions service books over the wireless network. When you activate a BlackBerry device, change an IT policy, or request that a BlackBerry® Enterprise Server resend service books, the BlackBerry Enterprise Server uses the BlackBerry Policy Service to send the updates to the BlackBerry handheld device.

If the BlackBerry Policy Service experiences overloads or processing bottlenecks, then, it may not be able to update the BlackBerry devices with critical changes in IT policies; this in turn may affect device security, user account behavior and more! Using this test, you can closely monitor the transaction load on the Policy Service, proactively detect surges in failed and pending transaction counts, and thus quickly isolate processing bottlenecks. This way, you can instantly initiate measures to clear the bottlenecks and ensure the prompt delivery of updates of devices.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Policy Service 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

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 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

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
Transactions received by policy server	Indicates the number of transactions that were received by the BlackBerry Policy Service from all the BlackBerry handheld devices during the last measurement period.	Number	
Message size	Indicates the size of the messages that were sent from the BlackBerry Policy Service to all the BlackBerry handheld devices during the last	KB	

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		
Pending requests to policy server	Indicates the number of requests that are yet to be delivered by the policy service to the BlackBerry handheld devices.	Number	A low value is desired for this measure. A consistent increase in this value could indicate a processing bottleneck.
Transactions sent by policy server	Indicates the number of transactions that were sent by the BlackBerry Policy service to all the BlackBerry handheld devices during the last measurement period.	Number	
Failed requests for policy server	Indicates the number of requests that failed to be delivered to the BlackBerry Policy Service from the BlackBerry handheld devices during the last measurement period.	Number	Ideally, the value of this measure must be 0.

4.3.3 Blackberry Threads Test

Internally, the BlackBerry Enterprise Server assigns threads to handle specific operations; for example, sending a message to a BlackBerry wireless device, or synchronizing wirelessly a delete action on the device. Occasionally, these threads can take an excessive amount of time to complete their work. When some tasks do not complete and the assigned thread becomes unresponsive, the said thread becomes a "hung thread". This test updates you with the status of threads assigned by the BlackBerry Enterprise Server, and alerts you when hung threads are detected.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Enterprise Server 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 *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
Hung threads	Indicates the current number of hung threads i.e., the threads that have been unresponsive for a period of time in the	Number	A hung thread might prevent BlackBerry device users in your organization's BlackBerry Domain from sending or receiving email messages. Therefore the value of this

Measurement	Description	Measurement Unit	Interpretation
	BlackBerry Enterprise Server.		measure must be 0.
Running threads	Indicates the number of threads that are currently running in the BlackBerry Enterprise Server.	Number	

4.4 BlackBerry Dispatcher Layer

The BlackBerry Dispatcher is designed to compress and encrypt all information sent to the BlackBerry device. The BlackBerry Dispatcher is also designed to decompress and decrypt all information that users send from the BlackBerry device, and to send that information to other BlackBerry services and components. The BlackBerry Dispatcher sends the data through the BlackBerry Router, to and from the wireless network.

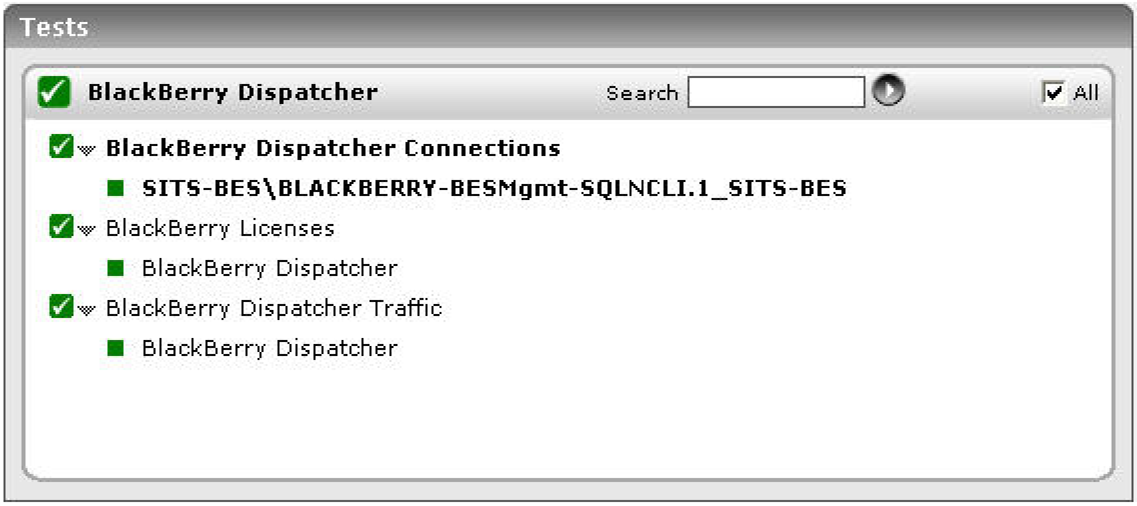
Using the tests mapped to this layer, administrators can achieve the following:

a. Understand the load on the Dispatcher;

b. Detect the non-availability of a connection with the Dispatcher;

c. Be proactively alerted to a potential delay in the Dispatcher's responsiveness to requests from devices;

d. License usage of the Dispatcher



☑ BlackBerry Dispatcher Connections

- SITS-BES\BLACKBERRY-BESMgmt-SQLNCLI.1_SITS-BES

☑ BlackBerry Licenses

- BlackBerry Dispatcher

☑ BlackBerry Dispatcher Traffic

- BlackBerry Dispatcher

Figure 4.6: The tests mapped to the BlackBerry Dispatcher layer

4.4.1 BlackBerry Dispatcher Traffic Test

To determine the load on the dispatcher, use this test.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Dispatcher operating on the BlackBerry Enterprise Server 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

Parameter	Description
	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 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
Messages sent by dispatcher	Indicates the total number of messages sent from the BlackBerry Dispatcher to the BlackBerry handheld devices.	Number	These are good indicators of the load on the dispatcher.
Messages received by dispatcher	Indicates the total number of messages received by the BlackBerry Dispatcher from the BlackBerry handheld devices.	Number	

4.4.2 BlackBerry Dispatcher Connections Test

If devices are unable to connect to the BlackBerry Dispatcher, they will neither be able to send data or receive data from the BlackBerry Infrastructure. Continuous availability of the BlackBerry Dispatcher is hence a must. This test periodically checks the connectivity between the devices and the BlackBerry Dispatcher, and promptly alerts you if devices are unable to connect to the dispatcher. In the process, the test also reveals how responsive the dispatcher is to requests from devices, and thus turns the spotlight on errors and delays in request processing by the dispatcher.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Dispatcher operating on the BlackBerry Enterprise Server 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

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 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

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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Connection state</td><td>Indicates whether the BlackBerry Dispatcher is connected to the handheld device or not.</td><td></td><td>This measure indicates whether the connection is Established or Not Established between the BlackBerry Dispatcher and the BlackBerry handheld device. The states and their equivalent numeric values are mentioned in the table below:
<table>
<tr><th>Numeric Value</th><th>State</th></tr>
<tr><td>0</td><td>Not Established</td></tr>
<tr><td>1</td><td>Established</td></tr>
</table>
<b>Note:</b></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure reports the above-mentioned **State**s while indicating the connection status of the BlackBerry Dispatcher. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents only - i.e., 0 or 1.
Average response time	Indicates the average time taken by the Messaging Dispatcher to get connected to the handheld device.	Mins	A low value is desired for this measure. A high value or a value that steadily increases could indicate a sudden/gradual deterioration in responsiveness. This would require further investigation.
Total errors	Indicates the total number of errors encountered by the BlackBerry Dispatcher when connected to the handheld device.	Number	A low value is desired for this measure. A high value or a value that steadily increases could indicate connectivity issues which would require further investigation.

4.4.3 BlackBerry Licenses Test

CAL (Client Access License) keys control how many user accounts can exist on a BlackBerry® Enterprise Server at the same time. To ensure the continued use of the BlackBerry infrastructure, adequate licenses or CAL keys need to be available on the BES.

This test reports the license usage details of the BlackBerry Dispatcher.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Dispatcher operating on the BlackBerry Enterprise Server 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 *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
Total licenses	Indicates the total number of CALs that exist for this BlackBerry Enterprise Server.	Number	
Used licenses	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
	CALs that are currently in use in this BlackBerry Enterprise Server.		
Free licenses	Indicates the total number of CALs that are still available for use in this BlackBerry Enterprise Server.	Number	
Available licenses	Indicates the percentage of unused licenses on the BES.	Number	A high value is desired for this measure. A very low value indicates that the BES may shortly run out of licenses.

4.5 BlackBerry Applications Layer

The BlackBerry Messaging Agent connects to your organization's messaging server to provide messaging services, calendar management, contact lookups, attachment viewing, and attachment downloading. The BlackBerry Messaging Agent also generates device transport keys and acts as a gateway for the BlackBerry Synchronization Service to access organizer data on the messaging server. The BlackBerry Messaging Agent synchronizes configuration data between the BlackBerry Configuration Database and user mailboxes.

The tests mapped to the **BlackBerry Applications** layer enables you to promptly detect the following:

- Connection failures to the messaging agent
- Slowdowns in the messaging agent
- Load on the messaging agent and how well the agent processes the load

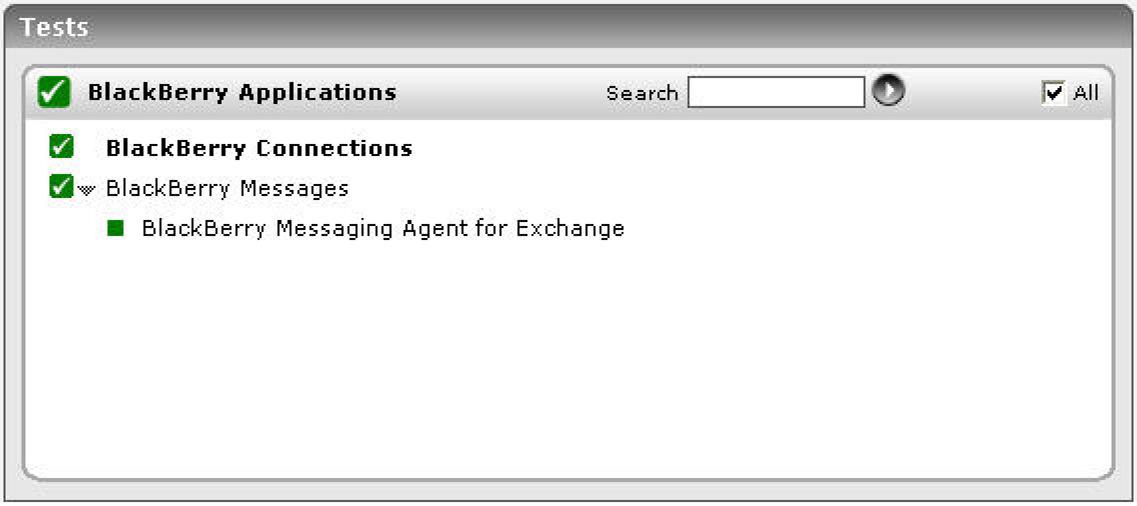

Tests
☑ BlackBerry Applications
Search
☑ All
☑ BlackBerry Connections
☑ BlackBerry Messages
🟩 BlackBerry Messaging Agent for Exchange

Figure 4.7: The tests mapped to the BlackBerry Applications layer

4.5.1 BlackBerry Connections Test

If users are unable to connect to the messaging agent using their BlackBerry devices, or are experiencing significant delays while accessing the messaging services via the agent, they are bound to be displeased with the quality of their experience with the BlackBerry infrastructure. In order to avoid user complaints, the connectivity to and the responsiveness of the messaging agent should be periodically monitored, and administrators alerted to deviations much before users notice them. The **BlackBerry Connections Details** test does just that. This test runs periodic connectivity checks on the messaging agents, and reports connection failures that occurred during the last 10 minutes. In addition, the test also reports how responsive the messaging agent is to service requests from devices, and proactively alerts administrators to potential slowdowns.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for each BlackBerry Messaging Agent operating on the BlackBerry Enterprise Server 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

Parameter	Description
	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 transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm

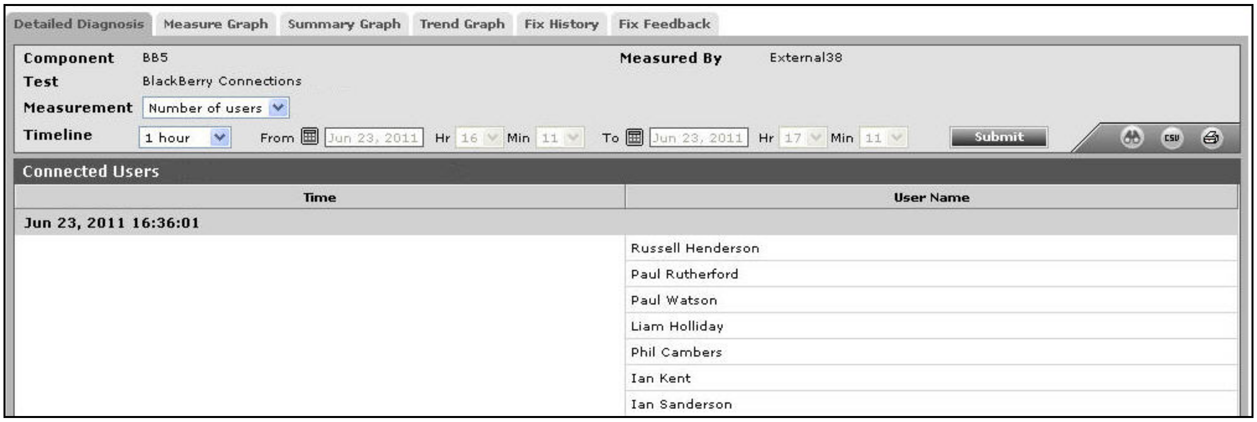
Parameter	Description
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
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
Number of users	Indicates the total number of BlackBerry users who are currently connected to the BlackBerry Messaging Agent.	Number	The detailed diagnosis of this measure shows the TimeStamp and the name of the users whose handheld devices are connected to the BlackBerry Messaging Agent.
Failed connections in the last 10 mins	Indicates the number of times the handheld devices have failed to connect to the Messaging Agent in the last 10	Number	A low value is desired for this measure. A high value indicates persistent issues in connectivity. This could be owing to a poor network connection or improper configuration or device or

Measurement	Description	Measurement Unit	Interpretation
	minutes.		domain failure.
Average response time	Indicates the average time taken by the handheld device to get connected to the Messaging Agent.	Mins	A high value or a value that steadily increases could indicate a sudden/gradual deterioration in responsiveness. This would require further investigation.

The detailed diagnosis of the *Number of users* measure shows the TimeStamp and the name of the users whose handheld devices are currently connected to the BlackBerry Messaging Agent.



Component BB5

Test BlackBerry Connections

Measured By External38

Measurement Number of users

Timeline 1 hour From Jun 23, 2011 Hr 16 Min 11 To Jun 23, 2011 Hr 17 Min 11

Connected Users

Time	User Name
Jun 23, 2011 16:36:01	
	Russell Henderson
	Paul Rutherford
	Paul Watson
	Liam Holliday
	Phil Cambers
	Ian Kent
	Ian Sanderson

Figure 4.8: The detailed diagnosis of the Number of users measure

4.5.2 BlackBerry Messages Test

A good indicator of the health of the messaging agent is its ability to process and deliver all messages it receives to user handhelds promptly. If too many messages remain undelivered, then, you may want to investigate the reasons for the same and plug the holes quickly, so that the messages are delivered to the device without delay. With the help of this test, you can not only determine the message load on the messaging agent at any given point in time, but can also assess how well the messaging agent handles this load.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Messaging Agent 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 *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
Failed messages	Indicates the total number of messages that the Messaging Agent failed to process during the last measurement period.	Number	A low value is desired for this measure. A high value or a value that increases steadily indicates that the messaging agent is experiencing processing bottlenecks. Further

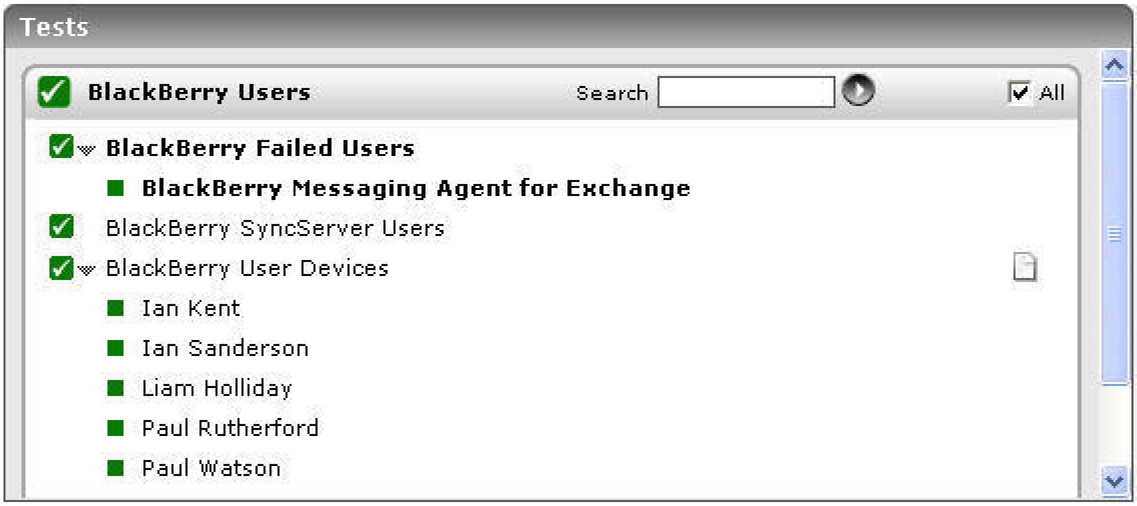
Measurement	Description	Measurement Unit	Interpretation
			investigation is hence recommended.
Pending messages	Indicates the number of messages that have been recognized for delivery to the BlackBerry handheld devices from the messaging agent.	Number	When the BlackBerry Enterprise Server is unable to deliver a message to a BlackBerry handheld device, the pending count on the BlackBerry Enterprise Server for that BlackBerry handheld device user will increase by one. Messages cannot be delivered to the BlackBerry handheld device if it is outside an area of wireless network coverage or is turned off. Once the BlackBerry handheld device is turned on, or returns to an area with wireless network coverage, the pending messages will be delivered. The pending count on the server will then decrease on the BlackBerry Enterprise Server.
Expired messages	Indicates the number of messages that were not delivered to the BlackBerry handheld device and are subsequently purged by the Blackberry Enterprise Server during the last measurement period.	Number	Ten minutes after the connection between the BlackBerry® Enterprise Server and the BlackBerry® Infrastructure closes, the BlackBerry Infrastructure notifies the sender's BlackBerry handheld device and deletes the message that is not delivered. The wireless network can queue up to 5 undelivered messages for up to 7 days. If more than 5 undelivered messages exist in the queue, the BlackBerry Enterprise Server stores the messages in the BlackBerry Configuration Database. The BlackBerry Infrastructure does not store data to send to BlackBerry devices.

Measurement	Description	Measurement Unit	Interpretation
			If the BlackBerry Infrastructure is not responding and the connection closes unexpectedly, the wireless network deletes the undelivered messages. The BlackBerry device does not receive the messages and it does not send acknowledgment packets to the BlackBerry Enterprise Server. When the BlackBerry Infrastructure becomes available again, the BlackBerry Enterprise Server resends messages that it did not receive acknowledgment packets for.

4.6 BlackBerry Users Layer

The tests mapped to this layer monitor the user connections to the BES and report the following:

- The number of failed user connections;
- The number and names of users who have disabled VPN, Wifi, and BBR on their devices;
- The users with devices that are running low on battery charge, signal strength, and flash memory;
- The users with the maximum number of pending and failed messages on the BES;



Tests

☑ BlackBerry Users Search ☑ All

☑ BlackBerry Failed Users

🟩 BlackBerry Messaging Agent for Exchange

☑ BlackBerry SyncServer Users

☑ BlackBerry User Devices

🟩 Ian Kent

🟩 Ian Sanderson

🟩 Liam Holliday

🟩 Paul Rutherford

🟩 Paul Watson

Figure 4.9: The tests mapped to the BlackBerry Users layer

4.6.1 BlackBerry Failed Users Test

Many factors influence a user's experience with the BlackBerry Infrastructure. Notable among them are a user's inability to initialize with the BlackBerry Enterprise Server, and processing bottlenecks in the BES that cause user transactions to be processed slowly. This test monitors both these factors, and hence serves as a good measure of the user experience with BES.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Messaging Agent 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

Parameter	Description
	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.
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

Parameter	Description
	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
Failed users	Indicates the number of users who failed to initialize with the BES.	Number	A low value is desired for this measure. A high value is a cause for concern. User initializations can fail owing to a general communication failure or because the MAPI Profile(s) of users got corrupted or due to issues with the BES Management database.
Pending transactions	Indicates the total number of transactions that were pending in the processing queue of the BlackBerry Enterprise Server.	Number	A low value is desired for this measure. A high value or a value that increases suddenly may indicate a processing bottleneck in the BlackBerry Enterprise server.

4.6.2 BlackBerry SyncServer Users Test

This test reports the status of user connections to Wifi, VPN, and BBR, and also reveals the names of users who are currently connected to and not connected to Wifi, VPN and BBR.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the BlackBerry Enterprise Server being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed

Parameter	Description
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 transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm

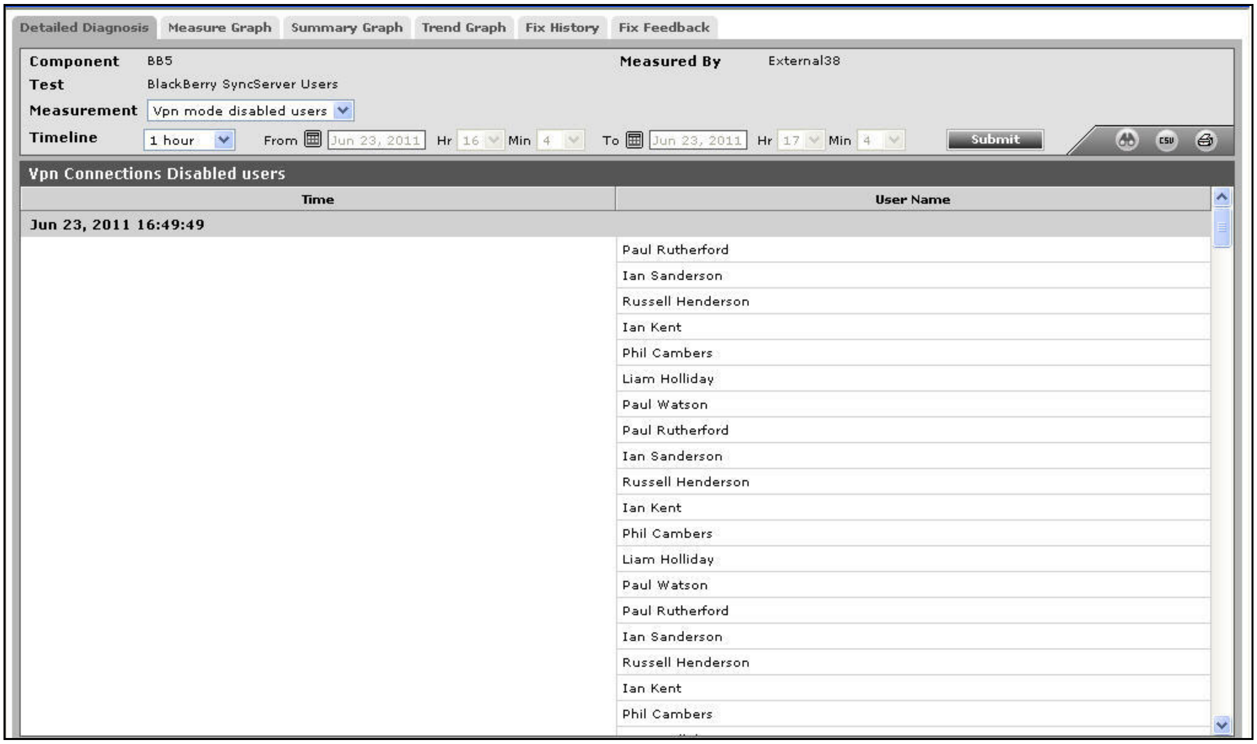
Parameter	Description
	• **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are 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
Vpn mode enabled users	Indicates the number of BlackBerry users who are currently connected to Virtual Private Networks.	Number	Use the detailed diagnosis of this measure for the names of users who are currently connected to VPN.
Vpn mode disabled users	Indicates the number of users with VPN-enabled devices, but who are not connected to Virtual	Number	Use the detailed diagnosis of this measure for the names of users who are not connected to VPN currently.

Measurement	Description	Measurement Unit	Interpretation
	Private Networks, currently.		
Wifi mode enabled users	Indicates the number of users who are currently connected to the wireless network.	Number	Use the detailed diagnosis of this measure for the names of users who are currently connected to the wireless network.
Wifi mode disabled users	Indicates the number of users with Wifi-enabled devices, but who are currently not connected to the wireless network.	Number	Use the detailed diagnosis of this measure for the names of users who are not currently connected to the wireless network.
Bbr mode enabled users	Indicates the number of users who are currently connected to the BlackBerry Router.	Number	Use the detailed diagnosis of this measure for the names of users who are currently connected to BBR.
Bbr mode enabled users	Indicates the number of users with BBR-enabled devices, who are not currently connected to the BlackBerry Router.	Number	Use the detailed diagnosis of this measure for the names of users who are not connected to the BBR, currently.

The detailed diagnosis of the *Vpn mode disabled users* measure will reveal the names of users with VPN-enabled devices, who are not connected to VPN currently.



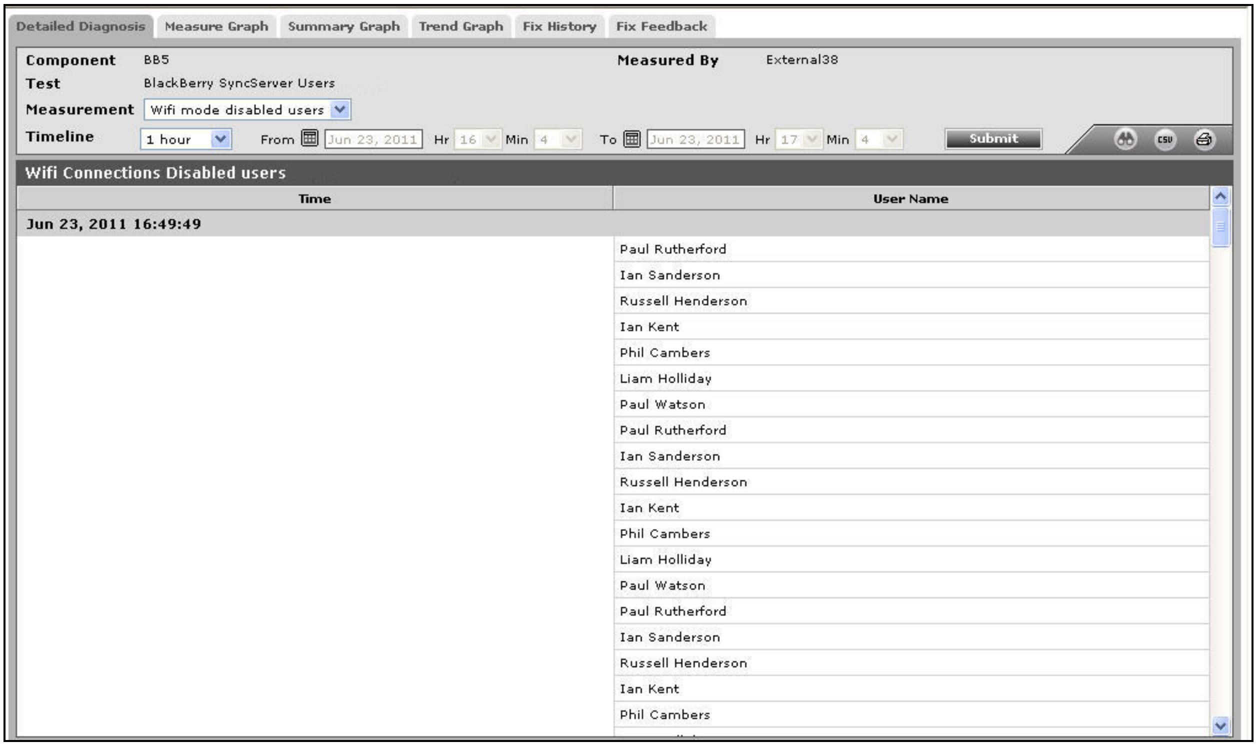
Component	BB5	**Measured By**	External38
Test	BlackBerry SyncServer Users		
Measurement	Vpn mode disabled users		
Timeline	1 hour	From Jun 23, 2011 Hr 16 Min 4	To Jun 23, 2011 Hr 17 Min 4

Vpn Connections Disabled users

Time	User Name
Jun 23, 2011 16:49:49	
	Paul Rutherford
	Ian Sanderson
	Russell Henderson
	Ian Kent
	Phil Cambers
	Liam Holliday
	Paul Watson
	Paul Rutherford
	Ian Sanderson
	Russell Henderson
	Ian Kent
	Phil Cambers
	Liam Holliday
	Paul Watson
	Paul Rutherford
	Ian Sanderson
	Russell Henderson
	Ian Kent
	Phil Cambers

Figure 4.10: The detailed diagnosis of the Vpn mode disabled users

The detailed diagnosis of the *Wifi mode disabled users* measure will reveal the names of users with Wifi-enabled devices, who are not currently connected to the wireless network.



Component BB5

Measured By External38

Test BlackBerry SyncServer Users

Measurement Wifi mode disabled users

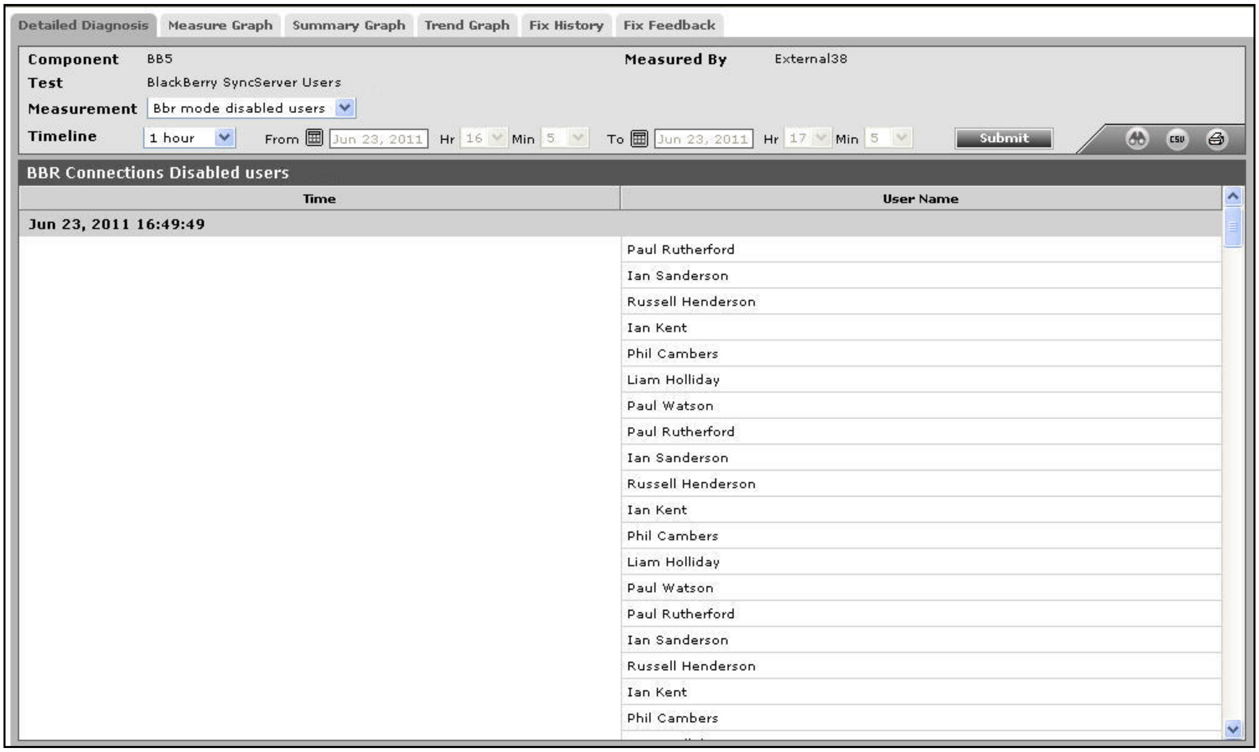
Timeline 1 hour From Jun 23, 2011 Hr 16 Min 4 To Jun 23, 2011 Hr 17 Min 4

Wifi Connections Disabled users

Time	User Name
Jun 23, 2011 16:49:49	
	Paul Rutherford
	Ian Sanderson
	Russell Henderson
	Ian Kent
	Phil Cambers
	Liam Holliday
	Paul Watson
	Paul Rutherford
	Ian Sanderson
	Russell Henderson
	Ian Kent
	Phil Cambers
	Liam Holliday
	Paul Watson
	Paul Rutherford
	Ian Sanderson
	Russell Henderson
	Ian Kent
	Phil Cambers

Figure 4.11: The detailed diagnosis of the Wifi mode disabled users measure

The detailed diagnosis of the *Bbr mode disabled users* measure will reveal the names of users who are not currently connected to the BlackBerry Router.



Component BB5

Measured By External38

Test BlackBerry SyncServer Users

Measurement Bbr mode disabled users

Timeline 1 hour From Jun 23, 2011 Hr 16 Min 5 To Jun 23, 2011 Hr 17 Min 5

BBR Connections Disabled users

Time	User Name
Jun 23, 2011 16:49:49	
	Paul Rutherford
	Ian Sanderson
	Russell Henderson
	Ian Kent
	Phil Cambers
	Liam Holliday
	Paul Watson
	Paul Rutherford
	Ian Sanderson
	Russell Henderson
	Ian Kent
	Phil Cambers
	Liam Holliday
	Paul Watson
	Paul Rutherford
	Ian Sanderson
	Russell Henderson
	Ian Kent
	Phil Cambers

Figure 4.12: The detailed diagnosis of the Bbr mode disabled users

4.6.3 BlackBerry User Devices Test

This test auto-discovers the BlackBerry handheld devices that are connected to the BlackBerry Enterprise Server and reports the health of each device. Devices running low on flash memory, signal strength, and battery charge can thus be isolated.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for each user's BlackBerry device that is connected to the BlackBerry Enterprise Server 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

Parameter	Description
	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 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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Network type</td><td>Indicates the type of radio communication technology used by this user's BlackBerry handheld device to communicate over a wireless network.</td><td></td><td>The network types reported by this measure and their corresponding numeric equivalents are described below:
<table>
<tr><th>Numeric Value</th><th>Type</th></tr>
<tr><td>1</td><td>GPRS</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>Numeric Value</th><th>Type</th></tr><tr><td>2</td><td>3G</td></tr><tr><td>3</td><td>IDEN</td></tr><tr><td>4</td><td>CDMA</td></tr><tr><td>5</td><td>802.11</td></tr><tr><td>6</td><td>UNKNOWN</td></tr></table>
<b>Note:</b>
By default, this measure reports the above-mentioned <b>Type</b>s while indicating the types of radio communication technology. However, in the graph of this measure, the types will be represented using the corresponding numeric equivalents only - i.e., 1 to 6.</td></tr>
<tr><td>Available flash memory</td><td>Indicates the available number of flash memory blocks in this user's BlackBerry handheld device.</td><td>Number</td><td>Flash memory (sometimes called "flash RAM") is a type of constantly-powered nonvolatile memory that can be erased and reprogrammed in units of memory called blocks. It is a variation of electrically erasable programmable read-only memory (EEPROM) which, unlike flash memory, is erased and rewritten at the byte level, which is slower than flash memory updating.
If the BlackBerry handheld device runs low on flash memory, you may clear the browser cache to free up space, or you may choose to manually clear the pushed content cache.</td></tr>
<tr><td>Signal strength</td><td>Indicates the signal strength of this user's BlackBerry handheld device.</td><td>dBm_negative</td><td>The typical range of this measure is from -121 dBm to -40 dBm. A value of -256 indicates that no radio coverage i.e., network is available. The higher the negative value, the signal strength</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			is stronger.
Available battery charge	Indicates the available battery power in this user's BlackBerry handheld device.	Percent	Low battery power indicates that the BlackBerry handheld device needs to be charged.

4.6.4 BlackBerry User Messages Test

Whenever the BlackBerry Enterprise server experiences processing bottlenecks or flaky connectivity with the BlackBerry devices, the delivery of messages to the devices is bound to be affected. Anomalies can range from a delay in delivery to total failure of the delivery mechanism. To assess the extent of the damage, administrators would need to know the length of the pending message queue, the count of failed messages, and also the number and names of users who are affected by the delay/delivery failure. The **BlackBerry User Message Details** test provides this information. For every user whose BlackBerry device is connected to BES, this test reports the number of pending messages, failed messages, and expired messages, so that administrators can accurately identify the devices/users who were worst hit by processing delays/failures in the BES.

Target of the test : A BlackBerry Enterprise Server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for each user's BlackBerry device that is connected to the BlackBerry Enterprise Server 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 *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

Parameter	Description
	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
Filtered messages	Indicates the number of messages that were filtered based on the filter preferences set by this user on his/her BlackBerry handheld device during the last measurement period.	Number	By using the Filter option, the user provides directions to the BlackBerry server to automatically redirect the email messages to the specified location or the user can just try to block the messages using this option.
Pending messages	Indicates the number of messages that were waiting to be delivered to this user's BlackBerry handheld device.	Number	When the BlackBerry Enterprise Server is unable to deliver a message to a BlackBerry handheld device, the pending count on the BlackBerry Enterprise Server for that BlackBerry handheld device user will increase by one.

Measurement	Description	Measurement Unit	Interpretation
			Messages cannot be delivered to the BlackBerry handheld device if it is outside an area of wireless network coverage or is turned off. Once the BlackBerry handheld device is turned on, or returns to an area with wireless network coverage, the pending messages will be delivered. The pending count on the server will then decrease on the BlackBerry Enterprise Server. Comparing the value of this measure across users will help you identify to which user the maximum number of pending messages were addressed.
Expired messages	Indicates the number of messages that were not delivered to this user's BlackBerry handheld device and are subsequently purged by the Blackberry Enterprise Server during the last measurement period.	Number	Ten minutes after the connection between the BlackBerry® Enterprise Server and the BlackBerry® Infrastructure closes, the BlackBerry Infrastructure notifies the sender’s BlackBerry device and deletes the message that is not delivered. The wireless network can queue up to 5 undelivered messages for up to 7 days. If more than 5 undelivered messages exist in the queue, the BlackBerry Enterprise Server stores the messages in the BlackBerry Configuration Database. The BlackBerry Infrastructure does not store data to send to BlackBerry devices. If the BlackBerry Infrastructure is not responding and the connection closes unexpectedly, the wireless network deletes the undelivered messages. The BlackBerry device does not

Measurement	Description	Measurement Unit	Interpretation
			receive the messages and it does not send acknowledgment packets to the BlackBerry Enterprise Server. When the BlackBerry Infrastructure becomes available again, the BlackBerry Enterprise Server resends messages that it did not receive acknowledgment packets for. Comparing the value of this measure across users will help you identify to which user the maximum number of expired messages were originally addressed.
Failed messages	Indicates the number of email messages that the messaging agent received from this user's BlackBerry handheld device and was unable to process during the last measurement period.	Number	Comparing the value of this measure across users will help you identify which user's messages failed the most.
Forwarded messages	Indicates the number of messages that were forwarded to this user's BlackBerry handheld device from the BlackBerry Enterprise Server during the last measurement period.	Number	
Failed connections	Indicates the number of times the connection between the BlackBerry Enterprise Server and this user's BlackBerry handheld device failed during the last measurement period.	Number	Comparing the value of this measure across users will help you identify which user's handheld experienced the maximum number of connection failures. You may want to investigate the network links between such devices and the BES to ascertain the reasons for the frequent failures.

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.