# BlackBerry Enterprise Mobility Server

## Monitoring and reporting

Administration

3.5

# Contents

# Monitoring BEMS

You can monitor the health and status of BEMS instances, users, and nodes using the monitoring tools. You can also monitor the status of the BEMS services using log files.

# Monitoring probes and tools

If you have BEMS installed in your environment, you can use monitoring probes to monitor the health and status of your BEMS instances, users, and and nodes. To use monitoring probes, you must enable them. You can run the monitoring tools and use the monitoring probes on the computers that host BEMS or from a remote computer. You can use the following monitoring tools:

- Java Management Extensions (JMX)-compliant monitoring tools: Use this tool to monitor the Mail (Push Notifications) and BEMS-Docs services on the BEMS nodes (for example, notification success and failures, the state of devices and users, average required time of upload and download, and failures).
- Health service servlet: Use this servlet to monitor the health and system status of a specific BEMS node in your environment.

## Monitoring probes

The following table describes the monitoring probes you can use to view additional information for the health of your BEMS server and users. You can use monitoring probes to view information for a BEMS instance locally or from a remote computer.

**Note:** To use monitoring probes in your environment, you must enable them. If you are using the health service servlet, see Enable the health service servlet.

| Probe name | cURL Command | Output description |
|---|---|---|
| Push Notification Counter | Type `curl -k -i -X GET \ -H "Content-Type:application/json" \ -H "Authorization:Basic ZG9tYWluXHVzZXI6cGFzc3dvcmQ=" \ 'https://<BEMS instance name> :8443/monitor/push.notifications'` | **SuccessfulPushes**<br>This probe specifies the number of push notifications, per push notification type (for example, APNS, GNP, and GCM) that have the instance sent for users supported by this instance.<br>You want to see the number increase over short intervals of time. If it stops rising then BEMS is not sending any push notifications. |
| Total user count | Type `curl -k -i -X GET \ -H "Content-Type:application/json" \ -H "Authorization:Basic ZG9tYWluXHVzZXI6cGFzc3dvcmQ=" \ 'https://<BEMS instance name>:8443/monitor/mail.users/UsersCount'` | **UsersCount**<br>This probe specifies the total number of users across the BEMS cluster which successfully registered a device and are successfully auto discovered by BEMS. The UsersCount does not reflect the number of devices receiving push notifications. |

| Probe name | cURL Command | Output description |
|---|---|---|
| Stale user count | type `curl -k -i -X GET \ -H "Content-Type:application/json" \ -H "Authorization:Basic ZG9tYWluXHVzZXI6cGFzc3dvcmQ=" \ 'https://<BEMS instance name>:8443/monitor/mail.users/StaleUsersCount'` | **StaleUsersCount**<br>This probe specifies the total number of users across the BEMS cluster which successfully registered a device, but for which BEMS is no longer sending push notifications because the device hasn't registered in the past 72 hours. |
| EWS user count | Type `curl -k -i -X GET \ -H "Content-Type:application/json" \ -H "Authorization:Basic ZG9tYWluXHVzZXI6cGFzc3dvcmQ=" \ 'https://<BEMS instance name>:8443/monitor/mail.ewslistener/EWSUserStats'` | **EWSConnectedUserCount**<br>This probe specifies the number of users on the Microsoft Exchange Web Services instance, for which BEMS connects to the Microsoft Exchange Server, and is attempting to monitor the users' mailboxes. This EWSConnectedUserCount reflects the number of users most likely to be receiving push notifications unless BEMS is experiencing errors with its Microsoft Exchange Web Services connections to the Microsoft Exchange Server.<br>The EWSConnectedUserCount should be equal across all Microsoft Exchange Web Services instances in a cluster. If this count drops to 0 then the Microsoft Exchange Web Services instance is not servicing any user mailboxes. |

# Java Management Extensions (JMX)-compliant monitoring tools

You can now use Java Management Extensions (JMX)-compliant monitoring tools to monitor the Mail (Push Notifications) and BEMS-Docs services. JMX is a Java Standard which is compatible with many tool suites including JConsole which is distributed with every JDK installation.

## Monitoring the status of Push Notifications using JMX-compliant monitoring tools

You can view the status of the BEMS node on Push Notifications statistics including the following:

- The state of devices and users.
- Notification success and failure
- The time of the last notification received
- The state of the BEMS infrastructure, such as processing time and response to database requests

## Monitoring the status of the BEMS-Docs service using JMX-compliant monitoring tools

You can view the status of the BEMS node on BEMS-Docs statistics including the following:

- The average completion time of upload and download requests

- The average completion time of requests
- The number of requests sent to supported storage providers (for example, CMIS and Microsoft SharePoint on-premises and Microsoft SharePoint Online)
- Request, upload, and download success and failure

## Monitoring attributes

The following table describes the statistics that you can use to monitor the health of BEMS server, users, and BEMS-Docs using the monitoring tool.

| Statistic | Description |
|---|---|
| **Push Notifications** | |
| RelayStats | **<*notification type*>RelayStats**<br>This attribute specifies the number of push notifications for each push notification type (for example, APNS, GNP, and FCM). If this number stops rising, then BEMS is not sending any push notifications.<br>The numbers should increase over short intervals. |
| EWSStats | **EWSConnectedUserCount**<br>This attribute specifies the number of users on the Microsoft Exchange Web Services instance that BEMS uses to connect to the Microsoft Exchange Server so that it can monitor the users' mailboxes. This attribute reflects the number of users most likely to be receiving push notifications unless BEMS is experiencing errors with its Microsoft Exchange Web Services connections to the Microsoft Exchange Server.<br>The EWSConnectedUserCount should be equal across all Microsoft Exchange Web Services instances in a cluster. If this count drops to 0, then the Microsoft Exchange Web Services instance is not servicing any user mailboxes. |
| UserStats | **UsersCount**<br>This attribute specifies the total number of users across the BEMS cluster which successfully registered a device and are successfully autodiscovered by BEMS. The UsersCount does not reflect the number of devices receiving push notifications.<br>**StaleUsersCount**<br>This attribute specifies the total number of users across the BEMS cluster that BEMS is no longer sending push notifications to because the devices that were registered previously haven't registered in the past 72 hours. |
| HealthStats | **HealthStats**<br>This attribute specifies the overall health of the BEMS status, including health of consumer threads, producer threads, ActiveMQ, and access to the database. |

| Statistic | Description |
|---|---|
| ClientAPIStats | **ClientAPIStats**<br>This attribute identifies generic problems with the BEMS service by monitoring the average and maximum processing time of requests to the BEMS database. This statistic is for the last minute only. For example, if the LookupUser is {Min:10, Max:90000, Average:50000, Count:26}, it means that BEMS received 26 LookupUser requests in the last minute and the average duration is 50,000 milliseconds. |
| DatabaseStats | **DatabaseStats**<br>This attribute can identify common failure points for the BEMS Infrastructure. This attribute monitors statistics such as the average, maximum, minimum, and number of requests to BEMS if the NumOfRequests is 25, it means BEMS received 25 database requests in the last minute. If the database stops, the processing time displays **Infinity**. |
| AutodiscoverStats | **EAS**<br>This attribute specifies the total number of successful or failed Active Directory requests for EAS client requests.<br>**EWS**<br>This attribute specifies the total number of successful or failed Active Directory requests for all EWS requests and client requests.<br>**Tests**<br>This attribute specifies the total number of successful or failed Active Directory requests for both EWS and EAS tests. |
| **BEMS-Docs** | |
| DocsConfigInfo | This attribute specifies the overall BEMS-Docs configuration information, including the version of BEMS that is installed, the status of all bundles, and database status. |
| DocsServices | This attribute specifies overall health of the BEMS-Docs service, including the total number of requests, downloads, and uploads with the average processing time. The success and failure of the statistics are also included. |
| DocsStorageProviders | This attribute specifies the total number of requests and downloads to a specific fileshare (for example, Microsoft SharePoint, Microsoft SharePoint Online, CMIS, and Box). |

## Enabling monitoring the health of BEMS

When you enable JMX to view monitoring attributes, you complete the following actions.

| Step | Action |
| --- | --- |
| 1 | Enable JMX. |
| 2 | To enable remote access, Update the RMI Server Host IP address for remote access. |
| 3 | View statistics using the JMX tool. |

#### Enable JMX

You must modify the GoodServerDistribution-wrapper.conf file on the computer that hosts the BEMS instance to allow jconsole to connect to BEMS and view the monitoring attributes. By default, this feature is disabled.

1. In a text editor, navigate to the GoodServerDistribution-wrapper.conf file. By default, this file is located in <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\etc. Make a backup of this file and save it to your desktop.
2. Below the **# Use the Garbage First (G1) Collector** section, uncomment the following properties:
   - wrapper.java.additional.<*n*>=-Dcom.sun.management.jmxremote.port=<*port*>
   - wrapper.java.additional.<*n*>=-Dcom.sun.management.jmxremote.authenticate=false
   - wrapper.java.additional.<*n*>=-Dcom.sun.management.jmxremote.ssl=false

   Where <*n*> must be changed to the next unique, incremental identifier in the GoodServerDistribution-wrapper.conf file. For example, in the following example, you must change the <*n*> for jmxremote.port to 23.

   ```
   # Needed for Certicom Security Provider
   wrapper.java.additional.19=-Dcerticom.keyagreement.ecdh=rawECDH
   # Use the Garbage First (G1) Collector
   wrapper.java.additional.20=-XX:+UseG1GC
   wrapper.java.additional.21=-Djava.security.properties="%KARAF_ETC%/
   java.security"
   wrapper.java.additional.22=-Dkeystore.pkcs12.legacy
   # Uncomment to enable
   wrapper.java.additional.n=-Dcom.sun.management.jmxremote.port=1616
   wrapper.java.additional.n=-Dcom.sun.management.jmxremote.authenticate=false
   wrapper.java.additional.n=-Dcom.sun.management.jmxremote.ssl false
   ```
3. Record the port number. This port number is required to log in to jconsole and access BEMS locally and remotely.
4. Save and close the file.
5. Restart the Good Technology Common Services service.

#### Update the RMI Server Host IP address for remote access

To enable remote access to the computer that hosts BEMS, you must update the default RMI Server Host IP address.

**Before you begin:**

- Make sure that you have enabled JMX.

1. On the BEMS Karaf Console, open a browser window and navigate to https://<*BEMS instance hostname*>:8443/system/console/configMgr.
2. Scroll to and click **Apache Karaf JMX Management**.
3. Search for **RMI Server Host** enter the IP address of the computer that hosts the remote BEMS.
4. Save and close the file.
5. Restart the Good Technology Common Services service.

#### View statistics using the JMX tool

**Before you begin:**

- Verify that jconsole is available on the computer that is used to connect to the Java Management extensions (JMX) on the BEMS. The jconsole comes as part of every Java Development Kit (JDK).
- Verify that you have the port number from Enable JMX.
- If you connect remotely, verify that you have the RMI Server Host from Update the RMI Server Host IP address for remote access.

1. Open the jconsole app on the computer that hosts the service that you want to view statistics (Push Notifications service or BEMS-Docs service). By default, the app is located in <*drive*>:\%JAVA_HOME%\bin.
2. In the **Remote Process** field, enter the *hostname*:*port*. Where the hostname and port are the following:
   - If you log on locally, the hostname is 127.0.0.1.
   - If you log on remotely, the hostname is the RMI Server Host that you specified in Update the RMI Server Host IP address for remote access.
   - The port number that you recorded from Enable JMX.
3. Click **Connect**.
4. Click **Insecure connection**.
5. In the **Java Monitoring & Management Console**, click the **MBeans** tab.
6. Do any of the following:

| View Statistics | Steps |
|---|---|
| **Push Notifications** | |
| View statistics about the FCM, GCM, APNS, and APNS push notifications. | Click **com.good.gcs.notifications > instance > RelayStats > Attributes**. |
| View statistics about users on the Microsoft Exchange Web Services instance. | Click **com.good.gcs.pushnotify > instance > EWSStats > Attributes**. |
| View statistics about users in the BEMS cluster that have registered a device. | Click **com.good.gcs.pushnotify > instance > UserStats > Attributes**. |
| View the overall health of BEMS. | Click **com.good.gcs.core.health > instance > HealthStats > Attributes**. |
| View the client API status statistics for the previous minute for requests received by BEMS. | Click **com.good.gcs.clientapi > instance > Client API Status > Attributes**. |
| View the average, maximum, minimum, and number of requests to the BEMS database. | Click **com.good.gcs.database > instance > DatabaseStats > Attributes**. |

| View Statistics | Steps |
|---|---|
| View statistics for EAS and EWS Autodiscover and administrator functions. | Click **com.good.gcs.pushnotify > instance > AutodiscoverStats**. |
| **BEMS-Docs** | |
| View the overall BEMS-Docs configuration information. | Click **com.good.server.docs.monitoring > instance > DocsConfigInfo** |
| View statistics about success and failure of BEMS-Docs uploads, downloads, requests, and the average process duration. | Click **com.good.server.docs.monitoring > instance > DocsServices** |
| View statistics about the number of requests and downloads by storage providers. | Click **com.good.server.docs.monitoring > instance > DocsStorageProviders** |

# Monitoring the health status of a node

You can enable the health service servlet to monitor the health and system status of a node in your environment. The health and system status is specific to the node that the feature is enabled on. It does not provide health information on a cluster in the environment. By default, this feature is disabled and must be enabled on each node in the environment.

When you enable the health service servlet, you complete the following actions.

| Step | Action |
|---|---|
| 1 | Configure the node for BEMS to authenticate with the authentication source. |
| 2 | Enable the health service servlet. |
| 3 | Run the health checks on a node. |

## Configure the node for BEMS to authenticate with the authentication source

You must configure the node to allow BEMS to authenticate with the authentication source (realm) in Karaf before you can enable the health service servlet to monitor the health and system status of a node in your environment.

1. On the computer that hosts BEMS, open the **BEMS Karaf Console**. Open a browser window and navigate to https://<*BEMS instance hostname*>:8443/system/console/configMgr.
2. Enter your login credentials.
3. Scroll to and click **com.good.gcs.monitor.MonitorComponent.name**.
4. In the **com.good.gcs.monitor.MonitorComponent.realm.name** field, type `gems-ad`.
5. In the **com.good.gcs.monitor.MonitorComponent.role.name** field, type `admin`.
6. Click **Save**.

### Enable the health service servlet

**Before you begin:** Make sure that you have configured the node for BEMS to authenticate with the authentication source.

1. On the computer that hosts BEMS, open the **BEMS Karaf Console**. Open a browser window and navigate to https://<*BEMS instance hostname*>:8443/system/console/configMgr.
2. Enter your login credentials.
3. Scroll to and click **com.good.gcs.core.health.HealthServiceImpl.name**.
4. In the **com.good.gcs.core.health.HealthServiceImpl.healthCheck.enabled.name** field, type `true`.
5. Click **Save**.
6. Restart the Good Technology Common Services.

### Run the health checks on a node

For information about monitoring probes, see Monitoring probes.

**Before you begin:** Enable the health service servlet

1. On the computer that hosts BEMS, open a browser and complete one of the following tasks:
   - To monitor the node health statistics: type `https://`*`BEMS instance hostname`*`:8443/monitor/`
   - To monitor the node's health at a higher level (for example, including health information about BEMS, type `https://`*`BEMS instance hostname`*`:8443/health`
2. If you are prompted, enter your credentials. Press **OK**.

# Using BEMS log files

You can use BEMS log files to identify and troubleshoot issues with the BEMS services in your organization's environment. Logging capabilities allow you to:

- Track the activity of the BEMS components using the BEMS logs
- Log critical instant messaging server information used in your environment
- Audit user activity such as user upload and download of files
- Track user presence status information

The Mail (Push Notifications) service and the Connect service log files are independent. The Presence service and the Docs service log files are logged to the BEMS-Core log files. For more information about logging and how to change the logging level for specific BEMS components, visit support.blackberry.com/community to read article 42408.

# Push Notifications (Mail) log files

The BlackBerry Push Notifications (Mail) log files provide diagnostic information to assist in troubleshooting and monitoring the service. These log files are located in the BEMS Karaf Console. To give login and configuration permissions to members of the administration group, see "Add dashboard administrators" in the BEMS Core content.

The log files are stored in the bemlogs. By default, the log files are located in: `C:\blackberry\bemslogs`.

## View relevant logs in the BEMS Karaf Console

The BEMS Karaf Console provides advanced configuration and tuning options for BEMS. It should be used with care as it offers advanced maintenance capabilities intended for expert users of the system.

1. Open a browser and go to the BEMS Karaf Console located at `https://localhost:8443/system/console/logs` and login as administrator with the appropriate Microsoft Active Directory credentials.
2. Scroll through the log activity. It's listed in chronological order and displays the last 100 log lines.

**After you finish:** You can view the logs from the BEMS installation directory.

## Troubleshooting: Push Notifications (Mail) log files

### BEMS cannot connect to the Push Notifications database

#### Possible cause

The Microsoft Exchange configuration information was applied before the Database information.

#### Possible solution

1. Restart the Good Technology Common Services.
2. Verify the Database information. For instructions, see "Configure the Microsoft SQL Server database for Push Notifications service" in the Mail configuration content.
3. Repopulate the Microsoft Exchange Server information. For instructions, see "Configure BEMS to communicate with the Microsoft Exchange Server or Microsoft Office 365" in the Mail configuration content.

# BlackBerry Connect log files

BEMS-Connect service logs information in different log files and saves them to the different folder locations depending on the installation configuration of the BEMS-Connect service. These log files are required when troubleshooting Connect issues. The log files contain critical information for the instant messaging server that is used in your environment (for example, Microsoft Lync Server, Cisco Unified Communications Manager for communications, and Skype for Business using non-trusted application mode or trusted application mode).

## Finding log files for the Connect service

By default, a server log file is created for each BEMS server and is stored daily on the computer that hosts BEMS.

BEMS-Core log files are displayed as gems_<*server_name_date_time stamp*>.log. By default, the BEMS log files are stored daily in `C:\BlackBerry\bemslogs`. The Connect service logs related information in the BEMS-Core log files for Cisco Unified Communications Manager, and Skype for Business when the environment is configured for non-trusted application mode.

**Note:** The timestamp for each file is reset daily at 0:00 (midnight). It is also reset each time that the Good Technology Connect or Good Technology Common Services service is restarted and when a maximum file size is reached.

The following table summarizes the log files that are generated by the BEMS-Connect service.

| Log file | Default log file location | Description |
|---|---|---|
| `Connect_<server_name>_<date_time_stamp>.log` | `C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect\Logs` | • This log file logs BlackBerry Connect app connections data.<br>• In Microsoft Lync Server or Skype for Business on-premises using trusted application mode environments, this log also logs all of the service log data including communications with the instant messaging platform.<br>• The log file is reset when it reaches a maximum of 20 MB and a new log file is started. The log files are automatically deleted after three days.<br>• The BEMS-Connect service log4net.config file controls the information that is logged in the log file. For more information, visit http://support.blackberry.com/community to read article 41080. |

| Log file | Default log file location | Description |
|---|---|---|
| Connect-LongTerm_<*server_name*>_<*date_time_stamp*>.log | C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect\Logs | • This log file logs similar information to the Connect_<*server_name*>_<*date_time_stamp*>.log file (above) over a longer duration, but with less details. For example, this log file only logs some INFO level logging, all ERROR and WARN level logging. It doesn't log DEBUG level logging. By default, the Connect_<*server_name*>_<*date_time_stamp*>.*log* log file logs additional INFO logging and DEBUG log lines.<br>• The log file is reset when it reaches a maximum of size 20 MB and a new log file is started. The log files are automatically deleted after 20 days. |
| Connect_MSMData_<*date_stamp*>.log | C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect\Logs | • This log file logs BEMS-Connect app MSM-specific data that is used by the Good Mobile Service Manager.<br>• This log file isn't reset after a maximum size or deleted after a specified number of days.<br>• This log file is not required for troubleshooting BEMS-Connect issues. |
| gems_<*server_name*>_<*date_time_stamp*>.log | C:\BlackBerry\bemslogs | • This log file logs BEMS-Connect interaction information with Skype for Business on-premises using non-trusted application mode or Cisco Unified Communications Manager that is configured in your environment.<br>• This log file is reset when it reaches a maximum size of 100 MB.<br>• The log file is automatically purged after 10 days. |

## Troubleshooting: Connect log files

**Error message: The process was terminated due to an unhandled exception. Microsoft.Rtc.Internal.Sip.TLSException**

**Possible cause**

The SSL certificate was not created with the correct cryptographic service provider and key spec. The KeySpec property sets or retrieves the type of key generated. Valid values are determined by the cryptographic service provider in use, typically Microsoft RSA.

**Possible solution**

Verify that the Provider, ProviderType, and KeySpec values are the same as the examples below or the CA must reissue a new SSL and appropriate provider and key spec values.

1. On the computer that hostsBEMS, open the Windows PowerShell and type the following command: `certutil.exe –v –store "my" <name of ssl cert>" > c:\temp\ssl.txt`
2. In a text editor, open the **ssl.txt** file. By default, the ssl.txt file is located in <*drive*>:\temp.
3. Search for **CERT_KEY_PROV_INFO_PROP_ID**.
4. The SSL certificate information should return the following information:

```
CERT_KEY_PROV_INFO_PROP_ID(2):
Key Container = 9ad85141c0b791ad17f0687d00358b70_dd7675d5-867d-479c-90b0-
cd24435fe903
Provider = Microsoft RSA SChannel Cryptographic Provider
ProviderType = c
Flags = 20
KeySpec = 1 -- AT_KEYEXCHANGE
```

# BlackBerry Presence log files

The BlackBerry Presence service logs presence information in the Core log files and saves them to the bemslogs folder stored daily in `C:\BlackBerry\bemslogs`. These log files are required when troubleshooting Presence issues. If your environment is configured for Microsoft Lync Server or Skype for Business on-premises using trusted application mode, additional log text files, LPP-log.txt, are created.

## Finding log files for the Presence service

By default, a server log file is created for each BEMS server and is stored daily on the computer that hosts BEMS.

BEMS-Core names the log files gems_<*server_name_time stamp*>.log.

By default, the BEMS log files are stored daily in `C:\BlackBerry\bemslogs`.

**Note:** The timestamp is reset daily at 0:00. It is also reset each time that the Good Technology Common Services service is restarted and when the file size is a maximum of 100 MB.

When the Presence service is restarted, a new log file (LPP-log.txt) is not generated. When the log file reaches 10 MB, a new log is created. When 20 log files are created, the older log files are automatically deleted.

When using BEMS-Presence for Microsoft Lync Server or Skype for Business on-premises using trusted application mode, the Presence service also writes Lync Presence Provider log files and names files LPP-log.txt. By default, the BEMS Presence log files are stored in `C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Presence\Logs\`

# BlackBerry Docs log files

The BlackBerry Docs service logs the necessary Docs information in the Core log files and saves them to the bemslogs folder stored daily in `C:\BlackBerry\bemslogs`. These log files are required when troubleshooting Docs issues.

## Auditing user actions in the Docs service

If you have the Docs service installed in your environment, you can audit user actions in BEMS to identify and troubleshoot issues between users and the Docs service. When enabled, user actions (for example, user downloads, deletions, browsing history, and files created) are logged to the BEMS database. To view the audit reports, you require access to the Microsoft SQL Server where the BEMS-Docs database is located, and that the Microsoft SQL Server Reporting Services are available.

## Configure audit properties

Your audit settings enable or disable the Docs service audit logs. When you enable audit logs, you can choose how long you want to keep the audit logs, the audit properties to include, and when to delete old actions. If you disable the audit settings, the audit records already logged are not deleted and remain in the database. Perform an audit purge to clear the audit logs from the database.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Audit**.
3. On the **Audit Settings** tab, select the **Enable Audit Logs** checkbox.
4. In the **Audit Operations** section, select the audit operations you want the log files to include logging for.
   - Browse: Logs user's browsing history of the repository (for example, subfolders and files) in a displayed list
   - File Download: Logs download of files to the user's device to read them
   - File Upload: Logs upload of files from the user's device to the repository for storage
   - Folder Creations: Logs folder creation to the repository
   - Folder Delete: Logs folder deletion from the repository
   - Check out: Logs when users lock a file for editing
   - Check In: Logs when users release a file from editing
   - Purge: Logs when administrators remove the audit logs from the database
5. Click **Save**. It can take up to two minutes for the changes to take effect.

**After you finish:**

- Entitle your users to use the Docs service and then, set up your file shares, SharePoint sites, and Box storage. For more information on managing repositories, see "Managing Repositories" in the Docs configuration content.
- View the Docs service audit report
- Optional, view the number of records that are logged and purge the audit logs. For instructions, see Purge audit logs from the database.

## Purge audit logs from the database

You can remove audit records logged to the database earlier than the purge date selected. Configuring this option allows you to see the total number of records that have been logged and delete them from the database if necessary.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Audit**.
3. On the **Audit Purge** tab, in the **Purge audit logs from the database before** field, select a purge-before date.
4. Click **Purge**.

## View the Docs service audit report

These steps require that you have Microsoft SQL Server and permissions to access it, and the Microsoft SQL Server Reporting Services are available. For more information, see your SQL Server documentation or contact your SQL Server administrator.

**Before you begin:**

- Make sure that the audit properties are enabled. For instructions, see Configure audit properties.
- Your environment has a Microsoft SQL Server and you have permissions to access it.
- The Microsoft SQL Server has the Microsoft SQL Server Reporting Services available.

1. With SQL Server administrator permissions, in a browser, open Microsoft SQL Server Reporting Services. By default, the web address is `http://<SQL Server hostname>/reports`
2. Start the **Report Builder**.
3. Create a new report.
4. Create a data source connection. Specify the following fields:
   - **Name** field: Enter a descriptive name for the report (for example, docs_audit_report_*date*)
   - **Select Connection type** drop-down: Select **Microsoft SQL Server**.
   - **Connection string** field: If required, enter a string that points to the Docs DB FSBAudit table.
5. Design the query. Specify the following settings:
   - **Database view** column: under Tables, select FSBAudit and AuditActionType.
   - **Select fields** section: make a relationship between the two tables. Click ActionName > AutoDetect.
   - **Arrange fields** screen: arrange the fields to group the data and values to how you want them to display. For example, if you create a report that is based on the username, you would specify the following:
     - **Available fields** column: select **ActionPath**.
     - **Row groups** column: select **Username** to display the username that completes the action in the report.
     - **Values** column: specify the values to display in the table (for example, action time, action type, and action path).
       - **ActionTime** provides information for when the action occurred.
       - **ActionType** details the action (for example, accessing or downloading a file).
       - **ActionPath** provides the path to the file for which the action was completed.
6. Save the settings and run the report. The report is saved to the Microsoft SQL Server Reporting Services.
7. Double-click the report that you want to view.

## Troubleshooting the BlackBerry Docs service

#### BlackBerry Work Docs fails to find a Microsoft SharePoint view by name

#### Possible cause

Maximum HTTP URL length is set to short.

#### Possible solution

Increase the maxUrlLength setting.

1. In Microsoft IIS, under site or server, open **Configuration Editor**.
2. In the drop-down at the top, expand **system.web** and select **httpRuntime**.
3. Change the **maxUrlLength** property to 2048. By default, the maxUrlLength is 260 characters.

# Appendix: BEMS Windows Event Log Messages

To view the BEMS Windows Event Log messages, open the Windows Event Viewer on the computer that hosts the BEMS instance. Expand the Windows Logs and click Application. Search for Event ID 4096.

| Message | Component | Level | Context |
|---|---|---|---|
| Error Node exceeded capacity (100%). <*number of users including users over exceeded capacity*>/<*number of users for maximum capacity*> | autodiscover/ ewslistener | Error | This error occurs when the BEMS instance reaches maximum user capacity. BEMS features might not work as expected for any new users added to the BEMS instance. For example, notifications. |
| Warn Node close to exceed capacity (80%). <*number of users*>/<*number of users for maximum capacity*> | autodiscover/ ewslistener | Warn | This warning occurs when the BEMS instance reaches 80% of user capacity or if one BEMS instance is working at overcapacity and one BEMS instance is working under capacity. BEMS automatically reassigns users between the two BEMS instances. |
| Error communicating with BlackBerry Proxy or Good Proxy Server - HTTP code {}, Message {} | server-core/gd-core | Error | Could not connect to the BlackBerry Proxy or Good Proxy server while verifying authorization token (during Push Registration from G3 Mail context) |
| Failed to retrieve the list of BlackBerry Proxy or Good Proxy servers - code {} - Reason {} | server-core/gd-core | Error | Used for high availability and load balancing of requests to the BlackBerry Proxy or Good Proxy server. The list of known BlackBerry Proxy or Good Proxy servers are maintained in memory and requests are load-balanced through this list. |
| Failed to retrieve the list of BlackBerry Proxy or Good Proxy servers | server-core/gd-core | Error | Used for high availability and load balancing of requests to the BlackBerry Proxy or Good Proxy server. The list of known BlackBerry Proxy or Good Proxy servers are maintained in memory and requests are load-balanced through this list. |
| Incorrect BlackBerry Proxy or Good Proxy Server configuration | server-core/gd-spring | Error | Communicate with the BlackBerry Proxy or Good Proxy server to verify Authorization token using HTTP(s) protocol. If URL is syntactically wrong or configuration error then error is logged in event log. |

| Message | Component | Level | Context |
|---|---|---|---|
| Autodiscover failed for {} users with exception {} | server-notifications/ autodiscover | Warn | Failed to retrieve user's settings through autodiscover. Needs administrator attention to fix the issue. The user will not receive notifications until issue is resolved. This is a batch request and the log only prints the number of users that failed auto discover. |
| Invalid syntax for property {}, must be a valid URL | server-notifications/ autodiscover | Error | Server is configured with an invalid URL used for bypassing the steps to find the autodiscover end point. BEMS ignores this URL and follows the regular steps to perform autodiscover. |
| User {} being quarantined after {} attempts to perform autodiscover | server-notifications/ autodiscover | Warn | BEMS can not autodiscover the user's settings for configured number of attempts. The user mentioned is marked as 'QUARANTINED' and does not receive notifications. The status can be reset through karaf command (user:reset). |
| No response from server while performing autodiscover for user {} | server-notifications/ autodiscover | Warn | Autodiscover failed for the user mentioned. |
| Autodiscover failed for user {}, error code: {}, Detail: {} | server-notifications/ autodiscover | Warn | Autodiscover failed for the user mentioned. |
| Failed to retrieve user settings while performing autodiscover for user {} | server-notifications/ autodiscover | Warn | Autodiscover failed for the user mentioned. |
| No valid EWS URL setting configured for the user {} | server-notifications/ autodiscover | Warn | Autodiscover failed for the user mentioned. |
| Error communicating with Database server - {error msg} | server-notifications/ autodiscover | Error | BEMS failed to connect to SQL database. Needs immediate attention. |
| Database Error - {error msg} | server-notifications/ autodiscover | Error | BEMS failed to connect to SQL database. Needs immediate attention. |
| Lost connection with exchange server. Last known error {} | server-notifications/ ewslistener | Error | EWSListener: Lost connection with exchange server. This might be due to Exchange server\Autodiscover service down. |

| Message | Component | Level | Context |
|---|---|---|---|
| Error subscribing user {} with exchange server {} | server-notifications/ ewslistener | Error | Subscribe to the user email address with exchange server to track modifications of user mailbox. |
| User {} marked for reautodiscover | server-notifications/ ewslistener | Info | Does a database call to mark the user for reautodiscovery. This task is done every $n$ interval of time. |
| Error communicating with Database server - {error details} | server-notifications/ pushnotifydbmanager | Error | Bootstrap database connection. |
| {} is no longer the master (producer) since database server time {} | servernotifications/ pushnotifyha-dbwatcher | Error | High availability System: Check whether the node itself is Producer or not. Prints the error in event log when the server has lost ownership of the high availability system (not master any more). |
| {} is the master (producer) since database server time {} | servernotifications/ pushnotifyha-dbwatcher | Info | High availability System: Check whether the node itself is Producer or not. If it was not master before; the fail-over is happening. |
| Detected Server {} is inactive. Users will be load balanced to other active servers | servernotifications/ pushnotifyha-dbwatcher | Error | High availability System: If server is detected as inactive\heartbeat fails, the users of the bad server are reassigned to other active server. |
| Error communicating with Database server - {error details} | servernotifications/ pushnotifyprefs | Error | Database error due to server down \login error, etc. |
| { Good Dynamic Proxy Server connection error details } | server-console/config | Error | Connect BlackBerry Dynamics Module – Test from dashboard with GP down, connection failure error. |
| Connection to Good Dynamic Proxy Server is successful | server-console/config | Info | Connect BlackBerry Dynamics – Test from dashboard when GP is up and running, successful test. |
| Connection Successful, Server: -{}: Database : {} | server-console/config | Info | Mail – DB – Test database configurations from dashboard. Connection successful. |
| Exception during connection test - {} | server-console/config | Error | Mail – DB – Test database configurations from dashboard. Connection issues due to bad password or user or host info. |

| Message | Component | Level | Context |
|---|---|---|---|
| Invalid configuration properties- {} | server-console/config | Error | Mail – DB – Test database configurations from dashboard. Validation of database configuration values. |
| { Good Dynamic Proxy Server connection error details } | server-console/config | Error | Presence BlackBerry Dynamics – Test from dashboard with the BlackBerry Proxy or Good Proxy down, connection failure error. |
| Connection to Good Dynamic Proxy Server is successful | server-console/config | Info | Presence BlackBerry Dynamics – Test from dashboard when the BlackBerry Proxy or Good Proxy is up and running, successful test. |
| Lync Presence Provider Ping failed with error status {} and reason - {} | server-presence/ presencebundle | Error | Connection to Presence server. If response received, log the reason for failure. |
| Lync Presence Provider Ping failed with exception {}: {} - set status {} | server-presence/ presencebundle | Error | Connection to Presence server. Most likely connection refused because down |
| Lync Presence Provider Ping failed, cause unknown | server-presence/ presencebundle | Error | Connection to Presence server. |
| Presence Service failed to reset LPP, interrupted with error: {} | server-presence/ presencebundle | Error | Reset all contacts presence status. |
| Presence Service failed to reset LPP, timed out with error: {} | server-presence/ presencebundle | Error | Reset all contacts presence status. Timeout error. |
| Failed to reset LPP, {} with error: {} | server-presence/ presencebundle | Error | Reset all contacts presence status. |
| Presence Service started | server-presence/ presencebundle | Info | Presence service started. |
| Presence Service stopped | server-presence/ presencebundle | Info | Presence service stopped. |
| Bad Lync Presence Provider Subscription URI: {} | server-presence/ presencebundle | Error | Presence service provider subscription URI. |
| Bad Lync Presence Provider Ping URI: {} Ping | server-presence/ presencebundle | Error | Presence service provider subscription URI. |

| Message | Component | Level | Context |
|---|---|---|---|
| Redis Cache & Queue services are not available at the moment. | server-presence/ presencebundle | Error | When cache provider is set to Redis and Redis service is unavilable. |
| GNP Relay Service not available | server-presence/ presencebundle | Warn | GNP service which sends GNP notification is not available or down. |

# Legal notice

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada