BlackBerry UEM

Monitoring and reporting

Administration

12.17

Contents

Monitoring and reporting

You can create event notifications, generate reports from the dashboard and the user list, manage licenses for devices, and monitor BlackBerry Dynamics app performance in BlackBerry UEM

You can also monitor the status of BlackBerry UEM using log files, audit log files, and SNMP tools.

Using dashboard reports

The dashboard uses graphs to present information from the BlackBerry UEM services about users and devices on your system. You can use the cursor to hover over a data point (for example, a slice in a pie chart) to see information about the users or devices.

If you need more information, you can display a report from the graph to see detailed information about users or devices. The maximum number of records in a report is 2000. You can generate a .csv file from a report and export the file for further analysis or reporting purposes.

To see a demonstration of how use the dashboard, visit our YouTube channel.

To open and manage a user account, you can click the user or device in a report. When you are finished with an account, you can click Back on the page (not the browser) to return to the report.

The following table describes the information each dashboard report displays.

Dashboard report	Description
Devices roaming and not roaming	A list of users with devices that are currently in a roaming state
Device activations	A dynamic representation of the devices activated each month in your organization over a 12-month period, based on when the devices were initially activated. The numbers change to reflect currently activated devices. For example, if a device that you activated in August is deactivated, the number of devices shown in August is reduced by one.
Top 5 assigned apps installed	The five most common apps assigned by your organization and installed on devices
Devices by platform	A list of the devices in your organization, by platform
Device compliance	A list of issues detected on iOS, or Android devices in your organization
Devices by last contact time	The number of days that have passed since devices last contacted the server
Devices by carriers	A list of the devices in your organization, by service provider
Top 5 device models	The five most common mobile device models in your organization

Change the type of graph

You can change the type of graph used to graph information.

Click ⚙ beside a graph and select a type of graph from the drop-down list.

Export a dashboard report to a .csv file

1. To open a report, click a graph.
2. To sort the records based on the column selected, click a column header.

3. Click **Export** and save the file.

Creating event notifications

You can set up event notifications to alert administrators by email about certain BlackBerry UEM events. Some examples of events include:

- A user account is added
- A device becomes non-compliant
- A device is deactivated
- An IT policy is assigned to a group
- The APNs certificate is 30 days from expiry (on-premises only)

For a complete list of events, see Event types.

Each event notification is associated with an email distribution list, a schedule, and an email template. You can create distribution lists that include individual email addresses, recipients with certain administrator roles, or recipients that belong to certain groups. Schedules define the days of the week and times of day that notifications are sent. Email templates define the content of email notifications.

Create a schedule for event notifications

You can configure schedule components to associate with event notifications. Event notifications are sent only for events that occur during the days and hours defined in the schedule.

1. On the menu bar, click **Settings > General settings**.
2. Click **Event notifications**.
3. On the **Schedule components** tab, click +.
4. Type a name for the schedule.
5. Select the days of the week to send notifications. Notifications are sent only for events that occur on the selected days.
6. Select one of the following options:
   - Select the **All day event** check box: Notifications are sent anytime.
   - Deselect the **All day event** check box: Select the hours each day that notifications are sent. Notifications are sent only for events that occur within these hours.
7. Click **Save**.

Create a distribution list for event notifications

You can create distribution lists to associate with event notifications. Distribution lists can include user groups, administrator roles, and individual email addresses.

1. On the menu bar, click **Settings > General settings**.
2. Click **Event notifications**.
3. On the **Distribution list** tab, click +.
4. Type a name for the distribution list.
5. If you want to include individual email addresses, click + in the **Email recipients** section, type an email address and click **Save**.

6. If you want to include administrators that belong to a group, select one or more groups in the **Available user groups** list and click ➔.
7. If you want to include administrators that have a particular role, select one or more roles from the **Available user roles** list and click ➔.
8. Click **Add**.

Create an event notification

Create an event notification to alert administrators about events in BlackBerry UEM.

Before you begin:

- If you don't want to use the default event notification email, create an event notification email template.
- Create a schedule for event notifications.
- Create a distribution list for event notifications.

1. On the menu bar, click **Settings > General settings**.
2. Click **Event notifications**.
3. On the **Event notifications** tab, click +.
4. Select one event type.
5. Click **Next**.
6. In the **Date/time to send email notification** drop-down list, select one of the following options:
   - **Always after an event**: Email notifications are sent whenever the event occurs.
   - Any preconfigured schedule in the list.
   - **Add new scheduler**: Create a schedule and click **Save**.
7. In the **Recipients** field, select one of the following options:.
   - **Add new distribution list**: Create a distribution list and click **Save**.
   - Any preconfigured distribution list.
8. In the **Email template** drop-down list, select the email template that you want to use for the event notification.
9. In the **Status** drop-down list, select **On** to enable the event notification or **Off** to disable the event notification.
10. Click **Preview email** to see the event notification email and the list of email addresses for the recipients.
11. Click **Save**.

Disable an event notification

You can disable an event notification without deleting the event notification.

1. On the menu bar, click **Settings > General settings**.
2. Click **Event notifications**.
3. In the **Notification type** column, click on an event notification.
4. In the **Status** drop-down list, click **Off**.
5. Click **Save**.

Event types

You can create event notifications for the following event types:

Administrator

- Administrator account locked

App management

- App added to user group
- App assigned to user
- App removed from user group
- App removed from user
- App definition created
- App definition deleted
- App definition updated
- App group disposition updated
- App user disposition updated
- Android Enterprise app configuration updated
- Android Enterprise app approved
- Android Enterprise new app permissions
- Android Enterprise app updated
- Android Enterprise app availability changed
- Android Enterprise app installation failed
- iOS VPP account expiry
- Android Enterprise app feedback
- Android Enterprise app error feedback

BDMI signing

- BDMI signing failed (on-premises only)

Compliance

- Compliance breached
- Compliance restored

BlackBerry Protect

- Safe browsing
- Safe messaging
- Malicious app removed from UEM
- Malicious app detected on device
- Sideloaded app detected on device

Connectivity

- Failed sending administrator email
- BlackBerry Infrastructure connection (with BlackBerry UEM Core) established (on-premises only)
- BlackBerry Infrastructure connection (with BlackBerry UEM Core) failed (on-premises only)
- BlackBerry Gatekeeping Service access failed
- DEP connection established
- DEP connection failed
- Directory connection synchronization failed
- Service connections for UEM instance changed

Enrollment

- DEP token expiry (30 days before expiry)
- Activation completed
- Activation failed
- Deactivated

Device

- Device deleted
- Device model added
- Device model updated
- Device OS added
- Device ownership change
- Command sent
- Command delivered
- Allow BlackBerry Gatekeeping Service
- SIM swap
- Android 10 device activated with MDM Controls
- User device state changed

Group

- Group created
- Group deleted
- Group added to user group
- Group added to user
- Group removed from user group
- User removed from group

Policies and profiles

- Policy or profile created
- Policy or profile deleted
- Policy or profile sent
- Policy or profile delivered
- Policy or profile delivery failed

- Policy or profile assigned to group
- Policy or profile assigned to user
- Policy or profile unassigned from group
- Policy or profile unassigned from user
- Policy or profile signature storing
- Policy or profile signature validation
- IT policy pack updated
- Metadata updated

Performance

- Device performance alert

User

- User created
- User deleted

Apple Push Notification

- APNs certificate expiry (30 days before expiry)

Licensing

- License expiration warning

Server certificates

- Certificate expiry

Managing licenses for devices

Licenses control the number of devices that your organization can activate with BlackBerry UEM and BlackBerry UEM Cloud. Some licenses also give your users access to other BlackBerry software such as BlackBerry Enterprise Identity and BlackBerry 2FA and BlackBerry Dynamics apps. You can use the Licensing summary page in the BlackBerry UEM management console to:

- View license information for each license type
- Monitor licensing status and review warnings or errors
- Identify and correct license compliance issues

For more information on available licenses, see the Licensing content.

Permissions to manage licenses

To manage licenses in BlackBerry UEM, the administrator account that you use must be assigned a role with the appropriate permissions. BlackBerry UEM administrators require the following permissions:

- View licensing summary
- Edit licensing settings

BlackBerry UEM Cloud administrators require only the View licensing summary permission.

The preconfigured roles in BlackBerry UEM have different permissions turned on by default. The Security Administrator role and the Enterprise Administrator role have licensing permissions.

View license information

You can view license information for your organization on the Licensing summary page and license information for a device in the user's device details. The management console displays license information based on the last snapshot of the license pool in the licensing infrastructure.

If you remove features from users or devices or deactivate devices, the changes will appear immediately on the user's Device tab, but they will not appear on the Licensing summary page until BlackBerry UEM takes a new snapshot of the license pool in the licensing infrastructure.

The Licensing summary displays the licenses in use across all on-premises and cloud instances in your organization. Each license type displays a warning if it will expire soon. By default, the warning appears 28 days before licenses expire. If you renew licenses, the new expiration date will appear in the Licensing summary after the existing licenses expire.

Note: If the Licensing summary page does not display any license information, the connection to the licensing infrastructure is not available.

1. On the menu bar, click **Settings > Licensing**.
2. View the following license information for each license type:
   - Total in use: The number of identity-based and server licenses in use.
   - SIM license: The number of identity-based licenses in use.
   - Server license: The total number of server licenses, the number of available licenses, the number of licenses in use, and the license expiration dates.

After you finish: To view license information for a device, go to the appropriate device tab for a user account.

Communicating with the licensing infrastructure

When you view the Licensing summary page in the management console, the license information is based on the last snapshot of your organization's license pool in the licensing infrastructure. BlackBerry UEM contacts the licensing infrastructure for the following events:

Level	Event	Activity
User	• Activate or deactivate a device • Add or remove a feature	License information is updated only for the user. The changes will not appear on the License summary page until BlackBerry UEM takes a new snapshot of the license pool in the licensing infrastructure.
Organization	• Obtain more licenses • Service is out of compliance • Scheduled contact (once a day)	The license pool is adjusted to optimize license usage and license information is updated for the organization. As a result, license usage may change for multiple users and license types. BlackBerry UEM takes a new snapshot of the license pool in the licensing infrastructure.

On the Licensing settings page, you can view the last contact time with the licensing infrastructure.

Licensing status

If a licensing issue requires your attention, a warning or error icon appears on the menu bar in the management console. If more than one issue exists, the icon for the most serious issue appears. You can monitor licensing status and review warnings or errors on the Licensing summary page.

Message	Icon	Description
Licensing infrastructure	OK	BlackBerry UEM successfully contacted the licensing infrastructure the last time that it tried to connect. You can view the last contact time on the Licensing settings page. This message is not displayed in BlackBerry UEM Cloud.
Licensing infrastructure - Unable to connect	Error	BlackBerry UEM could not contact the licensing infrastructure. Verify that your organization's firewall allows outbound connections over port 3101 (TCP). This message is not displayed in BlackBerry UEM Cloud.
Overall compliance status	OK	There are no licensing issues that require your attention.
In grace period, *x* days remaining	Warning	When usage is exceeded for one or more device types, features, or services, BlackBerry UEM starts a grace period for the applicable service to give you time to correct the license compliance issues. The message indicates the number of days that remain until the grace period ends.

Message	Icon	Description
Out of compliance	Error	When the grace period ends and one or more license compliance issues still exist, the organization is out of compliance for the applicable service.
Licenses will expire soon	Warning	Trial, subscription, or term licenses will expire soon. You can view the expiration dates for each license type.
Trial expires in *x* days	Warning	When the organization has trial licenses for a single trial period, BlackBerry UEM indicates the number of days that remain until the trial period ends. BlackBerry UEM displays this message if the organization has only trial licenses.
Next trial expires in *x* days	Warning	When the organization has trial licenses for multiple trial periods, BlackBerry UEM indicates the number of days that remain until the first trial period ends. BlackBerry UEM displays this message if the organization has only trial licenses.

View unlicensed features

Unlicensed features are tracked at the organization level, so you can view the list of unlicensed features when you log in to any BlackBerry UEM domain or BlackBerry UEM Cloud tenant. When the UEM service is in grace period or out of compliance, you can use the list of unlicensed features to help you identify license compliance issues.

1. On the menu bar, click **Settings > Licensing**.
2. Click **View list of unlicensed features** to view the following information:
   - Activation type or licensed feature: Each row displays a unique feature set which can include activation type, licensed feature, or both.
   - Number of violations: The number of users without a valid license that are associated with a feature set.

Change the expiration warning period

You can change the expiration warning period to customize when the BlackBerry UEM management console displays a warning that licenses will expire soon.

1. On the menu bar, click **Settings > Licensing > Licensing settings**.
2. In the **License expiration warning** drop-down list, click the appropriate warning period.
3. Click **Save**.

View and save a device report

You can generate a device report to view detailed information about each device that is associated with BlackBerry UEM.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Select the device tab.
5. Click **View device report**.
6. Click **Export** to save the device report to a file on the computer, if necessary.

Exporting app deployment reports

You can export app deployment reports for apps, including BlackBerry Dynamics apps, to an .html file from the Apps screen in the management console. The report includes information about apps deployed by BlackBerry UEM and the users that currently have the apps installed on their devices. For example, you can find device information about all users that have a specific app, including the device ID, model, OS version, and installation status.

You can choose the apps that you want to include in a report. Each app that you choose to include in the report is given a separate section listing its app version information and the device information for each user that has the app installed.

Note: For iOS devices with the User privacy activation type, the report lists all devices that the app has been assigned to. BlackBerry UEM can't confirm if the app is still installed on the device when the report is generated.

You can also open the .html file using Microsoft Excel for further analysis.

Export an app deployment report to an .html file

1. On the menu bar, click **Apps > Apps**.
2. For each app that you want to include in the report, select the check box beside the app. You can select the checkbox at the top of the apps list to select all apps.
3. Click  and save the file.

Activity and compliance violation reports for BlackBerry Dynamics apps

When BlackBerry UEM and BlackBerry Dynamics are integrated, you can export BlackBerry Dynamics app activity or compliance violation data from the management console. You can use this information to take action on inappropriate or suspicious activity. App activity reports include app activity data for each BlackBerry Dynamics app (for example, app version information, activation date, and the last contact with the server). Compliance violation reports include compliance violation data for each app (for example, the policy rules that were violated and when the violation occurred).

Export BlackBerry Dynamics app reports to a .csv file

If you export a report from BlackBerry UEM Cloud, each report has a limit of 5000 records. In an on-premises environment, the default number of records is 5000. You can change the limit in the BlackBerry Dynamics global properties.

1. On the menu bar, click **Settings > BlackBerry Dynamics > Reporting**.
2. In the **Export data to .csv** section, select the type of report that you want to export:
   - **BlackBerry Dynamics app activity**
   - **BlackBerry Dynamics app compliance violations**
3. Click **Export** and save the file.

Monitoring the performance of BlackBerry Dynamics apps

You can monitor the performance of the BlackBerry Work and BlackBerry Connect apps and choose the issues that you want to be reported.

Enable BlackBerry Work or BlackBerry Connect monitoring

To enable BlackBerry Work or BlackBerry Connect monitoring, you must configure the app configuration that is assigned to it.

1. On the menu bar, click **Apps**.
2. Click the BlackBerry Work or BlackBerry Connect app that you want to monitor.
3. On the BlackBerry Dynamics tab, in the **App configuration** table, click the name of the app configuration that you want to edit.
4. On the **Performance Reporting** tab, configure any of the following:
   - **Enable Performance Reporting**: Specify whether to monitor performance of the app.
   - **HTTP Connection Error**: Specify whether to report HTTP connection errors between the app and the specified application servers.
   - **HTTP Response Time**: Specify whether to report HTTP responses that are taking longer than the specified time. Enter the application server addresses to monitor.
   - **HTTP Status Code**: Specify whether to report a specified HTTP status code. Enter the application server addresses to monitor.
   - **Don't send reports for duration (in seconds)**: Specify the amount of time to wait before sending another report.
5. Click **Save**.

View device performance alert notifications

Before you begin: Enable BlackBerry Work or BlackBerry Connect monitoring

1. On the menu bar, click **Audit and logging** > **Device performance**.
2. Choose a date range and click **View**.
3. Under **Filters**, click a category to expand it.
4. Select the filters that you want to apply and click **Submit**.
5. If necessary, do one of the following:
   - To remove a filter, click ✕ beside the filter that you want to remove.
   - To clear all filters, click **Clear all**.
6. To export the results to a .csv file, click .

View a performance alert for a single device

Instead of viewing a list of performance alerts based on date and alert type, you can also view all of the performance alerts for a single device in the last 24 hours. If there are performance alerts for a device, a caution

icon appears on the device tab and a message is displayed that tells you how many alerts have been detected on the device.

Before you begin: Enable BlackBerry Work or BlackBerry Connect monitoring

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Select the device tab for the device that you want to view alerts for. A device with performance alerts or compliance violations is flagged with a caution icon.
5. If there are performance alerts for the device, click **View all** beside the performance alert message to view the list of performance alerts for that device.

Monitoring the performance of Android Enterprise devices

You can view security logs for Android Enterprise devices that have been activated using an Android Enterprise activation type.

View device performance alert notifications for Android Enterprise devices

Before you begin:

Enable the 'Send security logs to UEM' rule in the IT policy that is assigned to the users.

1. On the menu bar, click **Audit and logging > Android security**.
2. Choose a date range and click **View**.
3. Under **Filters**, click a category to expand it.
4. Select the filters that you want to apply and click **Submit**.
5. If necessary, do one of the following:
   - To remove a filter, click X beside the filter that you want to remove.
   - To clear all filters, click **Clear all**.
6. To search for a particular user, use the **Username** field.

Using log files

You can use log files to identify and troubleshoot issues with the BlackBerry UEM components or devices in your organization's environment. The BlackBerry UEM logging capabilities allow you to:

- Track the activity of the BlackBerry UEM components using the server logs
- Send BlackBerry UEM log file data to a syslog server or to a text file
- Retrieve log files from Android devices
- Audit phone call and SMS activity on Android devices

Managing BlackBerry UEM log files

The size of the log files varies depending on the number of users and devices in your BlackBerry UEM environment and their level of activity. If you have BlackBerry UEM installed in an on-premises environment, it is a best practice to monitor and control the amount of disk space used by the log files. To prevent them from taking up too much disk space, you can specify a maximum file size and debug level for the log files. The features for managing log files are not available in BlackBerry UEM Cloud.

You can configure logging settings at the following levels:

- Global logging settings: These settings apply to all the BlackBerry UEM instances in your organization that share the same database. These settings include the destination of the syslog messages and the maximum size for the log files.
- Per-user logging settings: These settings allow you to enable payload logging for individual user accounts for a specified length of time for troubleshooting purposes.
- Instance logging settings: These settings apply only to the BlackBerry UEM instance you select and override global settings. These settings include enabling the option of a local location for log files and the log file logging level.

Configure global logging settings

These settings are not included in BlackBerry UEM Cloud.

1. On the menu bar, click **Settings** > **Infrastructure** > **Logging**.
2. Configure the following global settings as required for your organization's environment:

Setting	Steps
To route system events to a syslog server	Select the **SysLog** checkbox and specify the host name and port for the syslog server where you want to route the BlackBerry UEM log events.
To be able to specify a location on the server instance where the BlackBerry UEM component log files are stored	Select the **Enable local file destination** checkbox.
To enable advanced logging of server-to-device communications for troubleshooting	Select the **Enable MDM payload logging** checkbox. **Note:** You can choose to enable MDM payload logging only for specific user accounts. For more information, see Configure per-user logging.

Setting	Steps
To enable payload logging for the BlackBerry Dynamics infrastructure.	Select the **Enable CAP payload logging** checkbox.
To enable the ability to audit only UEM/SQL communication without enabling debug logging	Select the **Enable SQL logging** checkbox.
To enable logging of REST calls outbound from BlackBerry UEM Core	Select the **Enable HTTP payload logging** checkbox.
To set a maximum size limit for the BlackBerry UEM component log files	In the **Maximum log file size** field, specify the maximum size, in MB, that each log file can reach. When a log file reaches the maximum size, BlackBerry UEM starts a new instance of the log file.
To set the maximum server log file age for the BlackBerry UEM component log files	In the **Maximum server log file age** field, specify the maximum number of days to keep the server log files before they are deleted. If you do not specify a value, the log files are not deleted.
To specify a network destination path for Android device log files	In the **Device log network location** field, specify the UNC path where you want to store activity log files that you retrieve from devices using the management console.
Maximum device app audit log file size	In the **Maximum device app audit log file size** field, specify maximum size, in MB, that the device app audit log file can reach.
Maximum device app audit log file age	In the **Maximum device app audit log file age** field, specify the maximum number of days to keep the device app audit log files before they are deleted. If you do not specify a value, the log files are not deleted.

3. Click **Save**.

Set a log level for individual BlackBerry UEM components

To help aid in troubleshooting and to prevent performance impact due to excess log file generation, you can enable individual BlackBerry UEM components to write to log files at different information levels. For example, you can configure the BlackBerry UEM Core to generate log files at the Debug level, and leave the rest of the components to generate log files at the Info level.

1. On the menu bar, click **Settings > Infrastructure > Logging**.
2. Expand **Global logging settings**.
3. In the **Service logging override** section, click +.
4. Select a UEM component.
5. In the **Logging level** drop-down lost, select a logging level.
6. Click **Save**.

After you finish: If necessary, you can override these settings. For more information, see Change the default settings for BlackBerry Connectivity Node instances, and Create a server group.

Configure per-user logging

To help aid in troubleshooting and to prevent performance impact due to excess log file generation, you can enable MDM payload logging for specific user accounts.

Note: For information about enabling MDM payload logging for all users, see Configure global logging settings.

1. On the menu bar, click **Settings** > **Infrastructure** > **Logging**.
2. Expand **Per-user logging**.
3. In the **Add a user** search field, search for the user account that you want to enable logging for.
   You can add up to 16 users
4. In the **Expiration** drop-down list, select the length of time to enable logging for that user.
5. Click **Save**.

Configure instance logging settings

1. On the menu bar, click **Settings** > **Infrastructure** > **Logging**.
2. Expand the server instance that you want to configure.
3. Configure the following settings as required for your organization's environment:

Setting	Steps
To specify the location where the BlackBerry UEM component log files are stored	In the **Server log path** field, type the path where you want to store the server log files. By default, log files are stored in `C:\Program Files\BlackBerry\UEM\Logs\`*`yyyymmdd`*. **Note:** You must select the **Enable local file destination** checkbox in the global logging settings before you can change this setting.
To set the level of detail included in the log files	In the **Log debug levels** drop-down list, select one of the following: • **Info**: Write daily activities, warning, and error messages to the log file. • **Warn**: Write warning and error messages to the log file. Warning messages are unexpected events that may require you to take action. • **Error**: Write all error messages to the log file. When an error condition appears, typically you must take action. • **Debug**: Write information required only to debug a problem. By default the debug level is set to **Info**.
To specify the folder for the Android device app audit log files	In the **Device app audit log path** field, type the path where you want to store device app audit log files.
To set a maximum size limit for the device app audit log file	In the **Maximum app audit log size** field, specify the maximum size, in MB, that the device app audit log files can reach. When a log file reaches the maximum size, BlackBerry UEM starts a new instance of the log file.

4. Click **Save**.

Change the maximum age for a log file

1. On the menu bar, click **Settings** > **Infrastructure** > **Logging**.
2. Expand **Global logging settings**.
3. Configure the maximum server log file age in days.
4. Click **Save**.

Finding log files in an on-premises environment

By default, a server log file is created for each on-premises BlackBerry UEM component and is stored daily on the computer where the component is installed. If you install multiple BlackBerry UEM instances, each computer creates its own log files. BlackBerry UEM names the log files *<server_name>_<component_identifier>_<yyyymmdd>_<log_number>.<file extension>* (for example, BBServer01_MDAT_20140730_0001.txt).

The following log files are available in an on-premises BlackBerry UEM solution:

- Log files for components used to manage iOS, Android, and Windows devices.

  Log files are:

  - ACCS - Tomcat access log files for BlackBerry UEM Core
  - BGS - BlackBerry Gatekeeping Service log files
  - BP - BlackBerry Proxy service log files
  - BSG - BlackBerry Secure Gateway log files
  - CORE - BlackBerry UEM Core log files
  - EVNT - BlackBerry UEM Core event log files
  - TMCT - Tomcat server log files for BlackBerry UEM Core
  - UI - BlackBerry UEM management console log files

  Additional log files are created when you first install BlackBerry UEM.

  By default these log files are stored in `<drive>:\Program Files\BlackBerry\UEM\Logs\<date or folder name>`
- Log files used for BlackBerry Secure Connect Plus are:
  - BSCP - BlackBerry Secure Connect Plus log files which log data for connections with the BlackBerry Secure Connect Plus app
  - BSCP-TS - BlackBerry Secure Connect Plus core log files which log data about the BlackBerry Secure Connect Plus component
- Log files for BBM logs, phone logs, PIN to PIN logs, SMS/MMS logs, and video chat logs are stored in .csv format and are used to audit app activity.

  By default, app audit log files for Android devices are stored in *C:\Program Files\BlackBerry\UEM\Logs*.

Finding log files for a BlackBerry Connectivity Node

By default, several log files are created for each BlackBerry Connectivity Node and stored daily on the computer where the BlackBerry Connectivity Node is installed.

The following log files are available in the BlackBerry Connectivity Node:

- Log files for components used to manage iOS, Android, and Windows devices.

Log files are:

- BCC - BlackBerry Cloud Connector log files
- BCC-ACCS - Tomcat access log files for BlackBerry Connectivity Node
- BCC-TMCT - Tomcat server log files for BlackBerry Connectivity Node
- BGS - BlackBerry Gatekeeping Service log files
- BP - BlackBerry Proxy service log files
- BSG - BlackBerry Secure Gateway log files

By default these log files are stored in `<drive>:\Program Files\BlackBerry Connectivity Node \Logs\<date or folder name>`

- Log files used for BlackBerry Secure Connect Plus are:
  - BSCP - BlackBerry Secure Connect Plus log files which log data for connections with the BlackBerry Secure Connect Plus app
  - BSCP-TS - BlackBerry Secure Connect Plus core log files which log data about the BlackBerry Secure Connect Plus component

Reading log files

BlackBerry UEM log files are saved in two formats, comma-separated value and text files.

BlackBerry Messenger contact and message, phone call, PIN , SMS, and video chat logs are stored in CSV format.

All other log files are stored in TXT format.

Reading .csv log files

Comma-separated log files contain different information depending what component, what device, or what device app, they log information for. An example of log files in .csv format is the device app audit files, such as the BBM or Phone call log.

You can identify information contained in .csv log files because each log line presents information in a simple and consistent manner, for example, each line in the SMS log file will present information in the following format:

```
Name.ID,"Email Address","Type of Message","To","From","Callback Phone
 Number","Body","Send/Received Date","Server Log Date","Overall Message
 Status","Command","UID"
```

Each line in a Phone log file, would present in the following format:

```
Name.ID,"Type of Call","Name","Phone Number","Start Date","Server Log
 Date","Elapsed Time","Memo","Command","UID","Phone Line"
```

Reading .txt log files

Log files stored as .txt files have two basic formats:

- The first format is the most common and usually starts with the date and time, providing information in the following manner:

  ```
  DateTime Appname ProcessID LoggingFeature LoggingComponent StructuredData
   LogLevel Message
  ```

For example:

```
2019-04-23T13:16:56.883+0100 - CORE {wff-thread-37} none|none [{{Correlation-
Id,b417051d-13c3-4a29-95f2-512c48b2b018}{Method,POST}{Uri,/tomcat/startup}
{host,computer.example.com}}] - INFO Discrete snapin load finished
```

- The second format, starting with a numerical level indicator, provides information in the following manner:

```
Level Date Thread CID Message
```

For example:

```
<#03>[30000] (09/10 00:00:00.122):{0x520} [DIAG] EVENT=Thread_report,
 THREADID=0x1390, THREADNAME="SRPReceiverHandler"
```

There may be some variation, based on the component or function that is being logged, but all log files stored as `.txt` files contain the following basic information.

Item	Description
Date or Timestamp	A timestamp in of the form <Date><Time><difference from UTC>. The Date/Time indicates the date and time of a particular event. **Note:** The date and time stamp are in the local server time.
Hostname or component identification	Component identification, or hostname, tells you which component that the log file is for. In some cases, this is clear, such as CORE, in others it is less clear, using a numerical identifier
Appname	The Appname is the same for all log files and is shown as MDM.
ProcessID or Thread	Represents the Java Thread Id of the thread which is currently logging a message. For example: `localhost-startStop-1`
MessageID	The MessageId identifies the type of message being sent to the log file. It is a combination of the feature and component being logged using the format <feature>|<component>. For example: `admin.application.management|appmgmt`
StructuredData	Zero or more name value pairs which represent structured data. For example: `[{{requestId,543ade23} {myContextInfo,runningContext}}]`

Item	Description
Message	The message indicates the activity and describes the nature of the event. A message could include information about the hardware or software running, or the problem that is occurring. For example: `INFO  Total 2 routes, of which 2 is started.`
Level	The event level indicates the type of log entry. Commonly, events will fit into one of the following categories: • ERROR = Error • WARN = Warning • INFO = Informational ENV = Environmental • DEBUG = Debug • Other • DIAG = Diagnostic In some log files, the level is shown with a numerical value, in the following format: • [10000] = Error • [20000] = Warning • [30000] = Informational • [40000] = Debug • [50000] = Other

Log file levels

Level	Description
DEBUG	This level specifies information that is valuable for debugging coding issues. Events can include the following: • States of suspect resources in error conditions • Transitions between internal and external components • REST requests to the BlackBerry UEM Core • Requests to Microsoft Active Directory
ERROR	This level specifies an error condition that requires you or a support specialist to take action. Events can include the following: • Encoding exceptions • Data level exceptions • Recoverable coding exceptions
INFO	This level specifies normal system events that administrators or support specialists might want to see. This level is the default log level for BlackBerry UEM.

Level	Description
WARN	This level can indicate a warning condition, that action might be required, or an unexpected event might have occurred. Events can include the following: • Inconsistent data • Unexpected requests • Authorization failures • Authentication failures

Using log files for troubleshooting

Component identifier	Logging component	Description
ACCS	Apache Tomcat server access log files	The Apache Tomcat ACCS log files record all requests for access to the BlackBerry UEM web services. You can use these log files when you want to check access requests to the BlackBerry UEM web services for success or failure.
BCC	BlackBerry Cloud Connector	Logs data about the BlackBerry Cloud Connector component. You can use these log files to verify that BlackBerry Cloud Connector is connected to the BlackBerry Infrastructure.
BGS	BlackBerry Gatekeeping Service	You can use these log files when troubleshooting issues with: • Devices that cannot activate in an environment where the BlackBerry Gatekeeping Service is in use • Connectivity to your BlackBerry Gatekeeping Service • Connectivity between BlackBerry UEM and the BlackBerry Infrastructure • The sending of policies and profiles • iOS and Android connectivity
BP	BlackBerry Proxy	Logs connection traffic between BlackBerry Dynamics containers and endpoints such as a Microsoft Exchange server.

Component identifier	Logging component	Description
BSCP	BlackBerry Secure Connect Plus	Logs data about the BlackBerry Secure Connect Plus component. You can use these log files to verify that BlackBerry Secure Connect Plus is connected to the BlackBerry Infrastructure. For example: 2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service| logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, /192.0.2.0:28231 => bcp.example.com/192.0.2.124:3101], responding with Pong. 2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service| logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, /192.0.2.0:28232 => bcp.example.com/192.0.2.124:3101]
BSCP-TS	BlackBerry Secure Connect Plus core	Logs data for connections with the BlackBerry Secure Connect Plus client. You can use these log files to verify that BlackBerry Secure Connect Plus is ready to receive calls from the BlackBerry Secure Connect Plus client on devices. For example: 47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation 49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created Use to verify that devices are using the secure tunnel. For example: 74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249
BSG	BlackBerry Secure Gateway	You can use these log files when troubleshooting issues with: • iOS devices that can't send or receive email messages • Connectivity between BlackBerry UEM and the BlackBerry Infrastructure • Connectivity between the BlackBerry Infrastructure and the Microsoft Exchange or Microsoft Office 365 mail server
CORE	BlackBerry UEM Core	You can use these log files when troubleshooting issues with: • Core services or transactions • BlackBerry 2FA transactions • Data migration from BES10
EVNT	BlackBerry UEM Core	You can use these log files to find notifications about specific events in the BlackBerry UEM Core.

Component identifier	Logging component	Description
TMCT	Apache Tomcat server log files	The Apache Tomcat TMCT log files record all activities of the Apache Tomcat web services. You can use these log files when troubleshooting issues with the management console.
UI	Management console	You can use these log files when troubleshooting issues with the management console.

Viewing device actions

Actions that were taken or are in progress on a device as a result of commands that you sent from the BlackBerry UEM management console, such as locking a device, disabling the work space, or deleting device data.

Availability of these commands depends on the device and activation type.

The status of a device command can be:

- Command canceled
- Command completed by device
- Command delivered to device
- Command delivery acknowledged by device
- Command failed
- Command in progress
- Notification acknowledged by device
- Notification sent to device
- Queued

View device actions

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. Click the tab for the device that you want to view the device actions for.
5. Click **View device actions**.

Retrieving device logs

You can retrieve log files from devices, using the following methods:

Method	Description	Supported devices
Get device logs using a BlackBerry UEM command	In an on-premises environment, you can retrieve log files from devices by using the "Get device logs" command. A snapshot of the log files for the device is collected every time you use the device command to retrieve them. Users are notified of your ability to collect system log files during device activation and may be notified again when you send the command to retrieve the log files, depending on the device settings. This command is not available in BlackBerry UEM Cloud. iOS and Android devices must have the BlackBerry UEM Client installed and the log files retrieved are BlackBerry UEM Client logs only.	• iOS • Android
Send log files from the BlackBerry UEM Client	Device users can email log files to their administrator from the Help menu in the BlackBerry UEM Client.	• iOS • Android
Send log files from the BlackBerry UEM App Catalog	Windows 10 device users can email log files to their administrator from the Help menu in the BlackBerry UEM App Catalog.	• Windows 10

Get device logs using a BlackBerry UEM command

In an on-premises environment, you can use a BlackBerry UEM command to get log files from the following device types:

- iOS
- Android

This command is not available in BlackBerry UEM Cloud.

Before you begin:

- iOS and Android devices must have the BlackBerry UEM Client installed.
- By default, the Junior HelpDesk role cannot retrieve log files.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Click the device tab.
5. In the **Manage devices** window, click **Get device logs**.
6. Click **Request**.

After you finish:

Retrieve the device log files. By default, the log files are stored in C:\Program Files\BlackBerry\UEM\Logs\device_logs.

Send log files from the BlackBerry UEM Client

Users can send you log files from the BlackBerry UEM Client for the following devices:

- iOS
- Android

1. On the device, tap the **UEM Client** icon.
2. Tap **Help**.
3. Tap **Send Logs** or **Bug report**.
4. Select the email account on the device to send the log file.
5. Tap **Send**.

   iOS and Android log files will be attached to the email as a .zip file.

Send log files from the BlackBerry UEM App Catalog

For Windows 10 devices, users can send you log files from the BlackBerry UEM App Catalog.

1. On the device, tap the **App Catalog** icon.
2. Tap **Help**.
3. Tap **Bug report**.
4. Select the email account on the device to send the log file.
5. Tap **Send**. The log files are attached to the email as a .zip file.

Logging phone call and SMS/MMS activity for Android Enterprise and Samsung Knox Workspace devices

You can log and review phone call and SMS/MMS activity for Android Enterprise and Samsung Knox Workspace devices. BlackBerry UEM can log this activity for devices that are activated with "Work space only (Premium)", "Work and personal - full control (Premium)" "Work and personal - full control (Samsung Knox)" and "Work space only (Samsung Knox)" activation types.

BlackBerry UEM stores separate .csv log files for both phone calls and SMS/MMS. BlackBerry UEM names the log files *<server_name>_<component_identifier>_<event_definition_version>_<yyyymmdd>_<log_number>.<file extension>* (for example, BBServer01_phone_1.0_20160730_0001.csv).

In a on-premises environment, the default log file location is: `<drive>:\Program Files\BlackBerry\UEM\Logs\device_logs\<date or folder name>`. In BlackBerry UEM Cloud the BlackBerry Connectivity Node stores the log files. The default location is: `<drive>:\Program Files\BlackBerry Connectivity Node\Logs\Device Logs`.

See Using log files for information about finding and reading log files.

Log phone call and SMS/MMS activity in an on-premises environment

In an on-premises environment, you need only to set the appropriate IT policy rules to log SMS/MMS and phone activity.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click +.
4. Click the IT policy that is applied to the device.

5. Click .
6. On the **Android** tab, select the IT policy rules for the activities that you want to log.
   - Send SMS/MMS logs to UEM
   - Send phone logs to UEM
7. Click **Save**.

Log phone call and SMS/MMS activity for BlackBerry UEM Cloud

Before you begin: To log SMS/MMS and phone activity for BlackBerry UEM Cloud, the BlackBerry Connectivity Node must be installed.

1. On the menu bar, click **Settings**.
2. Click **External integration > BlackBerry Connectivity Node setup**.
3. Click .
4. Select **Override logging settings** .
5. Select **Enable device application audit logging**.
6. Specify the **Maximum device application audit log file size**

   When the log file size on the device reaches the specified size, the device sends the log file to the BlackBerry Connectivity Node
7. Specify the **Maximum device application audit log file age**

   When the log file on the device reaches the specified age, the device sends the log file to the BlackBerry Connectivity Node
8. Click **Save**.
9. On the menu bar, click **Policies and Profiles**.
10. Click **Policy > IT policies**.
11. Click .
12. Click the IT policy that is applied to the device.
13. Click .
14. On the **Android** tab, select the IT policy rules for the activities that you want to log.
    - Send SMS/MMS logs to the BlackBerry Connectivity Node
    - Send phone logs to the BlackBerry Connectivity Node
15. Click **Save**.

Troubleshooting: SMS/MMS log files

Log files don't contain outgoing SMS/MMS messages

Cause

In your organization's IT policy for Android devices, the "Allow RCS features" and "Send SMS/MMS logs to UEM" options are selected and your organization's carrier supports Rich Communication Services (RCS).

Solution

Deselect the Allow RCS features option in your organization's IT policy and restart the affected device or stop and start the SMS messages app on the device.

Auditing events in BlackBerry UEM

If you have BlackBerry UEM installed in an on-premises environment, BlackBerry UEM keeps administrator and security audit events in log files that you can use to investigate any administrator actions and interactions between BlackBerry UEM and devices.

BlackBerry UEM records all actions that administrators perform in the management console and displays them in the Audit screen. You can filter the list of actions to display only the actions that are relevant to your investigation. For further analysis or reporting purposes, you can export the filtered list to a .csv file.

You can export security audit events to a .csv file from the Audit configuration screen. Security audit events include server actions such as the delivery of commands or policies, starting or stopping a BlackBerry UEM instance, initiation or termination of trust channels, certificate validation status, and changes to the audit settings. From the Audit configuration screen, you can choose the types of security events that you want to record in the log file. For some events, you can choose to log the event based on whether it completes successfully or doesn't complete.

Viewing and exporting administrator and security audit events is not supported for BlackBerry UEM Cloud.

Configure audit settings

You can enable or disable auditing of administrator or security events in BlackBerry UEM. When auditing is enabled, you can choose how long you want to keep records, the number of results to display, and when to delete old records. When auditing is disabled, all records are deleted.

This feature is not supported for BlackBerry UEM Cloud.

Note: Enabling security event auditing requires significant database resources. Use the UEM performance calculator to estimate the resources required.

1. On the menu bar, click **Settings** > **Infrastructure** > **Audit configuration**.
2. In the right pane, click ✎.
3. In the **Administrator event audit settings** section, do one of the following:

Task	Steps
Enable administrator event auditing	**a.** In the **Administrator event auditing** field, click **Enabled**. **b.** In the **Administrator audit record retention** field, type the maximum number of days to keep a record. **c.** In the **Maximum number of records** field, type the maximum number of records to display in the UI. If the number of records exceeds this value, then the administrator must shorten the date range or select a category to reduce the number of records. **d.** In the **Daily delete time (UTC)** field, choose the time of day to delete records.
Disable administrator event auditing and purge all records	**a.** In the **Administrator event auditing** field, click **Disabled**.

4. In the **Security event audit settings** section, do one of the following:

Task	Steps
Enable security event auditing	**a.** In the **Security event auditing** field, click **Enabled**. **b.** In the **Security audit record retention** field, type the maximum number of days to keep a record. **c.** In the **Daily delete time (UTC)** field, choose the time of day to delete old records. **d.** To stop auditing a security event, click ✕ beside the event type. **e.** To add security events to audit, click +. Select the events and click **Add**. **f.** Optionally, if a drop-down list is available in the **Setting** column beside an event type, choose the condition to log the event.
Disable security event auditing and purge all records	**a.** In the **Security event auditing** field, click **Disabled**.

5. Click **Save**.

After you finish:

- Restart the BlackBerry UEM Core service on every computer that hosts a BlackBerry UEM instance.
- Log in to the management console again.

View and filter the administrator audit events

The following task is for viewing and filtering the administrator event audit log only. To view the security audit event log, see Export security audit events to a .csv file. This feature is not supported for BlackBerry UEM Cloud.

1. On the menu bar, click **Audit and Logging** > **System audit**.
2. Click **Edit**.
3. Choose a category and date range. Click **Submit**.
4. Under **Filters**, click a category to expand it. **Note**: Under the **Roles** category, a role named Work Apps is displayed if a user is accessing work apps from their device. Work Apps is not an existing role; it is assigned dynamically to add the minimum set of permissions to access the user's work apps.
5. Select the filters that you want to apply and click **Submit**.
6. Optionally, in the right pane, click ⋮. Select the columns that you want to view.
7. If necessary, do one of the following:
   - To remove a filter, click ✕ beside the filter that you want to remove.
   - To clear all filters, click **Clear all**.

After you finish: If necessary, Export administrator audit events to a .csv file.

Export administrator audit events to a .csv file

When you export the administrator audit events to a .csv file, the .csv file includes the data that you filter. This feature is not supported for BlackBerry UEM Cloud.

1. On the menu bar, click **Audit and Logging** > **System audit**.
2. If necessary, in the left pane, filter the audit log to view only the data that you want to include in the .csv file.

3. Click and save the file.

Export security audit events to a .csv file

When you export the security audit events to a .csv file, the .csv file includes the all security events that were logged. this feature is not supported for BlackBerry UEM Cloud.

1. On the menu bar, click **Settings** > **Infrastructure** > **Audit configuration**.
2. In the **Security event audit settings** section, click **Export** and save the file.

Delete audit records

You can delete audit records before the next daily delete time. This feature is not supported for BlackBerry UEM Cloud.

1. On the menu bar, click **Settings** > **Infrastructure** > **Audit configuration** .
2. In the **Administrator event audit settings** or **Security event audit settings** section, click **Delete**.
3. Click **Delete**.

Monitoring BlackBerry UEM using SNMP tools

If you have BlackBerry UEM installed in an on-premises environment, you can use third-party SNMP tools to monitor the activity of severalBlackBerry UEM components. SNMP monitoring requires an SNMP service and an SNMP management tool. You run the SNMP service on the computers that host BlackBerry UEM. The SNMP service, located in the Windows Services, includes an SNMP agent that collects data from the BlackBerry UEM components.

You use an SNMP management tool (for example, a MIB browser) to view and analyze the data that is received from the agent. The management tool typically includes an SNMP trap management tool that is used to retrieve and interpret trap messages from the agent. The management tool can be installed on the computer that hosts BlackBerry UEM or on a separate computer.

There are two places where you configure SNMP:

- To monitor the BlackBerry UEM Core, BlackBerry Secure Connect Plus, BlackBerry Secure Gateway, and BlackBerry Cloud Connector you configure SNMP in the management console. See Configure SNMP to monitor components.
- To monitor BlackBerry UEM enterprise connectivity components, you configure the SNMP service.

By default, the management tool displays the OID of a condition, which is a sequence of integers that identify a class value in a class hierarchy. All SNMP OIDs and SNMP traps for BlackBerry UEM begin with a class value of 1.3.6.1.4.1.3530.8. A suffix (for example, 25.1.1), uniquely identifies each OID value.

MIBs specify the conditions that the SNMP agent monitors. A MIB is a database that defines and describes the variables and management data of BlackBerry UEM components, including what each SNMP trap value represents. The MIB determines the types of data the SNMP service can collect about the components. When you configure SNMP monitoring, you use the management tool to compile the MIB.

To learn about network security for SNMP, visit support.microsoft.com.

Monitoring BlackBerry UEM using SNMP tools is not supported for BlackBerry UEM Cloud.

Supported SNMP operations

You can use SNMP operations to collect data from the SNMP agent that runs on the computers where BlackBerry UEM is installed. BlackBerry UEM supports the following SNMP operations:

Operation	Description
Get	Retrieves the value for a specific MIB item.
Get next	Retrieves the value and OID of items in the order that they appear in the MIB file.
Trap	Sends SNMP trap messages from the SNMP agent to the SNMP trap management tool. SNMP trap messages contain data about specific actions that a BlackBerry UEM component performs.

System requirements: SNMP monitoring

Item	Requirement
Supported BlackBerry UEM components	You can configure SNMP monitoring for the following BlackBerry UEM components: • BlackBerry Cloud Connector • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry UEM Core Other BlackBerry UEM components do not support SNMP monitoring.
SNMP management tool	If the management tool does not include a MIB compiler, install a MIB compiler on the computer that hosts the management tool. If you want the SNMP service to send trap messages to report on server activity, verify that the management tool includes an SNMP trap management tool. Alternatively, you can install a standalone SNMP trap management tool on a computer that hosts BlackBerry UEM, or on a separate computer.
Network access	The computer that hosts the SNMP management tool, or a standalone SNMP trap management tool, must be able to access and receive data from the computers where BlackBerry UEM is installed.
SNMP service	On the computers where BlackBerry UEM is installed, install an SNMP service that includes an SNMP agent and SNMP trap service. An SNMP service is available in most versions of Windows. For more information, visit support.microsoft.com.
SNMP service settings	On the computers where BlackBerry UEM is installed, in the Windows Services, configure the following SNMP service settings: • A valid SNMP community name • A minimum of read-only permission for the SNMP community • The IP addresses of names of the computers that the SNMP service can accept SNMP data from.

MIBs for BlackBerry UEM

By default, the MIBs for BlackBerry UEM are on the computer where BlackBerry UEM is installed, in *<drive>*\Program Files\BlackBerry\UEM\Monitoring\bin\mib.

BlackBerry UEM includes the following MIBs that you can use to analyze data from BlackBerry UEM components:

MIB file	Description
BES-BCCMIB-SMIV2	Contains a definition of the OID tree root for the SNMP interface of BlackBerry Cloud Connector

MIB file	Description
BES-BCCMonitoringMIB-SMIV2	Contains definitions of the managed BlackBerry Cloud Connector objects that are accessible and retrievable using the SNMP management tool
BES-BSCPMIB-SMIV2	Contains a definition of the OID tree root for the SNMP interface of BlackBerry Secure Connect Plus
BES-BSCPMonitoringMIB-SMIV2	Contains definitions of the managed BlackBerry Secure Connect Plus objects that are accessible and retrievable using the SNMP management tool
BES-BSGMIB-SMIV2	Contains a definition of the OID tree root for the SNMP interface of the BlackBerry Secure Gateway
BES-BSGMonitoringMIB-SMIV2	Contains definitions of the managed BlackBerry Secure Gateway objects that are accessible and retrievable using the SNMP management tool
BES-CoreEventingMIB-SMIV2	Contains definitions of the traps and notifications that the BlackBerry UEM Core issues
BES-CoreMIB-SMIV2	Contains a definition of the OID tree root for the SNMP interface of the BlackBerry UEM Core
BES-CoreMonitoringMIB-SMIV2	Contains definitions of the managed objects that are accessible and retrievable using the SNMP management tool

Compile the MIB and configure the SNMP management tool

To enable your organization's SNMP monitoring software to monitor BlackBerry UEM components, you must use the SNMP management tool to compile the MIB files of BlackBerry UEM. If the tool does not include an MIB compiler, install a MIB compiler on the computer that hosts the tool.

Before you begin: Read the documentation for the SNMP management tool to learn how to use the tool to compile a MIB.

1. On the computer that hosts BlackBerry UEM, browse to *<drive>*\Program Files\BlackBerry\UEM\Monitoring \bin\mib.
2. Use the SNMP management tool (or the MIB compiler that you installed separately) to compile the .mib files.

Using SNMP to monitor components

To monitor the following components using SNMP, you must configure the settings in the BlackBerry UEM management console:

- BlackBerry UEM Core
- BlackBerry Secure Connect Plus
- BlackBerry Secure Gateway

The BlackBerry UEM Core consists of several subcomponents responsible for managing devices. BlackBerry Secure Connect Plus provides a secure IP tunnel between work space apps on Knox Workspace, and Android Enterprise devices and your organization's network. BlackBerry Secure Gateway provides a secure connection for iOS devices to your organization's mail server through the BlackBerry Infrastructure.

For information about key SNMP counters for monitoring performance and activity see the HTML content.

Configure SNMP to monitor components

To use SNMP to monitor the BlackBerry UEM Core, BlackBerry Secure Connect Plus, BlackBerry Secure Gateway, or BlackBerry Cloud Connector, you must configure the settings in the management console.

1. On the menu bar, click **Settings > Infrastructure > SNMP**.
2. Expand **Global settings** and select the **Enable SNMP monitoring** check box.
3. In the **Community** field, replace the default by typing a new community name.
4. In the IP address field, type the IPv4 UDP address for the server where the trap management tool is installed.
5. In the **Port** field, type the port number for the trap management tool. By default, the port number is 1620.
6. Click **Save**.
7. Expand each BlackBerry UEM instance name. If necessary, you can change the port numbers that you want BlackBerry UEM to use to listen for SNMP data requests. The following port numbers are assigned by default:

   - BlackBerry UEM Core: 1610
   - BlackBerry Secure Connect Plus: 1611
   - BlackBerry Secure Gateway: 1612
   - BlackBerry Cloud Connector: 1613

     Note: To change the port number for the BlackBerry Cloud Connector, you need to edit the value of `com.rim.platform.mdm.zed.snmp.monitoring.udpport` in the BlackBerry UEM database.

   You can't set ports for specific BCN components; however, these services start listening to the assigned default ports after being restarted if Windows SNMP services is installed and configured and **Enable SNMP monitoring** is selected.
8. Click **Save**.

After you finish: Complete one of the following tasks:

- If you enable monitoring for the BlackBerry UEM Core, in the Windows Services, restart the **BlackBerry UEM - UEM Core** service.
- If you enable monitoring for BlackBerry Secure Connect Plus, in the Windows Services, restart **BlackBerry UEM - BlackBerry Secure Connect Plus** service.
- If you enable monitoring for BlackBerry Secure Gateway, in the Windows Services, restart **BlackBerry UEM - BlackBerry Secure Gateway** service.
- If you enable monitoring for BlackBerry Cloud Connector, in the Windows Services, restart **BlackBerry UEM - BlackBerry Cloud Connector** service.

Send system events to a SIEM solution

Security Information and Event Management (SIEM) software collects, analyzes, and aggregates security data from multiple sources to detect potential security threats. To send BlackBerry UEM system events to your organization's SIEM software, you can add a SIEM connector. Currently, adding a SIEM connector is supported for UEM on-premises only

Note: UEM uses TCP to communicate with SIEM. Plain text is not supported.

1. On the menu bar, click **Settings > External integration > SIEM connectors**.
2. Click +.
3. In the **Name** field, type a name for the connector.
4. In the **Connector format** drop-down list, click a logging and auditing file format.
5. In the **SIEM endpoint server name** field, type the SIEM server name.
6. In the **Port** field, type the port of the SIEM server.
7. To use a TLS connection and host validation, verify that the **Enable TLS** and **Enable host validation** check boxes are selected.
8. In the **Status** drop-down list, do one of the following:
   - Click **Enabled** to use the connector.
   - Click **Disabled** to turn off the connector.
9. Click **Save**.

After you finish:

- If you enabled a TLS connection, in **Settings > External integration > Trusted certificates**, click + beside **SIEM server trusts** to upload a trust certificate.
- To see a list of auditable events, navigate to **Settings > Infrastructure > Audit Settings**, click ✎, and in the **Security event audit settings** section click +.

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