



# **BlackBerry UEM**

## **Administrative Guidance Document**

BlackBerry UEM 12



# Contents

- Server and device requirements.....6**
- Preinstallation and preupgrade requirements.....7**
- Firewall requirements.....10**
- Set an environment variable for the Java location.....11**
- Validate and install the BlackBerry UEM software..... 12**
  - deployer.properties file..... 12
- Upgrade the BlackBerry UEM software.....15**
- Logging in to BlackBerry UEM for the first time..... 16**
  - Log in to BlackBerry UEM for the first time.....16
- Create an LDAP client certificate used for mutual authentication and connect to an LDAP directory..... 17**
- Supported activation types.....18**
- Creating activation profiles..... 19**
  - Create an activation profile..... 19
  - Assign a profile or IT policy to a user group.....20
- Activating iOS devices that are enrolled in DEP.....21**
  - Steps to activate devices that are enrolled in DEP..... 21
  - Register iOS devices in DEP and assign them to the BlackBerry UEM server.....22
  - Assign an enrollment configuration to iOS devices.....22
  - Add an enrollment configuration..... 23
- Activate an Android device using a QR Code..... 25**

<b>Restricting enrollment.....</b>	<b>26</b>
<b>Import or export a list of approved device IDs.....</b>	<b>27</b>
<b>Set an activation password and send an activation email message.....</b>	<b>28</b>
<b>Configure management functions.....</b>	<b>29</b>
<b>Assign an app to a user account.....</b>	<b>37</b>
<b>Assign an app to a user group.....</b>	<b>38</b>
<b>Creating and managing administrator roles.....</b>	<b>39</b>
NIAP roles.....	39
Preconfigured roles.....	39
Permissions for preconfigured roles.....	39
Create a custom role.....	62
<b>Administrative commands for retrieving device information.....</b>	<b>64</b>
<b>Finding the last time the device contacted BlackBerry UEM.....</b>	<b>65</b>
<b>Locate the BlackBerry UEM version that you are using.....</b>	<b>66</b>
<b>Create an event notification.....</b>	<b>67</b>
<b>Set the session timeout parameters.....</b>	<b>68</b>
<b>Create a login notice for the consoles.....</b>	<b>69</b>
<b>Auditing.....</b>	<b>70</b>
Viewing audit log data.....	70
Setup export of server audit records to a syslog server.....	70
Setup export of device audit records to a syslog server.....	71
Storing audit logs.....	72
Auditing events in BlackBerry UEM.....	72
Configure audit settings.....	72
Audit record fields for server audits.....	72

TLS auditing.....	76
Certificate audit records.....	77
Auditing administrator actions.....	78
Deployer audit records.....	81
Device audit information.....	81
Enable audit record collection for Samsung Knox devices.....	81
Audit collection filter settings for devices.....	81
Audit record fields for devices.....	82
Searching audit logs for successes and failures.....	83

**Appendix A.....86**

**Appendix B.....88**

**Legal notice..... 90**

# Server and device requirements

The instructions in this document describe how to configure the BlackBerry UEM server and the BlackBerry UEM Client in a manner that is compliant with the Security Target document.

To see the Security Target document, refer to the [NIAP page](#) and search for BlackBerry.

The following are the required server and device versions for your organization to have a fully compliant NIAP certified BlackBerry UEM server:

- BlackBerry UEM 12
- BlackBerry UEM Client for Android version 12
- Apple iOS version 12
- Samsung Knox devices activated using the "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus" option. Note that to use KNOX premium features, you must activate the device using a KNOX premium license.
- iOS devices enrolled using DEP

To see more information about the BlackBerry evaluated product, refer to the [NIAP page](#) and search for BlackBerry.

# Preinstallation and preupgrade requirements

Review the following checklists before you begin installing or upgrading BlackBerry UEM.

## Hardware requirements

Review and complete the UEM [Performance Calculator](#).

The performance calculator provides minimum recommendations based on the values you enter. If you require additional capacity, redundancy, or room for growth, enter values that reflect these needs to accommodate any near future large app and user deployment projects.

Ensure your environment meets the [hardware requirements](#) for your needs.

Ensure that database latency requirements are met. BlackBerry UEM Core servers must have less than 5ms latency to the database server.

## Third-party software requirements

Verify that your computer is running [an operating system that supports BlackBerry UEM](#).

Verify that you have [a supported browser](#) on the computers that host the BlackBerry UEM management console.

The browser must support configuration of the following settings:

- Support for JavaScript
- Cookies turned on
- Support for TLS
- SSL certificate installed to permit trusted connections to the consoles

If you have a requirement to use a proxy server in your organization, verify that you have a supported proxy solution.

Ensure that Windows is up to date and that you perform any reboot required for the update.

Verify that your computer is running Windows PowerShell 2.0 or later for the following:

- RRAS for BlackBerry Secure Connect Plus setup during the BlackBerry UEM installation
- Exchange ActiveSync gatekeeping (optional)

Verify that you have installed JRE 8 on the servers where you will install BlackBerry UEM. [Visit support.blackberry.com](#) to review article 52117.

For more information about supported JRE versions, see the [Compatibility matrix](#).

Verify that you have [a mail server that supports BlackBerry UEM](#).

Verify that [the Exchange ActiveSync version meets the minimum requirements](#).

## Environment configuration requirements

Verify that the [BlackBerry UEM listening ports](#) are configured.

Verify that you opened the necessary ports on your organization's firewall. For more information about port and firewall requirements, visit [support.blackberry.com/community](http://support.blackberry.com/community) to read article 36470.

**Note:** BlackBerry UEM services do not support SSL Termination, SSL Offloading, SSL Packet Inspection or Deep Packet Inspection. Ensure these endpoint services are not enabled on your proxy/firewall.

Verify that the TCP/IP network protocols are turned on for your BlackBerry UEM database.

Verify that you have DNS support for resolving IP addresses into host names.

If you perform the installation or upgrade process on a computer that has more than one NIC, verify that the production NIC is first in the bind order in the Windows network settings.

If a Windows host operating system is configured in a workgroup instead of a domain, verify that you configured the primary DNS suffix. For information on configuring the primary DNS suffix, visit the Microsoft support website.

Ensure that the no count setting for the Microsoft SQL Server is disabled.

Verify that the BlackBerry UEM service account has local administrator permissions on each computer.

The Microsoft SQL Server account must have dbo as its default schema.

Ensure antivirus exclusions have been made for both the extracted installation files and the target installation and logging directories.

For more information, visit [support.blackberry.com/community](http://support.blackberry.com/community) to read article 36596.

If you previously upgraded from a legacy Good Control environment and modified the Java Heap value, make note of the existing value. You will need to reapply the change after upgrade. For more information, visit [support.blackberry.com/community](http://support.blackberry.com/community) to read article 56641.

## Additional considerations

Review all current [Critical Issue Advisories](#). Contact BlackBerry Technical Support if you are unsure whether a particular advisory applies to you.

Review the [Release Notes](#).

Review the [BlackBerry UEM Compatibility Matrix](#) and the [Mobile/Desktop OS Compatibility Matrix](#).

Review the [Installation and Upgrade Guide](#).

Review the information about [supported upgrade environments](#).

If you plan to install BlackBerry UEM in a DMZ, read [Installing BlackBerry UEM in a DMZ](#).



## Additional considerations

Plan for an appropriate amount of downtime based on the number of servers in your environment.

Upgrading the first server may take 45-60 minutes. Additional servers may take 15-45 minutes depending on which components are installed and whether or not these components can be installed in parallel. Consider adding additional time to account for rolling back servers if troubleshooting is required.

Verify that you have [the appropriate licenses](#).

Visit [support.blackberry.com/community](http://support.blackberry.com/community) to read article 38341 about licensing.

Make sure that your perpetual licenses are supported. Visit [support.blackberry.com/community](http://support.blackberry.com/community) to read article 36537.

Perpetual licenses are issued for specific versions of BlackBerry UEM and are not compatible with later versions. If perpetual licenses are covered by a valid support contract, automatic version updates are supported.

Visit [support.blackberry.com/community](http://support.blackberry.com/community) to review article 38980 about upgrades.

If your organization uses a proxy server for Internet access, verify that you have the computer name, port number, and credentials for the proxy server.

If your organization uses Apple VPP accounts, after the upgrade you must generate a new .vpp token file and edit your Apple VPP account information at Apps > iOS App licenses.

If you are planning a multistage upgrade, review the upgrade documentation for the versions you are upgrading to.

Decommission surplus nodes, if applicable. For more information, visit [support.blackberry.com/community](http://support.blackberry.com/community) to read article 46210 and see the [Installation and upgrade content](#) for instructions on how to remove BlackBerry UEM software.

# Firewall requirements

The BlackBerry UEM server requires only inbound port 443 to listen on for connections. BlackBerry recommends that you use the Windows firewall to block all inbound ports except port 443 and any other ports your organization requires for communication.

For more information about port and firewall requirements, visit [support.blackberry.com/community](https://support.blackberry.com/community) to read article 36470.

# Set an environment variable for the Java location

BlackBerry UEM requires you to install a JRE 8 implementation on the servers where you will install BlackBerry UEM, and that you have an environment variable that points to the Java home location. For more information about supported JRE versions, [see the Compatibility matrix](#). When you begin the installation, BlackBerry UEM verifies that it can find Java. If you have installed the Oracle Java SE Runtime Environment in the default location, BlackBerry UEM will find it and automatically set the environment variable. If BlackBerry UEM can't find Java, the setup application will stop and you must set an environment variable for the Java location and ensure that the Java bin folder is included in the Path system variable.

Visit [support.blackberry.com](http://support.blackberry.com) to read article 52117.

**Before you begin:** Verify that you have installed a supported JDK on the server where you will be installing BlackBerry UEM.

1. Open the **Windows Advanced system settings** dialog box.
2. Click **Environment Variables**.
3. Under the **System variables** list, click **New**.
4. In the **Variable name** field, type `BB_JAVA_HOME`.
5. In the **Variable value** field, type the path to the Java installation folder and click **OK**.
6. In the **System variables** list, select **Path** and click **Edit**.
7. If the Path doesn't include the Java bin folder, click **New** and add `%BB_JAVA_HOME%\bin` to the Path.
8. Move the `%BB_JAVA_HOME%\bin` entry high enough in the list that it won't be superseded by another entry and click **OK**.

# Validate and install the BlackBerry UEM software

**Before you begin:** Ensure you have installed Microsoft SQL Server. If you install the SQL Server on a different server, ensure platform IPsec is used to protect the connection.

1. Download the UEM software package.
2. Extract the downloaded software package. The following contents are extracted:
  - Manifest.mf
  - Manifest.sf
  - UEM-12.12.dat
  - Component files
  - Extractor.exe
  - 7 zip Tools directory
3. Run the BESKeyTool 'generatekey' command, which generates a new database encryption key. Open a command prompt as an administrator. Type: `java -cp <install unzip directory>\db\Database\tools\lib\* -Djava.library.path=<install unzip dir>\db\Database\tools\lib\dll\x64\ com.rim.platform.mdm.dal.utils.beskeytool.BESKeyTool generatekey`
4. Double-click the Extractor.exe file, which is the deployer. Windows OS verifies the signature of the deployer. BlackBerry's public key is included in the signature in the digital certificate.
  - If the digital signature verification fails, Windows does not allow the Setup.exe to run.
  - If the extractor.exe digital signature verification passes, the extractor.exe starts to extract files from the software package.
5. If the verification passes, in the dialog box that displays, clear the autorun option. **Note:** You must clear this option for a NIAP installation because you will be using a command line to install the software
6. The extractor.exe file then validates the digital signatures that are on the UEM-12.12.dat file.
  - If the digital signature verification fails, the extractor.exe file writes to local logs and the extractor.exe file stops working.
  - If the digital signature verification passes, files are extracted from the UEM-12.12.dat file.
7. Open a text editor in administrator mode.
8. Use the text editor to open the deployer.properties file. For more information on the file, refer to the [deployer.properties file](#) topic.
9. Change the deployer.properties file to include information that is specific to your organization's environment.
10. Use the text editor to open the niap.properties file. **Note:** The niap.properties file contains all the Cryptographic Engine Configuration requirements.
11. In a command prompt window, in the directory where you extracted the BlackBerry UEM installation files, type: `setup.exe --script --acceptbeseula --showlog --propertyFiles "niap.properties"`.  
The parameter `--showlog` is optional and is used if you want to see the progress of the installation on the computer screen.



**CAUTION:** Record all changes to the niap.properties file for use when you are upgrading your BlackBerry UEM server.

**Note:** No additional configuration is required to enable your cryptography settings.

## deployer.properties file

The following properties apply to the deployer.properties file.

Property	Description
install.path	Specify the location for the installation files. The default location for the installation files is C:/Program Files/BlackBerry/UEM.
logging.common.path	Specify the location for the log files. The default location for the log files is C:/Program Files/BlackBerry/UEM/Logs.
db.host1	Specify the name of the database server that hosts the BlackBerry UEM database. The default entry is localhost.
db.instance	If your environment uses named instances, specify the name of the database instance. If your environment does not use named instances, leave it blank.
db.port	Specify the port that the database server uses to connect to BlackBerry UEM. For a dynamic port, leave this field blank. For a static port, type the port number. The default entry is blank. If you specify a static port, leave the db.instance field blank.
db.static.port.enablement	For a dynamic port, set this field to #. For a static port, leave this field blank. The default entry is #.
db.name	Specify the name of the BlackBerry UEM database. Note if the database does not exist, the script will create a new database with the name that you specify
db.authentication.type	Type INTEGRATED.
db.user	Leave this field blank.
db.pass	Leave this field blank.
service.account.name	This field is automatically populated.
service.account.password	This field is required. Specify the password for the Windows service account.

Property	Description
db.backup.folder	Specify a location for the database backup file. To use the default backup folder, enter a period (.). To skip a database backup, leave this field blank.  The default entry is a period (.).
deploy.bcn	Set to true to install the device connectivity components.  The default entry is true.
deploy.mdm.ec	Set to true to install the primary BlackBerry UEM components.  The default entry is true.
deploy.ui	Set to true to install the BlackBerry UEM management console.  The default entry is true.
ui.port	Specify the port used by the BlackBerry UEM management console.  The default port is 443.
start.windows.services	Set to true to start the BlackBerry UEM services after the installation is complete.  Set to false if you do not want the BlackBerry UEM services to start after the upgrade is complete.  The default entry is true.
alternate.machine.fqdn	Optionally, specify an alternate FQDN to represent this computer in the BlackBerry UEM domain.

# Upgrade the BlackBerry UEM software

## Before you begin:

- Back up your BlackBerry UEM database
1. Download the UEM software package.
  2. Unzip the downloaded software package. The following contents are extracted:
    - Manifest.mf
    - Manifest.sf
    - UEM-12.12.1.dat
    - Extractor.exe
    - 7 zip Tools directory
  3. Double-click the Extractor.exe file, which is the deployer. Windows OS verifies the signature of the deployer. BlackBerry's public key is included in the signature in the digital certificate.
    - If the digital signature verification fails, Windows does not allow the Setup.exe to run.
    - If the extractor.exe digital signature verification passes, the extractor.exe starts to extract files from the software package.
  4. If the verification passes, in the dialog box that displays, clear the autorun option. Note: You must clear this option for a NIAP upgrade because you will be using a command line to install the software.
  5. Click **Unzip**.
  6. Go to C:\BlackBerry\UEM\BlackBerry UEM 12.12.1, and open the "deployer.properties" file in a text editor.
  7. Specify the password for the Windows service account (service.account.password).
  8. Save the file.
  9. To upgrade the UEM software, open a command prompt window with Administrative privileges, and navigate to the directory where you extracted the BlackBerry UEM upgrade files.
  10. Run the following script: `setup.exe --script --iacceptbeseula --showlog --propertyFiles "niap.properties"`. The parameter `--showlog` is optional and is used if you want to see the progress of the upgrade on the computer screen.  
The BlackBerry UEM software upgrades.

**Note:** No additional configuration is required to enable your cryptography settings.

# Logging in to BlackBerry UEM for the first time

The first time that you log in to the management console after you install BlackBerry UEM, you must enter your organization name, SRP ID, and SRP authentication key.



**CAUTION:** Do not reuse the SRP ID from previous BES5, BES10, BES12, or BlackBerry UEM instances when you install a new instance of BlackBerry UEM. You can view the SRP ID and authentication key for your BES10 and BlackBerry UEM instances in *myAccount*, under **My Organization > Servers**. If you do not already have a BlackBerry online account, visit [myAccount](#) and click Sign up.

## Log in to BlackBerry UEM for the first time

**Before you begin:** Verify that you have the BlackBerry UEM SRP identifier and SRP authentication key available.

If the setup application is still open, you can access the management console directly from the Console addresses dialog box.

**Note:** You may be prompted to provide the IP address and port number of the BlackBerry Router or a TCP proxy server.

**Note:** If you receive an error message that your SRP ID cannot be used with the BlackBerry UEM instance you installed, visit [support.blackberry.com/community](https://support.blackberry.com/community) to read article 37117.

1. In the browser, type **https://<server\_name>:<port>/admin**, where *<server\_name>* is the FQDN of the computer that hosts the management console. The default port for the management console is port 443.
2. In the **Username** field, type **admin**.
3. In the **Password** field, type **password**.
4. Click **Sign in**.
5. In the Server location drop-down selection, select the country of the computer that has BlackBerry UEM installed on it, and click **Next**.
6. Type the name of your organization, the SRP identifier, and the SRP authentication key.
7. Click **Submit**.
8. Change the temporary password to a permanent password.
9. Click **Submit**.

**After you finish:**

- When you log in to the management console, you can choose to complete or close the **Welcome to BlackBerry UEM** dialog box. If you close the dialog box, it will not appear during subsequent login attempts.



# Create an LDAP client certificate used for mutual authentication and connect to an LDAP directory

Note that the certificate you use must be signed by a Certificate Authority that the LDAP server trusts, and should be using one of the evaluated ciphersuites which are:

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384

1. To upload an LDAP client certificate to use when you are connecting to an LDAP directory, in a batch file, type the following:

```
SET BESRoot=C:\Program Files\BlackBerry\UEM
SET KEYSTORE_PATH=C:\Users\Administrator\Desktop\LDAP_Info\ldapClientCert
\clientauth.pfx
SET KEYSTORE_PASSWORD=password
ECHO Running KeyMaster to LDAP Client Cert with BESRoot: "%BESRoot%" java -
cp "%BESRoot%\tools\lib\*" -Djava.library.path="%BESRoot%\tools\lib\dll\x64"
com.rim.platform.mdm.keymaster.KeyMaster -keystore "%KEYSTORE_PATH%" -password
"%KEYSTORE_PASSWORD%" load -keystoreType DIRECTORY -BESRoot "%BESRoot%"
```

2. Start the UEM Core service.
3. Log in to the BlackBerry UEM management console.
4. Navigate to **Settings > External Integration > Company Directory**.
5. Add an LDAP directory.
6. When you are configuring the LDAP directory, ensure that you enable SSL, and import the trusted certificate that you uploaded in step 1.
7. Finish configuring the connection and click **Save**.

# Supported activation types

The following activation types are supported for NIAP compliance testing:

- iOS devices that are enrolled in DEP

Samsung Knox devices activated using a QR code:

- Work and personal - full control (Android Enterprise fully managed device with work profile)
- Work space only (Android Enterprise fully managed device)

For more information, refer to the Samsung NIAP configuration documentation.

# Creating activation profiles

You can control how devices are activated and managed using activation profiles. An activation profile specifies how many and what types of devices a user can activate and the type of activation to use for each device type.

The activation type allows you to configure how much control you have over activated devices. You might want complete control over a device that you issue to a user. You might want to make sure that you have no control over the personal data on a device that a user owns and brings to work.

The assigned activation profile applies only to devices the user activates after you assign the profile. Devices that are already activated are not automatically updated to match the new or updated activation profile.

When you add a user to BlackBerry UEM, the Default activation profile is assigned to the user account. You can change the Default activation profile to suit your requirements, or you can create a custom activation profile and assign it to users or user groups.

## Create an activation profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > Activation**.
3. Click **+**.
4. Type a name and description for the profile.
5. In the **Number of devices that a user can activate** field, specify the maximum number of devices the user can activate.
6. In the **Device ownership** drop-down list, select the default setting for device ownership. Perform one of the following actions:
  - If some users activate personal devices and some users activate work devices, select **Not specified**.
  - If users typically activate work devices, select **Work**.
  - If users typically activate personal devices, select **Personal**.
7. Optionally, select an organization notice in the **Assign organization notice** drop-down list. If you assign an organization notice, users activating BlackBerry 10, Windows 10, iOS, or macOS devices must accept the notice to complete the activation process.
8. In the **Device types that users can activate** section, select the device types as required. Device types that you don't select are not included in the activation profile and users can't activate those devices.
9. Perform the following actions for each device type included in the activation profile:
  - Click the tab for the device type.
  - In the **Device model restrictions** drop-down list, select whether to allow or restrict specified devices or to have no restrictions. Click **Edit** to select the devices you want to restrict or allow, and click **Save**.
  - In the **Allowed version** drop-down list, select the minimum allowed version.
  - On the **Windows** tab, you can select one or both form factor options and choose whether to allow or disallow those form factors in the **Device model restrictions** drop-down list.
  - In the **Activation type** section, select an activation type.
    - For Android devices, you can select multiple activation types and rank them to meet your organization's requirements.
    - The "MDM controls" activation type is deprecated for devices with Android 10 and later.
    - For Android devices, if you select an Android Enterprise activation type, you can select the **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure**

**Connect Plus.** option to enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise features (for devices that support Samsung Knox).

- For Android devices, if you select the "MDM controls" activation type and you do not want Knox MDM policy rules to be applied to the devices, clear the **Activate Samsung KNOX APIs on MDM Controls activations** check box. This setting applies only to devices that support KNOX MDM.
- For Android devices, if you select one of the Samsung Knox activation types and want to use Google Play to manage work apps, select **Google Play app management for Samsung Knox Workspace devices**. This option is available only if you have configured a connection to a Google domain. For more information, [see the Configuration content](#).
- For iOS devices, if you select the "User privacy" activation type and you want to enable SIM-based licensing, you must select the **Allow access to SIM card and device hardware information to enable SIM-based licensing** option.
- For iOS devices, if you select the "MDM controls" or User privacy (with SIM-based licensing) activation types, you can restrict unsupervised devices by selecting "Do not allow unsupervised devices to activate."

**Note:** To perform iOS app integrity checking, you must enable CylancePROTECT in your BlackBerry UEM domain. For more information, refer to the [CylancePROTECT content](#).

**10.**For Android devices, in the **SafetyNet attestation options** section, you can optionally select an attestation method. The choices are:

- Perform SafetyNet attestation for device: BlackBerry UEM sends challenges to test the authenticity and integrity of devices.
- Perform SafetyNet attestation on device activation: BlackBerry UEM sends challenges to test the authenticity and integrity of devices when they are activated.
- Perform SafetyNet attestation on BlackBerry Dynamics app activation: BlackBerry UEM sends challenges to test the authenticity and integrity of BlackBerry Dynamics apps when they are activated.

**11.**Click **Add**.

**After you finish:** If necessary, [rank profiles](#).

## Assign a profile or IT policy to a user group

1. On the menu bar, click **Groups > User**.
2. In the group list, click the name of the user group.
3. In the **Assigned profile** section, click **+**.
4. Click **IT policy** or a profile type.
5. In the drop-down list, click the name of the profile or IT policy that you want to assign to the group.
6. For IT policies and ranked profile types, if the profile type that you selected in step 6 is already assigned directly to the group, click **Replace**. Otherwise, click **Assign**.

# Activating iOS devices that are enrolled in DEP

You can enroll iOS devices in Apple's Device Enrollment Program and assign enrollment configurations to devices using the BlackBerry UEM management console. The enrollment configurations include extra rules, such as "Enable supervised mode," that are assigned to the devices during MDM enrollment.

You can use an Apple Business Manager account to synchronize BlackBerry UEM with DEP. Apple Business Manager is a web-based portal in which you can enroll and manage iOS devices in DEP, and manage Apple VPP accounts. If your organization uses DEP or VPP, you can upgrade to Apple Business Manager.

When the devices are activated, BlackBerry UEM sends IT policies and profiles that you assigned to users.

## Steps to activate devices that are enrolled in DEP

When you activate iOS devices that are enrolled in Apple's Device Enrollment Program, you perform the following actions:

Step	Action
1	Register iOS devices in DEP and assign them to the BlackBerry UEM server.
2	If you did not select "Automatically assign new devices to this configuration" when you created the enrollment configuration, or you want to assign a different configuration, <a href="#">assign an enrollment configuration</a> .
3	Optionally, add the BlackBerry UEM Client to the app list and assign it to user accounts or user groups. See <a href="#">Add an iOS app to the app list</a> .
4	If you do not want to use the default activation profile, see <a href="#">Create an activation profile and assign it to a user account or to a group that the user belongs to</a> . Optionally, <a href="#">Assign an activation profile to iOS devices</a> .
5	<a href="#">Set an activation password for the user</a> and send an activation email to users using the Apple DEP email template. When you set the activation password, you must select the "Default device activation" option. Company directory users can use their company directory usernames and passwords so you don't need to create an activation password. Users must enter their usernames in the format domain\username. Optionally, you can <a href="#">Assign a user to an iOS device</a> . When you assign a user to the device in BlackBerry UEM, they are not prompted for a username or password during device activation.
6	Distribute the devices to users and have them complete the setup. After the setup completes, users must install and open the BlackBerry UEM Client.

# Register iOS devices in DEP and assign them to the BlackBerry UEM server

To register the devices, you must enter the device serial numbers in the Apple Business Manager or DEP Portal and assign the devices to the BlackBerry UEM server. You can enter the serial numbers in the following ways:

- Type in each number
- Select the order number that Apple assigned to the devices when you purchased them
- Upload a .csv file containing the serial numbers

**Before you begin:** Configure BlackBerry UEM to use DEP. For more information, see the [on-premises Configuration content](#). or the [UEM Cloud Configuration content](#).

**Before you begin:** Configure BlackBerry UEM to use DEP. For more information, see the [on-premises Configuration content](#).

1. In a browser, type **business.apple.com** or **deploy.apple.com**.
2. Sign in to your Apple Business Manager or DEP account.
3. In the **Device Enrollment Program** section, click **Manage Devices**.
4. Follow the steps to enter the serial numbers for the devices.
5. Assign the serial numbers to the BlackBerry UEM server.





**After you finish:** [Assign an enrollment configuration to iOS devices](#).

## Assign an enrollment configuration to iOS devices

If you created an enrollment configuration and selected "Automatically assign all new devices to this configuration," BlackBerry UEM automatically assigns the configuration when DEP devices synchronize with BlackBerry UEM. Otherwise, you must assign an enrollment configuration to devices. BlackBerry UEM synchronizes with DEP on a daily schedule and whenever you view the Apple DEP devices page.


If the activation status for a device is still pending, you can remove an existing enrollment configuration and assign a new one.

In the BlackBerry UEM management console, the following icons indicate the status of enrollment configurations:

Status	Icon
	An enrollment configuration is assigned.
	No enrollment configuration is assigned.
	An enrollment configuration is applied, but it is pending activation.
	Activation was successful.

**Before you begin:** [Register iOS devices in DEP and assign them to the BlackBerry UEM server](#).

1. On the menu bar, click **Users > Apple DEP devices**.
2. Select the check boxes beside the devices that you want to assign an enrollment configuration to. You must select devices that are registered to the same DEP account.


3. Click .
4. In the **Enrollment configuration** drop-down list, select the enrollment configuration that you want to assign.
5. Click **Assign**.

**After you finish:**

Distribute the iOS devices to users. As part of the device setup, devices are activated with BlackBerry UEM. Users are prompted for a username and password. Company directory users can use their company directory username (in the format domain\username) and password. Local users need to use an activation password. See [Set an activation password for the user](#).

## Add an enrollment configuration

An enrollment configuration allows you to define how devices that are enrolled in DEP are set up when they are activated in BlackBerry UEM. You can create as many enrollment configurations as your organization needs.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Apple Device Enrollment Program**.
3. Click the name of a DEP account.
4. In the **DEP enrollment configurations** section, click .
5. Type a name for the configuration.
6. Complete one of the following tasks:
  - If you want BlackBerry UEM to automatically assign the enrollment configuration when DEP devices synchronize to BlackBerry UEM, select the "Automatically assign all new devices to this configuration" checkbox. BlackBerry UEM synchronizes with Apple DEP on a daily schedule and whenever you view the Apple DEP devices page.

**Note:** If you previously created an enrollment configuration with this setting and the configuration was applied to devices, BlackBerry UEM does not assign the new enrollment configuration.

**Note:** You can select only one enrollment configuration to be automatically assigned to new DEP devices. If you previously created an enrollment configuration with this setting, the setting is removed from the previous configuration and added to the new one.
  - If you want to manually assign the enrollment configuration to specific devices, leave the "Automatically assign all new devices to this configuration" box unchecked.
7. Optionally, type a department name and support phone number to be displayed on devices during setup.
8. In the **Device configuration** section, select from the following options:
  - Allow pairing - if selected, users can pair the device with a computer
  - Enable supervised mode - if selected, devices are activated in supervised mode. You must select at least one of "Enable supervised mode" or "Allow removal of MDM profile."
  - Mandatory - if selected, users are not prompted to accept the enrollment configuration
  - Allow removal of MDM profile - if selected, users can deactivate devices. You must select at least one of "Enable supervised mode" or "Allow removal of MDM profile."
  - Wait until device is configured - if selected, users cannot cancel the device setup until activation with BlackBerry UEM is completed. This setting is valid only if you select "Enable supervised mode."
9. In the **Skip during setup** section, select the items that you do not want to include in the device setup:
  - Passcode - if selected, users aren't prompted to create a device passcode
  - Location services - if selected, location services are disabled on the device
  - Restore - if selected, users can't restore data from a backup file

- Move from Android - if selected, users can't restore data from an Android device
- Apple ID - if selected users are prevented from signing in to Apple ID and iCloud
- Terms and conditions - if selected, users don't see the iOS terms and conditions
- Siri - if selected, Siri is disabled on devices
- Diagnostics - if selected, diagnostic information isn't automatically sent from the device during setup
- Biometric - if selected, users can't set up Touch ID
- Payment - if selected, users can't set up Apple pay
- Zoom - if selected, users can't set up Zoom
- Home button setup - if selected, users can't adjust the Home button's click
- Device-to-device migration - if selected, users can't transfer data from their previous device to their new device

**10.**Click **Save**.

**11.**If you selected "Automatically assign new devices to this configuration," click **Yes**.

**After you finish:** If you did not select "Automatically assign new devices to this configuration", see [Assign an enrollment configuration to iOS devices](#).



# Activate an Android device using a QR Code

QR Code activation is supported on Android devices.

**Before you begin:** You need a QR Code. You can find it in the activation email that you received from your administrator, or you can generate one in BlackBerry UEM Self-Service.


1. Factory reset the device
2. Tap on the screen 7 times which will start the QR code reader.
3. Read the license agreement and tap **I Agree**.
4. Scan the QR Code that you received in the activation email or that you generated in BlackBerry UEM Self-Service.
5. If you are prompted to enter the password for your email account or the passcode for your device, follow the instructions on the screen.

**After you finish:** To verify that the activation process completed successfully, you can perform one of the following actions:

- On the device, open the BlackBerry UEM Client app and tap **About**. In the Activated Device and Compliance Status sections, verify that the device information and the activation time stamp are present.
- In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

# Restricting enrollment

Perform this task if your internal guidance requires that you restrict your device to an internal list based on device ID.

1. In the management console, navigate to the activation profile for your organization's devices.
2. Click .
3. In the **Number of devices that a user can activate**, enter the number of devices that you want to activate.
4. Click **Allow only approved device IDs**.
5. Click **Save**.
6. Click **Users > Managed devices**.
7. Click **Set Activation password**.
8. Set the **Activation period expiration** time, which allows you to set a specific time that the user is enrolled for.

# Import or export a list of approved device IDs

You can import and export a list of unique device identifiers to restrict which devices can enroll with BlackBerry UEM. Currently the only unique identifier that BlackBerry UEM supports is the device serial number.



**CAUTION:** LG devices do not support this feature.

**Before you begin:** Ensure you have a .csv file that contains the list of unique device identifiers.

1. Navigate to **Settings > General settings > Activation defaults**.
2. In the **Import or export device IDs** section, beside the **Upload approved device IDs (.csv)** field, click **Browse**.
3. Navigate to your organization's .csv file.
4. Click **Open**.
5. Click **Save**.
6. After you have imported the list, to export the list, click **Export approved device IDs (.csv)**.

# Set an activation password and send an activation email message

You can set an activation password and send a user an activation email with the information required to activate one or more devices.

In on-premises environments, the email message is sent from the email address that you configured in the SMTP server settings.

**Before you begin:** [Create an activation email template.](#)

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. In the Activation details pane, click **Set activation password**.
5. In the **Activation option** drop-down list, perform one of the following tasks:
  - If you want the user to activate their device with the activation profile that is currently assigned to them, select **Default device activation**. You can see the activation profile that is assigned to the user in the IT policy and profiles section on the Summary tab.
  - If you want to pair an activation password with a specific activation profile, select **Device activation with specified activation profile**. For more information, see [Allowing users to activate multiple devices with different activation types](#).
6. In the **Activation password** drop-down list, perform one of the following tasks:
  - If you want to automatically generate a password, select **Autogenerate device activation password and send email with activation instructions**. When you select this option, you must select an email template to send the information to the user.
  - If you want to set an activation password for the user and, optionally, send an activation email, select **Set device activation password**.
7. Optionally, change the activation period expiration. The activation period expiration specifies how long the activation password remains valid.
8. If you want the activation password to be valid only for one device activation, select **Activation period expires after the first device is activated**.
9. In the **Activation email template** drop-down list, select the email template that you want to use.
10. Click **Submit**.

# Configure management functions

Use the following tables to configure management functions.

## Android

PP/ST Reference	MDMPP40 Management Function	Android - UEM Section	Android - UEM Action
1	transition to the locked state, (MDF Function 6)	Command	Users > Managed devices > Device Tab > Lock device
2	full wipe of protected data, (MDF Function 7)	Command	Users > Managed devices > Device Tab > Delete all device data
3	unenroll from management	IT Policy	Global (all Android devices) > Allow users to deactivate devices from UEM Client
4	install policies	IT Policy	User(User Group) > Assign Profile
5	query connectivity status	Command	Users > Managed devices > Device Tab > Update Device Information
6	query the current version of the MD firmware/software	Command	Users > Managed devices > Device Tab > Update Device Information
7	query the current version of the hardware model of the device	Command	Users > Managed devices > Device Tab > Update Device Information
8	query the current version of installed mobile applications	Command	Users > Managed devices > Device Tab > Update Device Information
9	import X.509v3 certificates into the Trust Anchor Database	CA Profile	Profiles and policies > Certificates-CA certificate > Create and Assign CA Profile to the user (User Group)
10	install applications	App Mgmt	Application Management
11	update system software	Compliance	Compliance > Device SR requirements profile
12	remove applications	App Profile	Unassign app profile
13	remove Enterprise applications	App Profile	Unassign app profile
14	wipe Enterprise data, (MDF Function 28)	Command	Users > Managed devices > Device Tab > Delete only work data

PP/ST Reference	MDMPP40 Management Function	Android - UEM Section	Android - UEM Action
15	remove imported X.509v3 certificates and [selection: no other X.509v3 certificates, [assignment: list of other categories of X.509v3 certificates] ] in the Trust Anchor Database	CA Profile	Profiles and policies > Certificates-CA certificate > Unassign CA Profile from user
17	import keys/secrets into the secure key storage, (MDF Function 9)	Shared Certificate	Assign Profile
18	destroy imported keys/secrets and [selection: no other keys/secrets	Shared Certificate	Assign Profile
19	read audit logs kept by the MD, (MDF Function 32)	IT Policy	Global (Samsung KNOX devices only) > Enable audit logging
25	a. password policy: a. minimum password length	IT Policy	Global > Password requirements > Minimum password length
25	b. password policy: b. minimum password complexity	IT Policy	Global > Password requirements > Complexity
25	c. password policy: c. maximum password lifetime (MDF Function 1)	IT Policy	Global > Password requirements - Password expiration timeout
26	a. Configure session locking policy: a. screen-lock enabled/disabled	IT Policy	Global > Allow user to configure screen timeout
26	b. Configure session locking policy: b. screen lock timeout	IT Policy	Global > Screen timeout
26	c. Configure session locking policy: c. number of authentication failures	IT Policy	Global > Password requirements - Maximum failed password attempts
27	wireless networks (SSIDs) to which the MD may connect (WLAN Client EP Function 2)	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > Android > BSSID
28	a. Security policy for each wireless network: a. specify the CA(s) from which the TSF will accept WLAN authentication server certificate(s)	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > Android > Trust > CA Certificate Profiles

PP/ST Reference	MDMPP40 Management Function	Android - UEM Section	Android - UEM Action
28	b. Security policy for each wireless network: b. ability to specify security type	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > Android > Security Type
28	c. Security policy for each wireless network: c. ability to specify authentication protocol	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > Android > Protocols > Authentication protocol
28	d. Security policy for each wireless network: d. client credentials to be used for authentication	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > Android > Authentication > Authentication type
29	a. application installation policy by [selection]: a. specifying authorized application repository(s)	IT Policy	Global > Allow installation of non Google Play apps
29	b. application installation policy by [selection]: b. specifying a set of allowed applications and versions (an application whitelist)	App Mgmt	Application Management - Admin chooses to import which version of APK to import into UEM Server
29	c. application installation policy by [selection]: c.denying application installation], (MDF Function 8)	App Mgmt	Application Management - Apps not imported by Admin cannot be installed on controlled area of device
30	a. enable/disable policy for [assignment:camera] a. across device	IT Policy	Global (all Android devices) > Disable camera
30	a. enable/disable policy for [assignment: microphone] a. across device	IT Policy	Global (all Android devices) > Allow microphone
31	a. enable/disable VPN protection: a. Across device	VPN Profile	Profiles and policies > Networks and Connections > VPN > Android
31	b. enable/disable VPN protection: selection: b. on a per-app basis,	VPN Profile	Profiles and policies > Networks and Connections > VPN > Android
32	enable/disable [assignment: list of radios]- Bluetooth	IT Policy	Global (all Android devices) > Allow Bluetooth
32	enable/disable [assignment: list of radios]- NFC	IT Policy	Global (Samsung KNOX devices only)->Allow NFC

PP/ST Reference	MDMPP40 Management Function	Android - UEM Section	Android - UEM Action
32	enable/disable [assignment: list of radios]- WiFi	IT Policy	Global (all Android devices)->Allow changing Wi-Fi settings
34	enable/disable policy for [Bluetooth tethering	IT Policy	Global (Samsung KNOX devices only) > Allow Bluetooth tethering
34	enable/disable policy for [USB tethering	IT Policy	Global (Samsung KNOX devices only) > Allow USB tethering
34	enable/disable policy for [Wi-Fi tethering	IT Policy	Global (Samsung KNOX devices only) > Allow Wi-Fi tethering
35	enable/disable policy for developer modes, (MDF Function 26)	IT Policy	Work profile (all Android devices) > Allow developer options
36	enable policy for data-at rest protection, (MDF Function 20)	Default function of device	
37	enable policy for removable media's data-at-rest protection, (MDF Function 21)	IT Policy	Global (Samsung KNOX devices only) > Require SD card encryption
38	enable/disable policy for local authentication bypass, (MDF Function 27)	IT Policy	Work profile (all Android devices) > Allow lock screen features Personal profile (all Android devices) > Allow lock screen features
40	f. enable/disable policy for display notification in the locked state of [selection: f. all notifications] (MDF Function 19)	IT Policy	Global (all Android devices) > Allow secure notifications on secure keyguard screens
47	the unlock banner policy, (MDF Function 36)	Custom profiles	Device profile > Organization notice
48	configure the auditable items (MDF Function 37)	IT Policy	Global (Samsung KNOX devices only) > Enable audit logging
49	a. enable/disable [selection: a. USB mass storage mode	IT Policy	Work profile (all Android devices) > Allow USB file transfer
51	enable/disable [selection: USB tethering authenticated by [ no authentication]] (MDF Function 41)	IT Policy	Global (Samsung KNOX devices only) > Allow USB tethering
51	enable/disable [selection: a. Hotspot functionality authenticated by [pre-shared key],	IT Policy	Global (all Android devices) > Allow tethering configuration



PP/ST Reference	MDMPP40 Management Function	Android - UEM Section	Android - UEM Action
52	a. enable/disable location services: a. across device,	IT Policy	Work profile (all Android devices) > Allow obtaining device location
54	enable/disable policy for the Always-On VPN protection across device (MDF Function 45)	VPN Profile	Profiles and policies > Networks and Connections > VPN > Android
55	enable/disable policy for use of Biometric Authentication Factor - Fingerprint	IT Policy	Work profile (all Android devices) > Allow fingerprint authentication
55	enable/disable policy for use of Biometric Authentication Factor - Iris	IT Policy	Work profile (Samsung KNOX devices only) > Allow iris authentication
55	enable/disable policy for use of Biometric Authentication Factor - Hybrid Authentication	IT Policy	Work profile (Samsung KNOX devices only) > Allow fingerprint authentication Work profile (Samsung KNOX devices only) > Allow iris authentication

## iOS

PP/ST Reference	MDMPP40 Management Function	iOS- UEM Section	iOS- UEM Action
1	transition to the locked state, (MDF Function 6)	Command	Users > Managed devices > Device Tab > Lock device
2	full wipe of protected data, (MDF Function 7)	Command	Users > Managed devices > Device Tab > Delete only work data
3	unenroll from management	Command	Users > Managed devices > Device Tab > Delete only work data
4	install policies	IT Policy	User(User Group) > Assign Profile
5	query connectivity status	Command	Users > Managed devices > Device Tab > Update Device Information
6	query the current version of the MD firmware/software	Command	Users > Managed devices > Device Tab > Update Device Information
7	query the current version of the hardware model of the device	Command	Users > Managed devices > Device Tab > Update Device Information
8	query the current version of installed mobile applications	Command	Users > Managed devices > Device Tab > Update Device Information

PP/ST Reference	MDMPP40 Management Function	iOS- UEM Section	iOS- UEM Action
9	import X.509v3 certificates into the Trust Anchor Database	CA Profile	Profiles and policies > Certificates-CA certificate > Create and Assign CA Profile to the user
10	install applications	App Mgmt	Application Management
11	update system software	Command	Users > Managed devices > Device Tab > Software Version (action available if new OS is available)
12	remove applications	App Profile	Unassign app profile
13	remove Enterprise applications	App Profile	Unassign app profile
14	wipe Enterprise data, (MDF Function 28)	Command	Users > Managed devices > Device Tab > Delete only work data
17	import keys/secrets into the secure key storage, (MDF Function 9)	Shared Cert or SCEP Profile	Assign Profile
18	destroy imported keys/secrets and [selection: no other keys/secrets	Shared Cert or SCEP Profile	Assign Profile
25	a. password policy: a. minimum password length	IT Policy	iOS > Password required for device > Minimum passcode length
25	b. password policy: b. minimum password complexity	IT Policy	iOS > Password required for device > Minimum number of complex characters
25	c. password policy: c. maximum password lifetime (MDF Function 1)	IT Policy	iOS > Password required for device > Maximum passcode age
26	a. Configure session locking policy: a. screen-lock enabled/ disabled	IT Policy	iOS > Password required for device > Maximum auto-lock
26	b. Configure session locking policy: b. screen lock timeout	IT Policy	iOS > Password required for device > Maximum auto-lock
26	c. Configure session locking policy: c. number of authentication failures	IT Policy	iOS > Password required for device > Maximum failed password attempts
27	wireless networks (SSIDs) to which the MD may connect (WLAN Client EP Function 2)	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > iOS

PP/ST Reference	MDMPP40 Management Function	iOS- UEM Section	iOS- UEM Action
28	a. Security policy for each wireless network: a. specify the CA(s) from which the TSF will accept WLAN authentication server certificate(s)	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > iOS > Trust > CA Certificate Profiles
28	b. Security policy for each wireless network: b. ability to specify security type	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > iOS > Security Type
28	c. Security policy for each wireless network: c. ability to specify authentication protocol	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > iOS > Protocols > Authentication protocol
28	d. Security policy for each wireless network: d. client credentials to be used for authentication	Wi-Fi Profile	Profiles and policies > Networks and Connections > Wi-Fi > iOS > Authentication > Authentication type
29	a. application installation policy by [selection]: a. specifying authorized application repository(s)	IT Policy	iOS > Allow App Store
29	b. application installation policy by [selection]: b. specifying a set of allowed applications and versions (an application whitelist)	Compliance	iOS > Compliance > Show only allowed apps on device
29	c. application installation policy by [selection]: c.denying application installation], (MDF Function 8)	Compliance	iOS > Compliance > Restricted app is installed
30	a. enable/disable policy for [assignment:camera] a. across device	IT Policy	iOS > Allow use of camera
31	a. enable/disable VPN protection: a. Across device	VPN Profile	Profiles and policies > Networks and Connections > VPN > iOS
31	b. enable/disable VPN protection: selection: b. on a per-app basis,	VPN Profile	Profiles and policies > Networks and Connections > VPN > iOS
40	f. enable/disable policy for display notification in the locked state of [selection: f. all notifications] (MDF Function 19)	IT Policy	Show Notification Center in lock screen

PP/ST Reference	MDMPP40 Management Function	iOS- UEM Section	iOS- UEM Action
44	[selection: certificate, public-key] used to validate digital signature on applications, (MDF Function 33)	CA Profile	Profiles and policies > Certificates-CA certificate > Create and Assign CA Profile to the user
47	the unlock banner policy, (MDF Function 36)	Device Profile	Device Profile: Set wall paper
55	enable/disable policy for use of Biometric Authentication Factor - Fingerprint	IT Policy	Allow Touch ID and Face ID to unlock device
55	enable/disable policy for use of Biometric Authentication Factor - Iris	IT Policy	Allow Touch ID and Face ID to unlock device

# Assign an app to a user account

If you need to control apps at the user level, you can assign apps or app groups to user accounts. When you assign an app to a user, the app is made available to any devices that the user has activated for that device type, and the app is listed in the work app catalog on the device.

You can also assign apps to users for device types that the user has not activated yet. If the user activates a different device type in the future, the proper apps are made available to that user's new device.

The same app can be assigned directly to the user account, or inherited from user groups or device groups. The settings for the app (for example, whether the app is required) are assigned based on priority: device groups have the highest priority, then user accounts, then user groups.

## Before you begin:

- Add the app to the available app list.
- Optionally, add the apps to an app group.

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. In the **Apps** section, click **+**.
5. Select the check box beside the apps or app group that you want to assign to the user account.
6. Click **Next**.
7. In the **Disposition** drop-down list for the app, perform one of the following actions:
  - To require users to install the app, select **Required**.
  - To permit users to install and remove the app, select **Optional**.

**Note:** If the same app is assigned to a user account, a user group that the user belongs to, and the device group the device belongs to, the disposition of the app assigned in the device group takes precedence.
8. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
9. For iOS and Android devices, if there is an available app configuration, select the app configuration to assign to the app.

# Assign an app to a user group

When you assign apps to a user group, the apps are made available to any applicable devices that the members of the user group have activated. You can also assign apps to user groups for device types that the members of the user group have not activated yet. This makes sure that if any member of the group activates a different device type in the future, the proper apps are made available to new devices.

If a user account is a member of multiple user groups that have the same apps or app groups assigned to them, only one instance of the app or app group appears in the list of assigned apps for that user account. The same app can be assigned directly to the user account, or inherited from user groups or device groups. The settings for the app (for example, whether the app is required) are assigned based on priority. Device groups have the highest priority, then user accounts, then user groups.

## Before you begin:

- Add the app to the available app list.
- Optionally, add the apps to an app group.

1. On the menu bar, click **Groups > User**.
2. In the group list, click the name of the user group.
3. In the **Assigned apps** section, click **+**.
4. In the search field, type the app name, vendor, or URL of the app that you want to add.
5. Select the check box beside the apps or app group that you want to assign to the user group.
6. Click **Next**.
7. In the **Disposition** drop-down list for the app, perform one of the following actions:
  - To require users to install the app, select **Required**.
  - To permit users to install and remove the app, select **Optional**.

**Note:** If the same app is assigned to a user account, a user group that the user belongs to, and the device group the device belongs to, the disposition of the app assigned in the device group takes precedence.
8. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
9. For iOS and Android devices, if there is an available app configuration, select the app configuration to assign to the app.

# Creating and managing administrator roles

You can review the preconfigured roles available for administrators in BlackBerry UEM to determine if you need to create custom roles or change role settings to meet your organization's requirements. You must be a Security Administrator to create custom roles, view information about a role, change role settings, delete roles, and rank roles.

## NIAP roles

BlackBerry UEM supports the following administrative roles:

- Security Configuration Administrator - This role is responsible for configuring the BlackBerry UEM settings (including selecting audit events to be collected).
- Device User Group Administrators - This role is responsible for setting up policies, accounts for mobile device users, inspecting the status of a given mobile device, and revoking/unenrolling a device.
- Auditor - This role only has permissions to view the BlackBerry UEM audit logs.
- MD user - This role can enroll devices into their account and cannot login to the BlackBerry UEM management console.
- Server Primary Administrator - an administrator on the Windows platform in which the UEM Server runs.

## Preconfigured roles

The Security Administrator role in BlackBerry UEM has full permissions to the management console, including creating and managing roles and administrators. At least one administrator must be a Security Administrator.

BlackBerry UEM includes preconfigured roles in addition to the Security Administrator role. You can edit or delete all roles except the Security Administrator role.

The following preconfigured roles are available:

- Security Administrator: Full permissions
- Enterprise Administrator: All permissions except for creating and managing roles and administrators
- Senior HelpDesk: Permissions to perform intermediate administrative tasks
- Junior HelpDesk: Permissions to perform basic administrative tasks

## Permissions for preconfigured roles

The following tables list the permissions that are turned on by default for each preconfigured role in BlackBerry UEM. The Security Administrator role in BlackBerry UEM has full permissions to the management console, including creating and managing roles and administrators.

### Roles and administrators

By default, the Security Administrator role in BlackBerry UEM includes permissions to create and manage roles and administrators. These permissions are not available in the management console and cannot be turned on for any other role.

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View roles	✓	NA	NA	NA
Create and edit roles	✓	NA	NA	NA
Delete roles	✓	NA	NA	NA
Rank roles	✓	NA	NA	NA
Create administrators	✓	NA	NA	NA
Delete administrators	✓	NA	NA	NA
Edit non-administrative attributes of administrators	✓	NA	NA	NA
Change password for other administrators	✓	NA	NA	NA
Change role membership for administrators	✓	NA	NA	NA

### Directory access

You can specify the company directories that the administrator can search.

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
All company directories	✓	✓	✓	✓
Selected company directories only				

### Group management

You can specify the groups that the administrator can manage. To manage users that do not belong to a group, administrators must have permission to manage all groups and users.

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
All groups and users	✓	✓	✓	✓
Selected groups				



## Users and devices

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View users and activated devices	✓	✓	✓	✓
Create users	✓	✓	✓	
Edit users	✓	✓	✓	✓
Assign user roles	✓	✓	✓	✓
Delete users	✓	✓	✓	
Export user list	✓	✓		
Generate an activation password and send email	✓	✓	✓	✓
Generate activation passwords and send activation email messages to multiple users	✓	✓	✓	
Specify an activation password	✓	✓	✓	✓
Specify multiple activation passwords with unique activation profiles for a user	✓	✓		
Specify whether activation passwords expire after first device is activated	✓	✓		
View user activation QR codes and access keys	✓	✓		
Specify account password	✓	✓	✓	✓
Change multiple account passwords	✓	✓	✓	

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Set BlackBerry 2FA preauthentication	✓	✓		
Manage devices	✓	✓	✓	✓
Enable work space	✓	✓	✓	✓
Disable work space	✓	✓	✓	✓
Lock work space	✓	✓	✓	✓
Reset work space password	✓	✓	✓	✓
Specify device password	✓	✓	✓	✓
Lock device and set message	✓	✓	✓	✓
Unlock device and clear password	✓	✓	✓	✓
Delete only work data	✓	✓	✓	✓
Delete only work data from multiple devices	✓			
Delete all device data	✓	✓	✓	✓
Delete all device data from multiple devices	✓			
Delete device	✓	✓		
Delete multiple devices	✓			
Specify work password and lock	✓	✓	✓	✓
Get device logs	✓	✓	✓	
Enable Activation Lock	✓	✓	✓	✓
Disable Activation Lock	✓	✓	✓	✓
Lost Mode	✓	✓	✓	✓
Turn on Lost Mode	✓	✓	✓	✓

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Turn off Lost Mode	✓	✓	✓	✓
Locate device	✓	✓	✓	✓
Check in device	✓	✓	✓	
Restart device	✓	✓	✓	✓
Update iOS software	✓	✓	✓	✓
Update iOS software on multiple devices	✓			
Turn off device	✓	✓	✓	✓
View device location details	✓	✓	✓	
View device location history	✓	✓		
View Exchange gatekeeping information	✓	✓		
View Apple DEP device information	✓	✓	✓	✓
Assign enrollment configurations	✓	✓		
View One-time Password tokens	✓	✓	✓	✓
Assign One-time Password tokens	✓	✓		
Send email to users	✓	✓	✓	
View Activation Lock bypass history	✓	✓	✓	
Manage BlackBerry Dynamics apps	✓	✓	✓	✓
Lock app	✓	✓	✓	
Unlock app	✓	✓	✓	✓

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Delete app data	✓	✓	✓	✓
Control logging for app	✓	✓	✓	
Manage Intune apps	✓	✓	✓	

### Dedicated device

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View shared device group settings	✓	✓		
Create and edit shared device groups	✓	✓		
Delete shared device groups	✓	✓		
View public device group settings	✓	✓		
Create and edit public device groups	✓	✓		
Delete public device groups	✓	✓		

### Groups

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View group settings	✓	✓	✓	✓
Create and edit user groups	✓	✓	✓	
Assign user roles	✓	✓	✓	
Add and remove users from user groups	✓	✓	✓	
Delete user groups	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Create and edit device groups	✓	✓	✓	
Delete device groups	✓	✓		

### Policies and profiles

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View IT policies	✓	✓	✓	✓
Create and edit IT policies	✓	✓		
Delete IT policies	✓	✓		
View email profiles	✓	✓	✓	✓
Create and edit email profiles	✓	✓		
Delete email profiles	✓	✓		
View IMAP/POP3 email profiles	✓	✓	✓	✓
Create and edit IMAP/POP3 email profiles	✓	✓		
Delete IMAP/POP3 email profiles	✓	✓		
View enterprise connectivity profiles	✓	✓	✓	✓
Create and edit enterprise connectivity profiles	✓	✓		
Delete enterprise connectivity profiles	✓	✓		
View device SR requirements profiles	✓	✓	✓	✓

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Create and edit device SR requirements profiles	✓	✓		
Delete device SR requirements profiles	✓	✓		
View activation profiles	✓	✓	✓	✓
Create and edit activation profiles	✓	✓		
Delete activation profiles	✓	✓		
View Wi-Fi profiles	✓	✓	✓	✓
Create and edit Wi-Fi profiles	✓	✓		
Delete Wi-Fi profiles	✓	✓		
View VPN profiles	✓	✓	✓	✓
Create and edit VPN profiles	✓	✓		
Delete VPN profiles	✓	✓		
View compliance profiles	✓	✓	✓	✓
Create and edit compliance profiles	✓	✓		
Delete compliance profiles	✓	✓		
View device profiles	✓	✓	✓	✓
Create and edit device profiles	✓			
Delete device profiles	✓	✓		
View proxy profiles	✓	✓	✓	✓
Create and edit proxy profiles	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Delete proxy profiles	✓	✓		
View web content filter profiles	✓	✓	✓	✓
Create and edit web content filter profiles	✓	✓		
Delete web content filter profiles	✓	✓		
View FileVault profiles	✓	✓	✓	✓
Create and edit FileVault profiles	✓	✓		
Delete FileVault profiles	✓	✓		
View location service profiles	✓	✓	✓	✓
Create and edit location service profiles	✓	✓		
Delete location service profiles	✓	✓		
View app lock mode profiles	✓	✓	✓	✓
Create and edit app lock mode profiles	✓	✓		
Delete app lock mode profiles	✓	✓		
View single sign-on profiles	✓	✓	✓	✓
Create and edit single sign-on profiles	✓	✓		
Delete single sign-on profiles	✓	✓		
View CA certificate profiles	✓	✓	✓	✓

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Create and edit CA certificate profiles	✓	✓		
Delete CA certificate profiles	✓	✓		
View shared certificate profiles	✓	✓	✓	✓
Create and edit shared certificate profiles	✓	✓		
Delete shared certificate profiles	✓	✓		
View SCEP profiles	✓	✓	✓	✓
Create and edit SCEP profiles	✓	✓		
Delete SCEP profiles	✓	✓		
View OCSP profiles	✓	✓	✓	✓
Create and edit OCSP profiles	✓	✓		
Delete OCSP profiles	✓	✓		
View certificate retrieval profiles	✓	✓	✓	✓
Create and edit certificate retrieval profiles	✓	✓		
Delete certificate retrieval profiles	✓	✓		
View CRL profiles	✓	✓	✓	✓
Create and edit CRL profiles	✓	✓		
Delete CRL profiles	✓	✓		
View managed domains profiles	✓	✓	✓	✓



Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Create and edit managed domains profiles	✓	✓		
Delete managed domains profiles	✓	✓		
View user credential profiles	✓	✓	✓	✓
Create and edit user credential profiles	✓	✓		
Delete user credential profiles	✓	✓		
View custom payload profiles	✓	✓	✓	✓
Create and edit custom payload profiles	✓	✓		
Delete custom payload profiles	✓	✓		
Assign IT policies and profiles to users	✓	✓	✓	✓
Assign IT policies and profiles to user groups	✓	✓	✓	✓
Assign IT policies and profiles to device groups	✓	✓	✓	✓
Assign IT policies and profiles to shared device groups	✓	✓		
Assign IT policies and profiles to public device groups	✓	✓		
Rank IT policies and profiles	✓	✓		
View CardDAV profiles	✓	✓	✓	✓

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Create and edit CardDAV profiles	✓	✓		
Delete CardDAV profiles	✓	✓		
View CalDAV profiles	✓	✓	✓	✓
Create and edit CalDAV profiles	✓	✓		
Delete CalDAV profiles	✓	✓		
View AirPrint profiles	✓	✓	✓	✓
Create and edit AirPrint profiles	✓	✓		
Delete AirPrint profiles	✓	✓		
View network usage profiles	✓	✓	✓	✓
Create and edit network usage profiles	✓	✓		
Delete network usage profiles	✓	✓		
View AirPlay profiles	✓	✓	✓	✓
Create and edit AirPlay profiles	✓	✓		
Delete AirPlay profiles	✓	✓		
View Enterprise Management Agent profiles	✓	✓	✓	✓
Create and edit Enterprise Management Agent profiles	✓	✓		
Delete Enterprise Management Agent profiles	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View BlackBerry Dynamics compliance profiles	✓	✓	✓	✓
Delete BlackBerry Dynamics compliance profiles	✓	✓		
View BlackBerry Dynamics profiles	✓	✓	✓	✓
Create and edit BlackBerry Dynamics profiles	✓	✓		
Delete BlackBerry Dynamics profiles	✓	✓		
View BlackBerry Dynamics connectivity profiles	✓	✓	✓	✓
Create and edit BlackBerry Dynamics connectivity profiles	✓	✓		
Delete BlackBerry Dynamics connectivity profiles	✓	✓		
View do not disturb profiles	✓	✓	✓	✓
Create and edit do not disturb profiles	✓	✓		
Delete do not disturb profiles	✓	✓		
View BlackBerry 2FA profiles	✓	✓	✓	✓
Create and edit BlackBerry 2FA profiles	✓	✓		
Delete BlackBerry 2FA profiles	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View Windows Information Protection profiles	✓	✓	✓	✓
Create and edit Windows Information Protection profiles	✓	✓		
Delete Windows Information Protection profiles	✓	✓		
View per-app notification profiles	✓	✓	✓	✓
Create and edit per-app notification profiles	✓	✓		
Delete per-app notification profiles	✓	✓		
View gatekeeping profiles	✓	✓	✓	✓
Create and edit gatekeeping profiles	✓	✓		
Delete gatekeeping profiles	✓	✓		
View Microsoft Intune app protection profiles	✓	✓	✓	✓
Create and edit Microsoft Intune app protection profiles	✓	✓		
Delete Microsoft Intune app protection profiles	✓	✓		
View home screen layout profiles	✓	✓	✓	✓
Create and edit home screen layout profiles	✓	✓		
Delete home screen layout profiles	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View Enterprise Identity authentication policy	✓	✓		
Create and edit Enterprise Identity authentication policy	✓	✓		
Delete Enterprise Identity authentication policy	✓	✓		
Assign Enterprise Identity authentication policy to users and groups	✓	✓		

## Apps

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View apps and app groups	✓	✓	✓	✓
Create and edit apps and app groups	✓	✓		
Delete apps and app groups	✓	✓		
Export app data	✓	✓	✓	✓
Assign apps and app groups to users	✓	✓	✓	✓
Assign apps and app groups to user groups	✓	✓	✓	✓
Assign apps and app groups to device groups	✓	✓	✓	✓
Assign apps and app groups to shared device groups	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Assign apps and app groups to public device groups	✓	✓		
Edit app rating and review settings	✓	✓		
Delete app ratings and reviews	✓	✓	✓	✓
View app installation ranking	✓	✓	✓	✓
Edit app installation ranking	✓	✓		
View app licenses	✓	✓	✓	✓
Create app licenses	✓	✓		
Edit app licenses	✓	✓		
Delete app licenses	✓	✓		
Assign app licenses to apps or app groups	✓	✓	✓	✓

### Restricted apps

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View restricted apps	✓	✓	✓	✓
Create restricted apps	✓	✓		
Delete restricted apps	✓	✓		

### Personal apps

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View personal apps	✓	✓		

## Settings

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View general settings	✓	✓	✓	✓
Edit activation defaults	✓	✓		
Create and edit email templates	✓	✓		
Delete email templates	✓	✓		
Edit console settings	✓	✓		
Edit language for automated emails	✓	✓		
Edit self-service console settings	✓	✓		
Create work space backup and restore settings <sup>1</sup>	✓	✓		
Delete work space backup and restore settings <sup>1</sup>	✓	✓		
Edit default variables <sup>1</sup>	✓	✓		
Edit login notices <sup>1</sup>	✓	✓		
Edit custom variables	✓	✓		
Edit organization notices	✓	✓		
Edit email domains	✓	✓		
Edit location service settings	✓	✓		
Edit customize console settings	✓	✓		
Edit delete command expiration settings	✓	✓		
Edit attestation settings	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Edit certificate settings	✓	✓		
Create and edit event notifications	✓	✓		
Delete event notifications	✓	✓		
Edit device support messages	✓	✓		
Edit certificate-based authentication settings <sup>1</sup>	✓			
Edit public web service access settings	✓			
View app management	✓	✓	✓	✓
Edit BlackBerry World for Work	✓	✓		
Edit internal app storage <sup>1</sup>	✓	✓		
Edit Work Apps for iOS	✓	✓		
Edit Windows 10 apps	✓	✓		
Edit default app rating and review settings	✓	✓		
View external integration settings	✓	✓	✓	✓
Edit Apple Push Notification settings	✓	✓		
Edit SMTP server settings <sup>1</sup>	✓	✓		
Edit Apple DEP settings	✓	✓		
Edit BlackBerry 2FA server settings	✓	✓		



Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Edit BlackBerry Connectivity Node settings <sup>2</sup>	✓	✓		
View One-Time Password tokens	✓	✓	✓	✓
Create and edit One-Time Password tokens	✓	✓		
Edit company directory settings	✓	✓		
Edit Microsoft Intune settings	✓	✓		
Edit Microsoft Exchange gatekeeping settings	✓	✓		
Edit Androidwork profile settings	✓	✓		
Edit certification authority settings	✓	✓		
Edit Samsung Knox bulk enrollment settings	✓	✓		
View trusted certificates	✓	✓		
Add trusted certificates	✓	✓		
Delete trusted certificates	✓	✓		
View BlackBerry Connectivity Node servers	✓	✓		
Create and edit BlackBerry Connectivity Node servers	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Delete BlackBerry Connectivity Node servers	✓	✓		
View BlackBerry Secure Gateway settings	✓	✓		
Edit BlackBerry Secure Gateway settings	✓	✓		
View administrator users and roles	✓	✓	✓	✓
View licensing summary	✓	✓	✓	✓
Edit licensing settings	✓	✓		
View migration settings	✓	✓		
Edit migration settings	✓	✓		
View infrastructure settings	✓	✓	✓	
Edit logging settings <sup>1</sup>	✓	✓		
Edit server-side proxy settings <sup>1</sup>	✓	✓		
View servers <sup>1</sup>	✓	✓		
Edit servers <sup>1</sup>	✓	✓		
Delete servers <sup>1</sup>	✓	✓		
Manage servers <sup>1</sup>	✓	✓		
View audit settings <sup>1</sup>	✓	✓		
Edit audit settings and purge data <sup>1</sup>	✓	✓		
View BlackBerry Secure Connect Plus settings <sup>1</sup>	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Edit BlackBerry Secure Connect Plus settings <sup>1</sup>	✓	✓		
View server certificates <sup>1</sup>	✓	✓		
Update server certificates <sup>1</sup>	✓	✓		
View BlackBerry Control settings	✓	✓	✓	✓
Edit BlackBerry Control settings	✓	✓		
View BlackBerry Dynamics NOC proxy server settings <sup>1</sup>	✓	✓	✓	✓
Edit BlackBerry Dynamics NOC proxy server settings <sup>1</sup>	✓	✓	✓	✓
Edit SNMP settings <sup>1</sup>	✓	✓		
Import IT policy pack and device metadata <sup>1</sup>	✓			
View collaboration service settings <sup>1</sup>	✓	✓	✓	✓
Edit collaboration service settings <sup>1</sup>	✓	✓		
View BlackBerry Dynamics settings	✓	✓	✓	✓
View BlackBerry Dynamics app services	✓	✓		
Edit BlackBerry Dynamics app services	✓			
Create BlackBerry Dynamics app services	✓			
Delete BlackBerry Dynamics app services	✓			

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View BlackBerry Dynamics server properties <sup>1</sup>	✓	✓		
Edit BlackBerry Dynamics server properties <sup>1</sup>	✓			
View BlackBerry Dynamics Direct Connect settings	✓	✓		
Edit BlackBerry Dynamics Direct Connect settings	✓			
View BlackBerry Dynamics server cluster settings <sup>1</sup>	✓	✓		
Edit BlackBerry Dynamics server cluster settings <sup>1</sup>	✓			
View BlackBerry Dynamics reporting	✓	✓	✓	
View BlackBerry Dynamics communication settings <sup>1</sup>	✓	✓	✓	
Edit BlackBerry Dynamics communication settings <sup>1</sup>	✓			
View BEMS Mail settings <sup>2</sup>	✓	✓		
Edit BEMS Mail settings <sup>2</sup>	✓			
View BEMS Docs settings <sup>2</sup>	✓	✓		
Edit BEMS Docs settings <sup>2</sup>	✓			
View Enterprise Identity settings	✓	✓		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View Enterprise Identity Enterprise settings	✓	✓		
Edit Enterprise Identity Enterprise settings	✓	✓		
View Enterprise Identity service settings	✓	✓		
Edit Enterprise Identity service settings	✓	✓		

<sup>1</sup> On-premises environments only

### Dashboard

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View dashboard	✓	✓	✓	✓

### Auditing

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View system audit logs <sup>1</sup>	✓	✓		
View device performance logs <sup>1</sup>	✓	✓		

<sup>1</sup> On-premises environments only

### Workspaces


Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Organization administrator	✓			


Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Helpdesk administrator	✓			
Audit helpdesk administrator	✓			

## Create a custom role


If the preconfigured roles available in BlackBerry UEM do not meet your organization's requirements, you can create custom roles for administrators. You can also create custom roles to restrict administrative tasks to a defined list of user groups. For example, you can create a role for new administrators that restricts their permissions to a user group for training purposes only.

**Before you begin:** You must be a Security Administrator to create a custom role.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Click **Roles**.
4. Click .
5. Type a name and description for the role.
6. To copy permissions from another role, click a role in the **Permissions copied from role** drop-down list.
7. Perform one of the following tasks:

Task	Steps
Allow administrators in this role to search all company directories	a. Select the <b>All company directories</b> option.
Allow administrators in this role to search selected company directories	a. Select the <b>Selected company directories only</b> option. b. Click <b>Select directories</b> . c. Select one or more directories and click  . d. Click <b>Save</b> .

8. Perform one of the following tasks:

Task	Steps
Allow administrators in this role to manage all users and groups	a. Select the <b>All groups and users</b> option.
Allow administrators in this role to manage selected groups	a. Select the <b>Selected groups only</b> option. b. Click <b>Select groups</b> . c. Select one or more groups and click  . d. Click <b>Save</b> .

9. Configure the permissions for administrators in this role.
10. Click **Save**.

**After you finish:** Rank roles.

# Administrative commands for retrieving device information

Query	How to configure	Description
Query the Connectivity status	All users > Managed devices > <device name> tab > Update device information button	Specify how often, in seconds, the device polls for Enterprise Management Agent server commands. The device polls only when the UEM Client is open on the device.
Query the current version of the device firmware/software	All users > Managed devices > <device name> tab > Update device information button.	This command sends and receives updated device information. For example, you can send newly updated IT policy rules or profiles to a device, and receive updated information about a device such as OS version. The device information is also updated every 15 minutes if any information has changed on the device.
Query the current version of the hardware model of the device	All users > Managed devices > <device name> tab > Update device information button.	This command sends and receives updated device information. For example, you can send newly updated IT policy rules or profiles to a device, and receive updated information about a device such as OS version. The device information is also updated every 15 minutes if any information has changed on the device.
Query the current version of installed mobile apps	This is built in. The UEM Client reports this information whenever it changes.	-
Set how often the device keeps audit logs	Policies and profiles > IT policies > Android tab > Enable Audit Logging > Log synchronization frequency	This option specifies how frequently, in hours, the device sends log files to BlackBerry UEM.



# Finding the last time the device contacted BlackBerry UEM

1. In the BlackBerry UEM management console navigate to Users > Managed devices.
2. Click a user's name.
3. Select the device tab for the device that you want to check the contact time for.  
The Last contact time displays in the left hand column.

# Locate the BlackBerry UEM version that you are using

1. Navigate to **Help > About BlackBerry UEM**.
2. The version number displays in the version field.

# 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. Do one of the following:
  - To create a notification for enrollment status, select one of the options under **Enrollment**, such as **Activation failed**.
  - To create a notification for a policy or profile, select one of the options under **Policies and profiles**, such as **Policy or profile delivery failed**.
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**.

# Set the session timeout parameters

1. On the menu bar, click **Settings > General settings > Console**.
2. In the **Session timeout** field, enter, in minutes, the amount of time before the session times out.
3. In the **Session timeout warning** field, enter, in minutes, the amount of time prior to you being logged out, that the session timeout warning displays. For example, if you set this field to two minutes, the warning message will display two minutes before you are logged out of your session.
4. Click **Save**.

# Create a login notice for the consoles

You can create a login notice to display to administrators or users in an on-premises environment when they access the management console or BlackBerry UEM Self-Service. The notice informs administrators or users about the terms and conditions they must accept to use the management console or BlackBerry UEM Self-Service.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **General settings**.
3. Click **Login notices**.
4. Click .
5. Perform any of the following tasks:

Task	Steps
Configure a login notice for the management console	<ol style="list-style-type: none"><li>a. Select the <b>Enable a login notice for the management console</b> check box.</li><li>b. Enter the information that you want to display to administrators when they access the management console.</li></ol>
Configure a login notice for BlackBerry UEM Self-Service	<ol style="list-style-type: none"><li>a. Select the <b>Enable a login notice for the self-service console</b> check box.</li><li>b. Enter the information that you want to display to users when they access BlackBerry UEM Self-Service.</li></ol>

6. Click **Save**.

# Auditing

BlackBerry UEM stores administrator and security audit events that you can use to investigate any administrator actions and interactions between BlackBerry UEM and devices. You can also set up a syslog server for storing both device audit logs and server audit logs. The syslog server must use a valid x509 certificate for the presented Server Certificate in the TLS negotiation. The syslog certificate must be chained to the trust root certificate (CA) which is loaded in the UEM server.

## Viewing audit log data

To view audit logs, refer to your syslog audit records, or you can view server audit records by clicking on the Export button in the Settings > Infrastructure > Audit settings > Security event audit settings section.

## Setup export of server audit records to a syslog server

The syslog server must be using TLS version 1.2, x509 certificates for authentication, and should be using one of the evaluated ciphersuites which are:

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384

1. Upload a syslog CA certificate. Note that there are four separate commands in this step. The commands cannot contain any line breaks.

```
SET BESRoot=C:\Program Files\BlackBerry\UEM
SET KEYSTORE_PATH=<path to CA certificate>
ECHO Running KeyMaster to load Syslog CA Cert with BESRoot: "%BESRoot%"
java -cp "%BESRoot%\tools\lib\*" -Djava.library.path="%BESRoot%\tools\lib\dll
\x64" com.rim.platform.mdm.keymaster.KeyMaster -keystore "%KEYSTORE_PATH%" load
-keystoreType SECURITY_AUDIT_SYSLOG_CACERTS -trusted -BESRoot "%BESRoot%"
```

2. If mutual authentication is configured, upload a client certificate. Note that there are five separate commands in this step. The commands cannot contain any line breaks.

```
SET BESRoot=C:\Program Files\BlackBerry\UEM
SET KEYSTORE_PATH=<path to client certificate>
SET KEYSTORE_PASSWORD=<user defined password>
ECHO Running KeyMaster to load Syslog Client Cert with BESRoot: "%BESRoot%"
java -cp "%BESRoot%\tools\lib\*" -Djava.library.path="%BESRoot%\tools\lib\dll
\x64" com.rim.platform.mdm.keymaster.KeyMaster -keystore "%KEYSTORE_PATH%" -
password "%KEYSTORE_PASSWORD%" load -keystoreType SECURITY_AUDIT_SYSLOG_CLIENT
-BESRoot "%BESRoot%"
```

3. Run the script in [Appendix A](#) against the BlackBerry UEM database. In the script, change the hostname and port number to match your environment, and set mutual authentication, if necessary.

Set the host name and port number, for example:

```
SET @v_hostname = 'localhost';
SET @v_port = '31000';
```

Set whether mutual authentication is enabled:

```
SET @v_use_mutual_auth = 'true';
```

4. Set any syslog specific formatting attributes as described in the script.
5. Execute the script.
6. Restart the BlackBerry UEM Core service.
7. Navigate to **Settings > Infrastructure > Audit Settings** and enable any security audits that you want to track.

## Setup export of device audit records to a syslog server

1. Upload a device audit syslog CA certificate. Note that there are four separate commands in this step. The commands cannot contain any line breaks.

```
SET BESRoot=C:\Program Files\BlackBerry\UEM
SET KEYSTORE_PATH=<path to CA certificate>
ECHO Running KeyMaster to load Device Audit Syslog CA Cert with BESRoot:
"%BESRoot%"
java -cp "%BESRoot%\tools\lib\*" -Djava.library.path="%BESRoot%\tools\lib\dll
\x64" com.rim.platform.mdm.keymaster.KeyMaster -keystore "%KEYSTORE_PATH%" load
-keystoreType DEVICE_AUDITLOG_SYSLOG_CACERTS -trusted -BESRoot "%BESRoot%"
```

2. If mutual authentication is configured, upload a Device Audit Syslog Client Key Pair: Note that there are five separate commands in this step. The commands cannot contain any line breaks.

```
SET BESRoot=C:\Program Files\BlackBerry\UEM
SET KEYSTORE_PATH=<path to device Audit certificate>
SET KEYSTORE_PASSWORD=user defined password
ECHO Running KeyMaster to load Device Audit Syslog CA Cert with BESRoot:
"%BESRoot%"
java -cp "%BESRoot%\tools\lib\*" -Djava.library.path="%BESRoot%\tools\lib\dll
\x64" com.rim.platform.mdm.keymaster.KeyMaster -keystore "%KEYSTORE_PATH%" -
password "%KEYSTORE_PASSWORD%" load -keystoreType DEVICE_AUDITLOG_SYSLOG_CLIENT
-BESRoot "%BESRoot%"
```

3. Run the script in [Appendix B](#) against the BlackBerry UEM database. In the script, change the hostname and port number to match your environment, and set mutual authentication, if necessary.

Set the host name and port number, for example:

```
SET @v_hostname = 'localhost';
SET @v_port = '514';
```

Set whether mutual authentication is enabled:

```
SET @v_use_mutual_auth = 'true';
```

4. Set any syslog specific formatting attributes as described in the script.
5. Execute the script.
6. Restart the BlackBerry UEM Core service.

## Storing audit logs

When an audit event is generated, it is stored in the BlackBerry UEM database. If you have an audit log server set up, UEM sends the records to the audit server every 15 minutes. In the UEM management console, you can configure the number of days that the records are stored in the UEM database (Settings > Infrastructure > Audit settings > Security event audit record retention).

Device audit logs are queued on the device and transferred from the device to the UEM server and then directly to the audit server; the UEM database does not store them.

## 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.

### 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.

1. On the menu bar, click **Settings > Infrastructure > Audit settings**.
2. In the right pane, click the edit icon.
3. To stop auditing a security event, click X beside the event type.
4. To add security events to audit, click + . Select the events and click **Add**.
5. Optionally, if a drop-down list is available in the Setting column beside an event type, choose the condition to log the event.
6. Click **Save**.

### Audit record fields for server audits

The server audit is formatted as a JSON payload with the following attributes.

Name	Description
recordId	Identity of the record that was generated.
date	The UTC date of the event.
eventCategory	The name of the event category.



Name	Description
event	The name of the event.
correlationId	Correlation identifier of the action that can be related to the log entries (this entry might not be present).
host	Name of the host where the event occurred.
username	The username of the user who generated the event. If the system generated the event, then the username will be 'system'.
tenant	The tenant of the user who generated the event. If the system generated the event, then the tenant will remain blank.
isSuccess	Whether the event was a success (true) or a failure (false).
details	The event specific details. You can find the additional searchable content in the details attribute.

### Server Audits - MDM

You can use the additional information column to search the audit records.

Requirement	Auditable events	Event	isSuccess	Additional information
FAU_GEN.1(1)	Audit Generation - Server Start	Server started	TRUE	Component
FAU_GEN.1(1)	Audit Generation - Server Stop	Server stopped	TRUE	Component
FAU_GEN.1(1)	Commands	Command sent	TRUE	Command Type, User Identity, Device Identity  See <a href="#">Administrative commands for retrieving device information</a>
FAU_ALT_EXT.1	Change in enrollment status	Event notification email sent	TRUE	type= Enrollment CompleteEvent
FAU_ALT_EXT.1	Failure to apply policies to a mobile device	Event notification email sent	TRUE	
FAU_SEL.1	Security Audit Event	Security audit settings modified	TRUE	Setting Changes

Requirement	Auditable events	Event	isSuccess	Additional information
FCS_CKM.1	Cryptographic Key Generation	Key generated	FALSE	
FCS_RBG_EXT.1	Extended: Random Bit Generation	Randomization initialized	FALSE	Message Description
FCS_TLSS_EXT.1	TLS Server	TLS Server	FALSE	<a href="#">See TLS Auditing</a>
FIA_ENR_EXT.1	Failure of Mobile Device user authentication	Device Enrollment started	FALSE	Enrollment username; Message Description= BadEnrollment PasswordException
FCS_TLS_EXT	TLS Protocol			<a href="#">See TLS Auditing</a>
FIA_X509_EXT	X.509 Certification Validation			<a href="#">See Certificate audit records</a>
FAU_GEN.1(1)	Administrator action			<a href="#">See Auditing administrator actions</a>
FMT_MOF.1(1)	Issuance of command to perform function	Command sent	TRUE	Command Type, User Identity, Device Identity
FMT_MOF.1(1)	Change of policy settings	Policy sent	TRUE	Policy Description, User Identity
FMT_MOF.1(2)	Enrollment by a user	Device enrollment completed	TRUE	User Identity, Device Identity
FMT_SAE_EXT.1	Enrollment attempted after expiration of authentication data.	Device enrollment started	FALSE	Message Description= Activation password has expired!, Enrollment username

Requirement	Auditable events	Event	isSuccess	Additional information
FMT_SMF.1(2)	Specification of Management Functions - Command Success	Command delivered	TRUE	Command Type, User Identity, Device Identity
FMT_SMF.1(2)	Specification of Management Functions - Command Failure	Command delivered	FALSE	Command Type, User Identity, Device Identity
FMT_SMF.1(2)	Specification of Management Functions - Policy Success	Policy delivered	TRUE	Policy Description, User Identity
FMT_SMF.1(2)	Specification of Management Functions - Policy Failure	Policy delivered	FALSE	Policy Description, User Identity
FPT_ITT.1(2)	Initiation of the trusted channel	Connection with device established	TRUE	Identify of Initiator (Perimeter ID of the Device)
FPT_ITT.1(2)	Termination of the trusted channel	Connection with device terminated	TRUE	Identify of Initiator (Perimeter ID of the Device)
FTP_ITC.1(2)	Initiation of the trusted channel	Connection with device established	TRUE	Identify of Initiator (Perimeter ID of the Device)
FTP_ITC.1(2)	Termination of the trusted channel	Connection with device terminated	TRUE	Identify of Initiator (Perimeter ID of the Device)
FPT_TST_EXT.1	Initiation of self-test.	Self test initiated	TRUE	Component
FPT_TST_EXT.1	Successful completion of self-test	Self test completed	TRUE	Component
FPT_TST_EXT.1	Failure of self-test	Self test completed	FALSE	Message Description, Component
FPT_TST_EXT.1	Failed completion of self-test	Self test completed	FALSE	Message Description, Component
FTA_TAB.1	Change in banner setting	Access banner modified	TRUE	

Requirement	Auditable events	Event	isSuccess	Additional information
FTP_ITC.1(1)	Initiation of Trusted Channel	Connection with external service established	TRUE	Non-TOE Endpoint Name, Non-TOE Endpoint URL,Trusted Channel Protocol
FTP_ITC.1(1)	Termination of Trusted Channel	Connection with external service terminated	TRUE	Non-TOE Endpoint Name, Non-TOE Endpoint URL,Trusted Channel Protocol
FTP_TRP.1(1)	Initiation of Trusted Channel	User logged in	TRUE	Identify of Administrator, Trusted Channel Protocol
FTP_TRP.1(1)	Termination of Trusted Channel	User logged out	TRUE	Identify of Administrator, Trusted Channel Protocol
FTP_TRP.1(2)	Initiation of Trusted Channel	Connection on listening port established	TRUE	Identify of Initiator, Identify of Recipient,Trusted Channel Protocol
FTP_TRP.1(2)	Termination of Trusted Channel	Connection on listening port terminated	TRUE	Identify of Initiator, Identify of Recipient,Trusted Channel Protocol

#### Server Audits - MAS

Requirement	Auditable events	Event	isSuccess	Additional Searchable Content
FAU_GEN.1(2)	MAS Server	Managed application installed	FALSE	

#### TLS auditing

All TLS related failures and audit records containing 'Event = TLS server connection error' or 'TLS client connection error' will be generated. The details of the audit record will contain additional information to determine the cause of the error.

**Note:** TLS failures due to Certificate validation will also have a certificate validation audit record

Table TLS Audit Records
Description:[FATAL Alert:BAD_CERTIFICATE - A corrupt or unuseable certificate was received. \njava.security.cert.CertificateParsingException: ASN.1: Unexpected ASN.1 tag]
Description:[FATAL Alert:BAD_CERTIFICATE - A corrupt or unuseable certificate was received. \njava.security.cert.CertificateParsingException: PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.3]
Description:[FATAL Alert:BAD_CERTIFICATE - A corrupt or unuseable certificate was received.\nTLSState: Key Exchange Alert.]
Description:[FATAL Alert:BAD_RECORD_MAC - A record was received with an incorrect MAC.\nDecrypting Message Failed. -Invalid content length.]
Description:[FATAL Alert:BAD_RECORD_MAC - A record was received with an incorrect MAC.\nDecrypting Message Failed. -MAC verify failed.]
Description:[FATAL Alert:DECRYPT_ERROR - A cryptographic operation failed.\nHandshake Verification Failed. -Verify Data does not match.]
Description:[FATAL Alert:DECRYPT_ERROR - A cryptographic operation failed.\nTLSState: Key Exchange Alert.]
Description:[FATAL Alert:HANDSHAKE_FAILURE - The handshake handler was unable to negotiate an acceptable set of security parameters.\nClientState: No Cipher Suite Available.]
Description:[FATAL Alert:HANDSHAKE_FAILURE - The handshake handler was unable to negotiate an acceptable set of security parameters.\nNone of client suites is enabled on server or ECC ciphersuite curve and/or pointformat does not match.]
Description:[FATAL Alert:HANDSHAKE_FAILURE - The handshake handler was unable to negotiate an acceptable set of security parameters.\nTLSState: Key Exchange Alert.]
Description:[FATAL Alert:HANDSHAKE_FAILURE - The handshake handler was unable to negotiate an acceptable set of security parameters.\nTLSState: Non Key Exchange Alert. - com.certicom.tls.record.handshake.ke.KeException: Could not verify client's certificate]
Description:[FATAL Alert:PROTOCOL_VERSION - The protocol version requested is recognized but not supported.\nServerState: No protocol agreed upon.]
Description:[FATAL Alert:UNEXPECTED_MESSAGE - A message out of sequence was received.\nThe fragment was of an unknown type. -java.lang.IllegalArgumentException: Handshake message is too long. Allowed max length is 65535]
Description:[FATAL Alert:UNEXPECTED_MESSAGE - A message out of sequence was received.\nThe fragment was of an unknown type. -java.lang.IllegalArgumentException: Unsupported Protocol Version]

## Certificate audit records

The following table shows the x509 validation related failures and audit records that contain an **Event = Certificate validated** or an **Event = Presented identifier verification** message. The details of the audit record contain additional information to help determine the cause of the error.

Messages
msg{CA certificate has invalid basicConstraints.isCA=false}
msg{certificate does not contain BasicConstraints extension}
msg{certificate does not contain required extended KeyUsage:[CLIENT_AUTHENTICATION]}
msg{certificate does not contain required extended KeyUsage:[SERVER_AUTHENTICATION]}
msg{Certificate has been revoked. reason:{PRIVILEGE_WITHDRAWN}}
msg{Certificate has been revoked. reason:{UNSPECIFIED}}
msg{Path does not chain with any of the trust anchors}
msg{Responder's certificate is not authorized to sign OCSP responses}
msg{Responder's certificate not valid for signing OCSP responses}
msg{Response is unreliable: its validity interval is out-of-date}
msg{signature check failed}
msg{Unable to determine revocation status due to network error}
msg{Unable to verify OCSP Response's signature}
msg{validity check failed}
Message Description={Certificate for <tlv-16x.example.com> doesn't match common name of the certificate subject}
Message Description={Certificate for <tlv-16x.example.com> doesn't match any of the subject alternative names}

### Auditing administrator actions

The following is an example of an administrator action audit record, with the Type, Group, Group Identity, and User Identity highlighted. In the audit record:

- Event = "Administrator action"
- Username = *<name>* - defines which user performed the administrative action

Administrator action	Sample audit
Add users to group	{ <code>"recordId":161701,"date":"2020-03-07T14:46:52.186-05:00","eventCategory": "Administration","event":"Administrator action"," correlationId": f4ce5c5d-02da-458d-9849-b1457a5e192b","host":"CI0700000003373.rim.net", "username":"admin","tenant":"BCOP1151","isSuccess":true," details": "Type=group;Action=added;Group GUID=f56e86b8-ef51-4a7b-86e0-bafca5c1b399; <b>Group Identity</b>=All users;User GUID=b82194ca-f73f-4460-9a9d-1c16982fb1c1;<b>User Identity</b>=user2"</code> }

The following table lists the administrator actions and the information to look for in the audit records.

Auditable event	Type	Action	Additional information
Add Users to Group	group	added	Group Identity;User Identity
Assign App Definition to Group	application	assigned	App Name;App Version.;Group Identity
Assign App Definition to User	application	assigned	App Name, User Identity
Assign Policy to Group	policy	assigned	Policy Name, Group Identity
Assign Policy to User	policy	assigned	Policy Name, User Identity
Create App Definition	application	created	App Name, App Version
Create Directory	directory	created	Directory Name, Directory Type
Create Policy	policy	created	Policy Name
Delete App Definition	application	deleted	App Id
Delete Directory	directory	deleted	Directory Name, Directory Type
Delete Policy	policy	deleted	Policy Name
Device Action	device	device action	User Identity, Device Action
Group Created	group	created	Group Identity

<b>Auditable event</b>	<b>Type</b>	<b>Action</b>	<b>Additional information</b>
Group Deleted	group	deleted	Group Identity
Group Updated	group	updated	Group Identity
Removed Users from Group	group	removed	User Identity
Set User Activation Password	user	set activation password	User Identity
Unassign App Definition to Group	application	unassigned	App Name, App Version, Group Identity
Unassign App Definition to User	application	unassigned	App Name, App Version, User Identity
Unassign Policy from Group	policy	unassigned	Policy Name, Group Identity
Unassign Policy from User	policy	unassigned	Policy Name, User Identity
Update App Definition	application	updated	App Name, App Version
Update Directory	directory	updated	Directory Name, Directory Type
Update Policy	policy	updated	Policy Name
User Created	user	created	User Identity
User Deleted	user	updated	User Identity
User Updated	user	updated	User Identity
Create Role	role	created	Role Name, Is Admin Role
Update Role	role	updated	Role Name, Is Admin Role
Delete Role	role	deleted	Role Name, Is Admin Role
Assign Role to User	role	assigned	Role Name, Is Admin Role, User Identity
Unassign Role from User	role	unassigned	Role Name, Is Admin Role, User Identity



Auditable event	Type	Action	Additional information
Assign Role to Group	role	assigned	Role Name, Is Admin Role, Group Identity
Unassign Role from Group	role	unassigned	Role Name, Is Admin Role, Group Identity

## Deployer audit records

Each time you run the Extractor.exe file, an audit record is created. The record is stored in the directory location where you ran the file.

Result	Information to search for
Extractor ran successfully	Signature validation for manifest files succeeded
Extractor failed	Signature validation failed for file

## Device audit information

### Enable audit record collection for Samsung Knox devices

1. In the IT policy for your Samsung Knox devices, in the **Global (Samsung Knox devices only)** section, click **Enable audit logging**.
2. Select the options that you want to enable logging for, such as **Enable iptables logging**.
3. Click **Save**.

### Audit collection filter settings for devices

When you configure audit collection, you can use IT policies to filter the events for devices.

IT policy	Options	Description
Audit log severity level	Alert, Critical, Error, Warning, Notice	Specifies the minimum severity level to log. Everything with the specified option and lower will be logged. For example, if you select Error, then Warning messages will also be logged.  To use Notice, you have to use the Enable verbose logging command for an individual device.
Audit log outcomes	Fail Success All	Specifies filtering based on the outcomes of each event
Log security group module events in audit log	on/off	Specify whether to include events for the security group module in the audit log.
Log system group module events in audit log	on/off	Specify whether to include events for the system group module in the audit log.

IT policy	Options	Description
Log network group module events in audit log	on/off	Specify whether to include events for the network group module in the audit log.
Log events group module events in audit log	on/off	Specify whether to include events for the events group module in the audit log.
Log application group module events in audit log	on/off	Specify whether to include events for the application group module in the audit log.
Enable audit logging (deselects all of the group module options above)	on/off	Specify if logging is enabled.
Enable kernel audit logs	on/off	Specify whether Kernel logging is enabled.
Enable iptables logging	on/off	Specify whether iptables logging is enabled.

### Audit record fields for devices

The audit records have 12 fields.

Item	Description
Event time	Long value that represents the UTC event time
Severity	Integer value representing the severity: 1 (alert), 2 (critical), 3 (error), 4 (warning), 5 (notice)
Group	Integer value representing the group code: 1 (security), 2 (system), 3 (network), 4 (events), 5 (application)
Outcome	Integer value representing the outcome of the event: 1 (success), 0 (failure)
PID	Integer value representing the process ID
USERID	Integer value representing the USERID for which the log was originated <ul style="list-style-type: none"> <li>ID 0 is for a normal user</li> <li>ID -1 is for system events</li> <li>ID 100-102 is for Workspace users (multiple Workspaces can be defined)</li> </ul>
Subject Identity	String representing the facility/Software Component name
Reason	Free-form message description of the event (generally a human-readable message)
Name.ID	Name of the BlackBerry UEM user enrolled on the device
version	Log format version

Item	Description
UUID	Internal unique device ID from the UEM server. To find the UUID, in the UEM management console, navigate to Users > Managed devices > <user name> > <device name> tab > View device report command.
groupID	Name of the process space that generated the audit events.

## Searching audit logs for successes and failures

The following table provides search terms that you can use to look for successes and failures of events. For additional guidance on device audit logs, refer to the Samsung documentation.

Requirement	Auditable events	Event types/Reason	Severity	Group	Outcome	
MDMA10: FAU_ALT_EXT.2	Success of sending policy change	Reason=IT policy <IT policy profile name> is applied	1	5	1	
	Reachability	Reason=Reaching out to server for commands	1	5	1	
	Failed App Install		Reason=Application <Application Version Id> fails to install or upgrade	1	5	0
			Reason=Hosted application installation for device owner : <App Package Name>	1	5	0
			Reason=Hosted application installation for profile owner : <App Package Name>	1	5	0
	Failure of policy change	Reason=Failed to apply IT policy	1	5	0	
MDMA10: FAU_GEN.1(2)	Startup of the agent	Reason=Startup of the MDM Agent	1	5	1	
	Shutdown of the agent	Reason=Android will be shutdown	5	2	1	
	MDM policy updated	Reason=IT policy <IT policy profile name> is re-applied	1	5	1	

MDMA10: FAU_SEL.1(2)	All modifications to the audit configuration that occur while the audit collection functions are operating.	Reason=disableAuditLog n:<Container/Personal>	1	4	1
		Reason=disableIPTablesLogging n:<Container/Personal>	1	4	1
		Reason=enableAuditLog n:<Container/Personal>	1	4	1
		Reason=enableIPTablesLogging n:<Container/Personal>	1	4	1
		Reason=setAuditLogRules n:<Container/Personal> Rules :AuditLogRulesInfo: KernelLogsEnabled = <true/ false>, OutcomeRule = <0/1/2>, SeverityRule = <1/2/3/4/5>, GroupsRule = [<Selection of 1, 2, 3, 4, 5>]	1	4	1
MDMA10: FIA_ENR_EXT.2	Enrollment in management	Reason=Reference identifier of MDM server <tenantID> during enrollment is: <BCP>	1	5	1
		Reason=Enrollment is successful			
MDMA10: FMT_POL_EXT.2	Failure of policy validation.	Reason=Payload rejected: <error>	1	5	0
MDMA10: FMT_SMF_EXT.4	Outcome (Success/failure) of function.	Reason=Enrollment is successful	1	5	1
		Reason=Processed X.509v3 certificates into the Trust Anchor Database	1	5	1
		Reason=MaConfig applied to MaConfigProfile	1	5	1

MDMPP40: FPT_ITT.1(2)	Initiation of the trusted channel between the Agent and UEM Server	Reason=Communication session established to [ <i>&lt;tenantID&gt;</i> ] via <i>&lt;protocol&gt;</i> : [ <i>&lt;proxy host&gt;</i> : <i>&lt;proxy port&gt;</i> ]	5	5	1
	Termination of the trusted channel between the Agent and UEM Server	Reason=Communication session disconnected from [ <i>&lt;tenantID&gt;</i> ] via <i>&lt;protocol&gt;</i> : [ <i>&lt;proxy host&gt;</i> : <i>&lt;proxy port&gt;</i> ]	5	5	1

# Appendix A

```
-- NIAP Script to enable Security Audit Export to Syslog
DECLARE @v_hostname NVARCHAR(2000)
        , @v_port NVARCHAR(2000)
        , @v_use_mutual_auth NVARCHAR(2000)
        , @v_facility NVARCHAR(2000)
        , @v_severity NVARCHAR(2000)
        , @v_use_rfc5424 NVARCHAR(2000)
        , @v_eom_marker NVARCHAR(2000)
        , @v_use_octect_counting NVARCHAR(2000)

-- Syslog Endpoint Settings (Required to be replaced)
SET @v_hostname = <FQDN of your syslog server>;
SET @v_port = <enter port number of your local syslog server>;

-- Whether to use mutual authentication
SET @v_use_mutual_auth = 'false';

-- The next set of variables are optional but configure the format of the syslog
-- message.
-- These settings only need to be changed if necessary.

-- The default Syslog format for security audits is in the following format:
-- <priority>yyyy-MM-dd'T'HH:mm:ssXXX hostname appname description

-- The priority is facility * 8 + severity
SET @v_facility = '13';
SET @v_severity = '5';

-- use RFC5424, 'true' or 'false' as to whether use the rfc5424 formatting
SET @v_use_rfc5424 = 'false';

-- The next group of settings configure how to differentiate between the syslog
-- messages over a TCP connection as denoted in rfc6587

-- octect counting prepends the length of the syslog message to message, so it
-- will be sent in the form <message length> <message>
SET @v_use_octect_counting = 'false';

-- end of message marker, is a comma separated list of byte values to be append
-- to the message. This setting only applies if
-- octect counting is disabled. If no bytes are required to be appended to the
-- end of the message '' (empty string) is a valid value.
SET @v_eom_marker = '10';

-- DO NOT MODIFY (Below)

-- Set the feature
EXEC dbo.setGlobalCfgSettingValue 0, 'feature.security.event.auditing.syslog',
    NULL, 'true';

-- Server Settings
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.security.event.auditing.syslog.enabled',
    NULL, 'true';
EXEC dbo.setGlobalCfgSettingValue 0,
    'mdm.security.event.auditing.syslog.transport', NULL, 'TCP';
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.security.event.auditing.syslog.use.tls',
    NULL, 'true';
```

```

EXEC dbo.setGlobalCfgSettingValue 0,
  'mdm.security.event.auditing.syslog.use.niap.compliance', NULL, 'true';
EXEC dbo.setGlobalCfgSettingValue 0,
  'mdm.security.event.auditing.syslog.use.mutual.auth', NULL, @v_use_mutual_auth;

-- High Water Mark
DECLARE @v_lastaudit VARCHAR(16);
SET @v_lastaudit = (SELECT TOP 1 CAST(id_security_audit AS VARCHAR(16)) FROM
  obj_security_audit ORDER BY id_security_audit DESC);
EXEC dbo.setGlobalCfgSettingValue 0,
  'mdm.security.event.auditing.syslog.last.sent.record.id', NULL, @v_lastaudit;

-- Endpoint Settings
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.security.event.auditing.syslog.host',
  NULL, @v_hostname;
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.security.event.auditing.syslog.port',
  NULL, @v_port;

-- Syslog settings
EXEC dbo.setGlobalCfgSettingValue 0,
  'mdm.security.event.auditing.syslog.facility', NULL, @v_facility;
EXEC dbo.setGlobalCfgSettingValue 0,
  'mdm.security.event.auditing.syslog.severity', NULL, @v_severity;
EXEC dbo.setGlobalCfgSettingValue 0,
  'mdm.security.event.auditing.syslog.use.rfc5424', NULL, @v_use_rfc5424;

-- Syslog TCP Settings
EXEC dbo.setGlobalCfgSettingValue 0,
  'mdm.security.event.auditing.syslog.use.octect.counting', NULL,
  @v_use_octect_counting;
EXEC dbo.setGlobalCfgSettingValue 0,
  'mdm.security.event.auditing.syslog.eom.marker', NULL, @v_eom_marker;

```

# Appendix B

```
-- NIAP Script to enable Device Audit Export to Syslog
DECLARE @v_hostname NVARCHAR(2000)
, @v_port NVARCHAR(2000)
, @v_use_mutual_auth NVARCHAR(2000)
, @v_facility NVARCHAR(2000)
, @v_severity NVARCHAR(2000)
, @v_use_rfc5424 NVARCHAR(2000)
, @v_eom_marker NVARCHAR(2000)
, @v_use_octect_counting NVARCHAR(2000)

-- Syslog Endpoint Settings (Required to be replaced)
SET @v_hostname = <FQDN of your syslog server>;
SET @v_port = <enter port number of your local syslog server>;

-- Whether to use mutual authentication
SET @v_use_mutual_auth = 'false';

-- The next set of variables are optional but configure the format of the syslog
-- message.
-- These settings only need to be changed if necessary.
-- The default Syslog format for device audits is in the following format:
-- <priority> yyyy-MM-dd'T'HH:mm:ssXXX hostname appname description
-- The priority is facility * 8 + severity
SET @v_facility = '13';
SET @v_severity = '5';

-- use RFC5424, 'true' or 'false' as to whether use the rfc5424 formatting
SET @v_use_rfc5424 = 'false';

-- The next group of settings configure how to differentiate between the syslog
-- messages over a TCP connection as denoted in rfc6587
-- octect counting prepends the length of the syslog message to message, so it
-- will be sent in the form <message length> <message>
SET @v_use_octect_counting = 'false';

-- end of message marker, is a comma separated list of byte values to be append
-- to the message. This setting only applies if octect counting is disabled.
-- If no bytes are required to be appended to the end of the message ''
-- (empty string) is a valid value.
SET @v_eom_marker = '10';

-- DO NOT MODIFY (Below)
-- Server Settings
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.writer', NULL, 'SYSLOG';
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.syslog.transport', NULL,
'TCP';
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.syslog.use.tls', NULL,
'true';
EXEC dbo.setGlobalCfgSettingValue 0,
'mdm.device.auditlog.syslog.use.niap.compliance', NULL, 'true';
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.syslog.use.mutual.auth',
NULL, @v_use_mutual_auth;

-- Endpoint Settings
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.syslog.host', NULL,
@v_hostname
```



```
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.syslog.port', NULL,
    @v_port;

-- Syslog settings

EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.syslog.facility', NULL,
    @v_facility;
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.syslog.severity', NULL,
    @v_severity;
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.syslog.use.rfc5424',
    NULL, @v_use_rfc5424;

-- Syslog TCP Settings
EXEC dbo.setGlobalCfgSettingValue 0,
    'mdm.device.auditlog.syslog.use.octet.counting', NULL, @v_use_octect_counting;
EXEC dbo.setGlobalCfgSettingValue 0, 'mdm.device.auditlog.syslog.eom.marker',
    NULL, @v_eom_marker;
```

# Legal notice

©2020 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

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