BlackBerry UEM

Using the management console

Administration

12.17

Contents

Using the BlackBerry UEM management console

Administrators use the BlackBerry UEM management console to manage devices and users for BlackBerry UEM and other BlackBerry enterprise software products. Administrators are users that are assigned an administrative role by user group or user account. The actions that administrators can perform are defined in the role that is assigned to them. A Security Administrator can assign each additional administrator a preconfigured role or a custom role. Each role has a set of permissions that specifies the information that administrators can view and the actions that they can perform in the BlackBerry UEM management console.

Roles help your organization to do the following:

- Reduce security risks associated with allowing all administrators to access all administrative options
- Define different types of administrators to better distribute job responsibilities
- Increase efficiency for administrators by limiting accessible options to their job responsibilities

Steps to set up UEM administration

When you set up the management console for UEM administration, you perform the following actions:

Step	Action
1	Configure console login settings for administrators and users.
2	If you have installed UEM in an on-premises environment, if desired, create a login notice for the consoles.
3	If desired, customize the color of the consoles and customize the login page and menu bar.
4	If desired, create bookmarks in the consoles.
5	If desired, change the language for automated email messages.
6	Review preconfigured roles and, if necessary, create a custom role.
7	Rank roles.
8	Create an administrator.

Setting console login options

You can specify how administrators and users authenticate with the BlackBerry UEM consoles and the login notices that appear after users and administrators log in.

You can allow administrators and users to log in using the following authentication methods:

Authentication option	Description
Single sign-on	If you connect BlackBerry UEM to Microsoft Active Directory in an on-premises environment, you can configure single sign-on authentication to permit administrators or users to bypass the login webpage and access the management console or BlackBerry UEM Self-Service directly. If single sign-on is enabled, BlackBerry UEM does not request a password or certificate to log in. This feature is not supported by BlackBerry UEM Cloud.
Directory-based authentication	If you connect BlackBerry UEM to your company directory, administrators and users can log in using their directory credentials. For more information, see the on-premises configuration content or the Cloud configuration content
Local password-based authentication	Local administrators and users can authenticate with a username and password.
Certificate-based authentication	You can set up certificate-based authentication so that administrators and users can log in using an authentication certificate. This feature is not supported by BlackBerry UEM Cloud.
BlackBerry 2FA authentication	You can set up BlackBerry 2FA authentication so that administrators and users can log in using two-factor authentication. For more information, visit support.blackberry.com/community to read article 73371. This feature is not supported in an on-premises environment.
BlackBerry Online Account authentication	You can set up BlackBerry Online Account authentication so that administrators can log in using their BlackBerry Online Account credentials. This feature is not supported in an on-premises environment.

You can also create a login notice for the consoles and set session timeout parameters.

Set the minimum password complexity for local administrators

You can set the minimum password length and complexity requirements for local administrator accounts. This setting takes effect when administrators change their account password.

1. On the menu bar, click **Settings** > **General settings** > **Console**.
2. In the **Minimum number of characters** field, enter the minimum number of characters that a console password must have.
3. In the **Minimum password complexity** field, select the minimum complexity for a console password:

- **No restriction**
- **1 letter, 1 number**
- **1 letter, 1 number, 1 special character**
- **1 uppercase letter and lowercase letter, 1 number, 1 special character**

4. Click **Save**.

Configure certificate-based console authentication

You can set up certificate-based authentication in an on-premises envorinment so that administrators and users can log in using an authentication certificate. BlackBerry UEM verifies certificates against the issuer, verifies that the certificate is valid using the certificate OCSP or CRL settings, and verifies that the certificate matches a user in the BlackBerry UEM database.

This feature is not supported by BlackBerry UEM Cloud.

Before you begin: Obtain copies of the CA certificates that issue your administrators' and users' client certificates in .cer or .der format.

1. On the menu bar, click **Settings** > **General settings** > **Certificate-based console authentication**.
2. Select **Enable certificate-based authentication**.
3. Click **Browse** and navigate to the location where you saved the CA certificate files. Select a file and click **Open** to upload the certificate to BlackBerry UEM.

   BlackBerry UEM trusts all certificates issued by that CA. Repeat this step to upload additional certificates.
4. Select **Check for user principal name for SAN** to require BlackBerry UEM to verify that the user principal name in the certificate matches a user in the BlackBerry UEM database.

   If the user principal name in the certificate matches a known user, BlackBerry UEM grants access according to the user's permissions.
5. Select **Check for email address** to require BlackBerry UEM to verify that the user email address in the certificate matches a user email address in the BlackBerry UEM database.

   If the user email address in the certificate matches a known user, BlackBerry UEM grants access according to the user's permissions. If you select both **Check for user principal name for SAN** and **Check for email address**, BlackBerry UEM checks the principal name before the email address and grants access if the principal name matches. If neither check finds a match between the certificate and a known user, BlackBerry UEM denies access.
6. Click **Save**.

After you finish: If users access BlackBerry UEM using Mozilla Firefox, the user must add their client certificate to the Firefox certificate store to authenticate with BlackBerry UEM using certificate-based authentication.

Configuring single sign-on for BlackBerry UEM

If you connect BlackBerry UEM to Microsoft Active Directory, you can configure single sign-on authentication to permit administrators or users to bypass the login webpage and access the management console or BlackBerry UEM Self-Service directly. When administrators or users log in to Windows, the browser uses their credentials to authenticate them with BlackBerry UEM automatically. Windows login information can include Microsoft Active Directory credentials or derived credentials (for example, from CAC readers or digital tokens).

Before you enable single sign-on to BlackBerry UEM for a Microsoft Active Directory connection, you must configure constrained delegation for the Microsoft Active Directory account that BlackBerry UEM uses for the directory connection.

Note: If you enable single sign-on, any changes that you make to the Microsoft Active Directory account will require that you restart the BlackBerry UEM services on each computer that hosts a BlackBerry UEM instance. Administrators and users must log out from their computers and log in again to use single sign-on for BlackBerry UEM.

When you configure single sign-on for BlackBerry UEM, you perform the following actions:

Step	Action
1	Configure constrained delegation for the Microsoft Active Directory account to support single sign-on.
2	Enable single sign-on for a Microsoft Active Directory connection.
3	Verify browser requirements for single sign-on.

Configure constrained delegation for the Microsoft Active Directory account to support single sign-on

To support single sign-on for BlackBerry UEM, you must configure constrained delegation for the Microsoft Active Directory account that BlackBerry UEM uses for the directory connection. Constrained delegation allows browsers to authenticate with BlackBerry UEM on behalf of administrators or users when they access the management console or BlackBerry UEM Self-Service.

1. Use the Windows Server ADSI Edit tool or setspn command-line tool to add the following SPNs for BlackBerry UEM to the Microsoft Active Directory account:
   - HTTP/*<host_FQDN_or_pool_name>* (for example, HTTP/domain123.example.com)
   - BASPLUGIN111/*<host_FQDN_or_pool_name>* (for example, BASPLUGIN111/domain123.example.com)

   If you configured high availability for the management consoles in a BlackBerry UEM domain, specify the pool name. Otherwise, specify the FQDN of the computer that hosts the management console.

   Note: Verify that no other accounts in the Microsoft Active Directory forest have the same SPNs.
2. Open Microsoft Active Directory Users and Computers.
3. In the Microsoft Active Directory account properties, on the **Delegation** tab, select the following options:
   - Trust this user for delegation to specified services only
   - Use Kerberos only
4. Add the SPNs from step 1 to the list of services.

Configure single sign-on for BlackBerry UEM

When you configure single sign-on for administrators and users logging in to BlackBerry UEM, you configure it for the management console and BlackBerry UEM Self-Service.

Before you begin:

- Configure constrained delegation for the Microsoft Active Directory account that BlackBerry UEM uses for the directory connection.
- If you enable single sign-on for multiple Microsoft Active Directory connections, verify that there are no trust relationships between the Microsoft Active Directory forests.

1. On the menu bar, click **Settings > External integration > Company directory**.
2. In the **Configured directory connections** section, click the name of a Microsoft Active Directory connection.

3. On the **Authentication** tab, select the **Enable Windows single sign-on** check box.
4. Click **Save**.
5. Click **Save**.
   BlackBerry UEM validates the information for Microsoft Active Directory authentication. If the information is invalid, BlackBerry UEM prompts you to specify the correct information.
6. Click **Close**.

After you finish:

- Restart the BlackBerry UEM services on each computer that hosts a BlackBerry UEM instance.
- Instruct administrators and BlackBerry UEM Self-Service users to configure their browsers to support single sign-on for BlackBerry UEM.

Console URLs for single sign-on

If you configure single sign-on for BlackBerry UEM, you must instruct administrators to access the management console and users to access BlackBerry UEM Self-Service using the following URLs:

Console	URL for single sign-on authentication
BlackBerry UEM management console	https://<*host_FQDN_or_pool_name*>:<*port*>/admin
BlackBerry UEM Self-Service	https://<*host_FQDN_or_pool_name*>:<*port*>/mydevice

Single sign-on authentication takes precedence over other authentication methods that permit administrators to log in to the management console and users to log in to BlackBerry UEM Self-Service. If your organization's security standards require that administrators or users use another authentication method, you must instruct them to access the management console or BlackBerry UEM Self-Service using the following URLs:

Console	URL for other authentication methods
BlackBerry UEM management console	https://<*host_FQDN_or_pool_name*>:<*port*>/admin?sso=n
BlackBerry UEM Self-Service	https://<*host_FQDN_or_pool_name*>:<*port*>/mydevice?sso=n

Note:

To confirm the ports that are assigned to BlackBerry UEM Self-Service and the management console, see the Installation and Upgrade content.

To learn more about BlackBerry listening ports, see the Planning content.

Browser requirements: Single sign-on

If you configure single sign-on for BlackBerry UEM, the following requirements apply to the browsers used by administrators and BlackBerry UEM Self-Service users.

Item	Requirement
Browser	Any of the following: • Internet Explorer • Microsoft Edge • Mozilla Firefox • Google Chrome For more information about supported versions, see the Compatibility matrix.
Browser settings	Internet Explorer with the following settings: • The management console and BlackBerry UEM Self-Service URLs are assigned to the local intranet zone (Internet Options > Security). • Enable Integrated Windows Authentication is selected (Internet Options > Advanced). Firefox with the following settings: • In the about:config list, https://, *<host_FQDN_or_pool_name>* is added to the "network.negotiate-auth.trusted-uris" preference. For more information, visit kb.mozillazine.org/about:config. Google Chrome uses the local intranet zone settings from Internet Explorer. The management console and BlackBerry UEM Self-Service URLs must be assigned to the local intranet zone (Internet Options > Security).

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.

This feature is not supported by BlackBerry UEM Cloud

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	a. Select the **Enable a login notice for the management console** check box. b. Enter the information that you want to display to administrators when they access the management console.
Configure a login notice for BlackBerry UEM Self-Service	a. Select the **Enable a login notice for the self-service console** check box. b. Enter the information that you want to display to users when they access BlackBerry UEM Self-Service.

6. 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**.

Log in to BlackBerry UEM

The management console allows you to perform administrative tasks for devices in your organization that are managed by BlackBerry UEM.

Before you begin:

- Locate the web address and login information for the management console. You can find the information in the inbox of the email account that is associated with your BlackBerry UEM account.
  - In an on-premises environment, the web address should be in the format https://<*hostname*>/admin/index.jsp
  - In a BlackBerry UEM Cloud environment, the web address should be in the format https://<*hostname*>/admin/index.jsp?tenant=<*tenant SRP number*>
- If you are using Microsoft Active Directory authentication, you must know the Microsoft Active Directory domain.

1. In the browser, type the web address for the BlackBerry UEM management console of your organization.
2. In the **Username** field, type your username.
3. In the **Password** field, type your password.
4. If necessary, in the **Sign in using** drop-down list, do one of the following:
   - Click **Direct authentication**.
   - Click **LDAP authentication**.
   - Click **Microsoft Active Directory authentication**. In the **Domain** field, type the Microsoft Active Directory domain.
5. Click **Sign in**.

   On first login to BlackBerry UEM Cloud, and following any updates to legal agreements, you are presented with separate EULAs for the BlackBerry SLA, BlackBerry UEM Cloud, and BlackBerry Workspaces (if applicable).

After you finish: You can change your login password by clicking the user icon in the top-right corner of the management console.

Customizing the appearance of the consoles

You can customize the appearance of the consoles by selecting a customized color scheme and by changing the text and images on the log in screen and the image on the menu bar. The colors, images, and text that you select are used in both the management console and the BlackBerry UEM Self-Service console.

Customize the color of the consoles

You can select a customized color scheme for the consoles. The colors that you select are used in both the management console and the BlackBerry UEM Self-Service console.

1. On the menu bar, click **Settings > General settings**.
2. Click **Customize console**.
3. Select two colors for the console. Perform one of the following actions:
   - Click the box to the left of the color code and select a color from the color palette.
   - Type hexadecimal color codes in the selection fields.
   - Select a color from the sample color boxes to the right of the color code.

   A preview of the color scheme displays on the page.
4. Click **Save**.

After you finish: Log out and log in again to see the updated color scheme.

Create website bookmarks in the consoles

You can create website bookmarks in the BlackBerry UEM management console and the BlackBerry UEM Self-Service console. You can create different bookmarks for each console. For example, you might create a bookmark in BlackBerry UEM Self-Service that links to customized help files for users' devices.

Before you begin: You must be a Security Administrator to create or edit bookmarks in the consoles.

1. Log in to BlackBerry UEM or BlackBerry UEM Self-Service.
2. In the upper-right corner, click ★▾.
3. Under **Add web address**, add bookmark information:
   a) Enter a name for the bookmark.
   b) Enter the URL for the website. The URL must begin with "http://" or "https://".
4. Click **Save**.

After you finish: Click ★▾ to view your bookmarks. All users can access the bookmarks, but you must be a Security Administrator to create or edit bookmarks.

Change the language for automated email messages

In the management console, you can change the language for automated email messages. BlackBerry UEM uses the language that you specify in email messages that you cannot edit (for example, notifications about administrator access and console passwords).

1. On the menu bar, click **Settings**.
2. In the left pane, expand **General settings**.
3. Click **Language**.
4. In the drop-down list, click the language that you want to use in automated email messages from BlackBerry UEM.
5. Click **Save**.

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.

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

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	
Set BlackBerry 2FA preauthentication	√	√		
Manage devices	√	√	√	√
Enable work space	√	√	√	√
Disable work space	√	√	√	√

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	√
Turn off Lost Mode	√	√	√	√
Locate device	√	√	√	√
Check in device	√	√	√	
Restart device	√	√	√	√

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	√
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	√	√		
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	√	√	√	√
Create and edit device SR requirements profiles	√	√		
Delete device SR requirements profiles	√	√		
View activation profiles	√	√	√	√
Create and edit activation profiles	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		
Delete proxy profiles	√	√		
View web content filter profiles	√	√	√	√
Create and edit web content filter profiles	√	√		
Delete web content filter profiles	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	√
Create and edit CA certificate profiles	√	√		
Delete CA certificate profiles	√	√		
View shared certificate profiles	√	√	√	√
Create and edit shared certificate profiles	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	√
Create and edit managed domains profiles	√	√		
Delete managed domains profiles	√	√		
View user credential profiles	√	√	√	√
Create and edit user credential profiles	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	√
Create and edit CardDAV profiles	√	√		
Delete CardDAV profiles	√	√		
View CalDAV profiles	√	√	√	√
Create and edit CalDAV profiles	√	√		
Delete CalDAV profiles	√	√		
View AirPrint profiles	√	√	√	√

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		
View BlackBerry Dynamics compliance profiles	√	√	√	√
Delete BlackBerry Dynamics compliance profiles	√	√		
View BlackBerry Dynamics profiles	√	√	√	√
Create and edit BlackBerry Dynamics profiles	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		
View Windows Informati Protection profiles	√	√	√	√
Create and edit Windows Information Protection profiles	√	√		
Delete Windows Informa Protection profiles	√	√		
View per-app notification profiles	√	√	√	√

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		
View Enterprise Identity authentication policy	√	√		
Create and edit Enterprise Identity authentication policy	√	√		
Delete Enterprise Identity authentication policy	√	√		

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

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Edit console settings	√	√		
Edit language for automated emails	√	√		
Edit self-service console settings	√	√		
Create work space backup and restore settings [1]	√	√		
Delete work space backup and restore settings [1]	√	√		
Edit default variables [1]	√	√		
Edit login notices [1]	√	√		
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	√	√		
Edit certificate settings	√	√		
Create and edit event notifications	√	√		
Delete event notifications	√	√		
Edit device support messages	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Edit certificate-based authentication settings [1]	√			
Edit public web service access settings	√			
View app management	√	√	√	√
Edit BlackBerry World for Work	√	√		
Edit internal app storage [1]	√	√		
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 [1]	√	√		
Edit Apple DEP settings	√	√		
Edit BlackBerry 2FA server settings	√	√		
Edit BlackBerry Connectivity Node settings [2]	√	√		
View One-Time Password tokens	√	√	√	√
Create and edit One-Time Password tokens	√	√		
Edit company directory settings	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		
Delete BlackBerry Connectivity Node servers	√	√		
View BlackBerry Secure Gateway settings	√	√		
Edit BlackBerry Secure Gateway settings	√	√		
View administrator users and roles	√	√	√	√

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View licensing summary	√	√	√	√
Edit licensing settings	√	√		
View migration settings	√	√		
Edit migration settings	√	√		
View infrastructure settings	√	√	√	
Edit logging settings [1]	√	√		
Edit server-side proxy settings [1]	√	√		
View servers [1]	√	√		
Edit servers [1]	√	√		
Delete servers [1]	√	√		
Manage servers [1]	√	√		
View audit settings [1]	√	√		
Edit audit settings and purge data [1]	√	√		
View BlackBerry Secure Connect Plus settings [1]	√	√		
Edit BlackBerry Secure Connect Plus settings [1]	√	√		
View server certificates [1]	√	√		
Update server certificates [1]	√	√		
View BlackBerry Control settings	√	√	√	√
Edit BlackBerry Control settings	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View BlackBerry Dynamics NOC proxy server settings [1]	√	√	√	√
Edit BlackBerry Dynamics NOC proxy server settings [1]	√	√	√	√
Edit SNMP settings [1]	√	√		
Import IT policy pack and device metadata [1]	√			
View collaboration service settings [1]	√	√	√	√
Edit collaboration service settings [1]	√	√		
View BlackBerry Dynamics settings	√	√	√	√
View BlackBerry Dynamics app services	√	√		
Edit BlackBerry Dynamics app services	√			
Create BlackBerry Dynamics app services	√			
Delete BlackBerry Dynamics app services	√			
View BlackBerry Dynamics server properties [1]	√	√		
Edit BlackBerry Dynamics server properties [1]	√			
View BlackBerry Dynamics Direct Connect settings	√	√		
Edit BlackBerry Dynamics Direct Connect settings	√			

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View BlackBerry Dynamics server cluster settings [1]	√	√		
Edit BlackBerry Dynamics server cluster settings [1]	√			
View BlackBerry Dynamics reporting	√	√	√	
View BlackBerry Dynamics communication settings [1]	√	√	√	
Edit BlackBerry Dynamics communicatio settings [1]	√			
View BEMS Mail settings [2]	√	√		
Edit BEMS Mail settings [2]	√			
View BEMS Docs settings [2]	√	√		
Edit BEMS Docs settings [2]	√			
View Enterprise Identity settings	√	√		
View Enterprise Identity Enterprise settings	√	√		
Edit Enterprise Identity Enterprise settings	√	√		
View Enterprise Identity service settings	√	√		
Edit Enterprise Identity service settings	√	√		

[1] On-premises environments only

[2] Cloud 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[1]	√	√		
View device performance logs [1]	√	√		

[1] On-premises environments only

Workspaces

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Organization administrator	√			
Helpdesk administrator	√			
Audit helpdesk administrator	√			

BlackBerry OS permissions

If you upgrade from BES5, the following additional permissions are available in on-premises environments:

- View BlackBerry OS IT policies
- Create and edit BlackBerry OS IT policies
- Delete BlackBerry OS IT policies
- View jobs
- Edit jobs
- View default distribution settings for jobs
- Edit default distribution settings for jobs
- Manage job tasks
- Change status of job tasks

Note: If you upgrade from BES5, the roles configuration in BES5 is copied to BlackBerry UEM. Roles that are copied may have similar names but different permissions. You should review the permissions for each role to determine if you need to turn on or turn off any permissions.

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 **All company directories** option.
Allow administrators in this role to search selected company directories	**a.** Select the **Selected company directories only** option. **b.** Click **Select directories**. **c.** Select one or more directories and click ➡. **d.** Click **Save**.

8. Perform one of the following tasks:

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

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

After you finish: Rank roles.

View a role

You can view the following information about a role:

- Company directories that administrators in the role can search.
- User groups that administrators in the role can manage.
- Permissions for administrators in the role.

Before you begin: You must be a Security Administrator to view a role.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Click **Roles**.
4. Click the name of the role that you want to view.

Change role settings

You can change the settings of all roles except the Security Administrator role.

Before you begin: You must be a Security Administrator to change role settings.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Click **Roles**.
4. Click the name of the role that you want to change.
5. Click ✎.
6. To change directory access, perform one of the following tasks:

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

7. To change group management, perform one of the following tasks:

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

8. Change the permissions for administrators in this role.
9. Click **Save**.

After you finish: If necessary, change the role ranking.

Delete a role

You can delete all roles except the Security Administrator role.

Before you begin:

- You must be a Security Administrator to delete a role.
- Remove the role from all user accounts and user groups that it is assigned to.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Click **Roles**.
4. Click the name of the role that you want to delete.
5. Click  .

How BlackBerry UEM chooses which role to assign

Only one role is assigned to an administrator. BlackBerry UEM uses the following rules to determine which role to assign to an administrator:

- A role assigned directly to a user account takes precedence over a role assigned indirectly by user group.
- If an administrator is a member of multiple user groups that have different roles, BlackBerry UEM assigns the role with the highest ranking.

Rank roles

Ranking is used to determine which role BlackBerry UEM assigns to an administrator when they are a member of multiple user groups that have different roles.

Before you begin: You must be a Security Administrator to rank roles.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Click **Roles**.
4. Use the arrows to move roles up or down the ranking.
5. Click **Save**.

Create an administrator

You can create an administrator by adding a role to a user account or user group. The user group can be a directory-linked group or local group. You can add one role to a user and one role to each group they belong to, and BlackBerry UEM assigns only one of the roles to the user.

Before you begin:

- You must be a Security Administrator to create an administrator.
- Create a user account that has an email address associated with it.
- If necessary, create a user group.
- If necessary, create a custom role.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Perform any of the following tasks:

Task	Steps
Add a role to a user account	**a.** Click **Users**. **b.** Click  . **c.** If necessary, search for a user account. **d.** Click the name of the user account. **e.** In the **Role** drop-down list, click the role that you want to add. **f.** Click **Save**.
Add a role to a user group	**a.** Click **Groups**. **b.** Click  . **c.** If necessary, search for a user group. **d.** Click the name of the user group. **e.** In the **Role** drop-down list, click the role that you want to add. **f.** Click **Save**.

BlackBerry UEM sends administrators an email with their username and a link to the management console. BlackBerry UEM also sends administrators a separate email with their password for the management console. If an administrator does not have a account password, BlackBerry UEM generates a temporary password and sends it to the administrator.

After you finish: If necessary, add user accounts to a user group that has a role assigned to it. Only Security Administrators can add or remove members of a user group that has a role assigned to it.

Change role membership for administrators

You can change the role assigned directly to other administrators. You cannot change your own role.

Before you begin: You must be a Security Administrator to change role membership for administrators.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Perform any of the following tasks:

Task	Steps
Change the role assigned to a user account	**a.** Click **Users**. **b.** If necessary, search for a user account. **c.** Click the name of the user account. **d.** In the **Role** drop-down list, click the role that you want to assign. **e.** Click **Save**.
Change the role assigned to a user group	**a.** Click **Groups**. **b.** If necessary, search for a user group. **c.** Click the name of the user group. **d.** In the **Role** drop-down list, click the role that you want to assign. **e.** Click **Save**.

Delete an administrator

You can delete an administrator by removing a role assigned directly to a user account or user group. When you remove a role from a user group, the role is removed from every user that belongs to the group. If no other roles are assigned, the user is no longer an administrator. User accounts and user groups remain in the management console and devices are not affected.

Note: At least one administrator must be a Security Administrator.

Before you begin: You must be a Security Administrator to delete an administrator.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Perform any of the following tasks:

Task	Steps
Remove a role from a user account	**a.** Click **Users > All users**. **b.** Select the user account that you want to remove the role from. **c.** Click  . **d.** Click **Delete**.
Remove a role from a user group	**a.** Click **Groups**. **b.** Select the user group that you want to remove the role from. **c.** Click  . **d.** Click **Delete**.

Setting up BlackBerry UEM Self-Service for users

BlackBerry UEM Self-Service is a web-based application that you can make available to users so that they can perform management tasks such as creating activation passwords, remotely locking their devices, or deleting data from their devices. Users do not need to install any software on their computers to use BlackBerry UEM Self-Service. You must provide the web address and login information to users.

In an on-premises environment, you can force users to read and accept a log in notice before they can log in to BlackBerry UEM Self-Service.

Set up BlackBerry UEM Self-Service

Set up BlackBerry UEM Self-Service so that users can log in and perform some self-service tasks.

1. On the menu bar, click **Settings > Self-Service**.
2. Click **Self-Service settings**.
3. Verify that **Allow users to access the self-service console** is selected.
4. Specify the number of minutes, hours, or days that a user can activate a device before the activation password expires.
5. Specify the minimum number of characters required in an activation password.
6. In the **Minimum password complexity** drop-down list, select the level of complexity required for activation passwords.
7. To automatically send an activation email to users when they create an activation password in BlackBerry UEM Self-Service, select the **Send an activation email** check box. You can use the default activation email template or select a different template from the drop-down list.
8. To send a login notification email to the user each time they log in to BlackBerry UEM Self-Service, select the **Send self-service login notification** check box.
9. Click **Save**.

After you finish: Provide the BlackBerry UEM Self-Service web address and login information to users.

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada