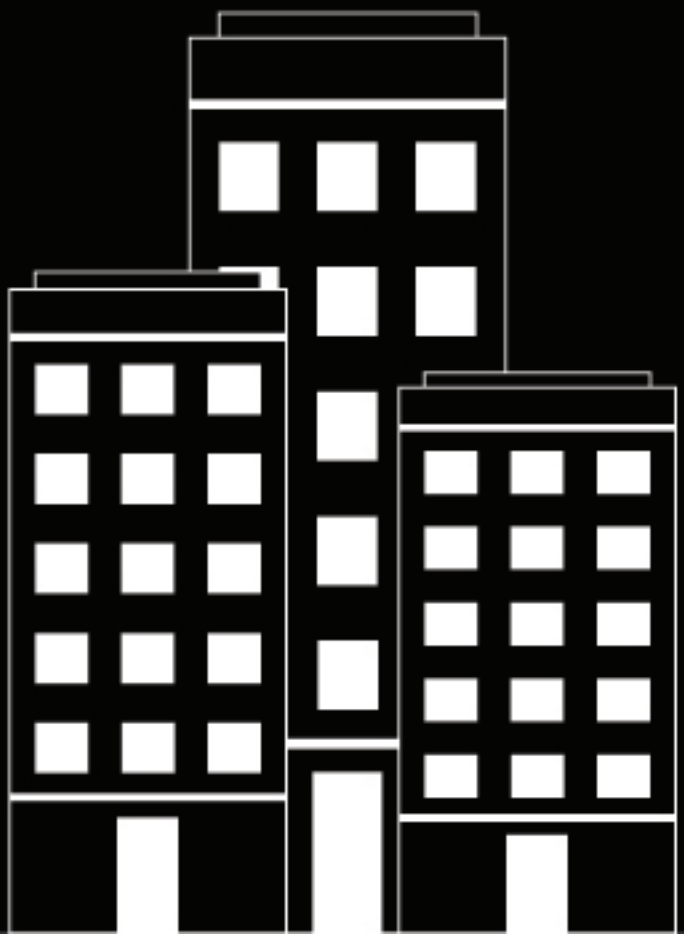

BlackBerry UEM

Managing administrators, users, and groups

Administration

12.19

Contents

Managing BlackBerry UEM administrators, users, and groups

This guide provides instructions and details for creating and configuring administrator accounts, user accounts, and groups to manage your organization's BlackBerry UEM environment.

Task	Description
Configure login options for the management console.	Configure how administrators and users authenticate with the UEM consoles, including password complexity, login notices, session timeout limits, and options like directory-based authentication and single sign-on.
Create and managing administrator roles.	Use preconfigured administrator roles or create custom roles to configure the level of control and permissions that administrators have in the management console.
Create an administrator.	Create administrator users to manage your organization's UEM environment.
Create and manage user accounts.	Create user accounts in UEM directly or create user accounts from your organization's company directory.
Create and manage user groups.	Create user groups to apply settings and configurations to multiple users.
Create and manage device groups.	Create device groups to apply settings and configurations to specific device types.
Create and manage shared device groups.	Create shared device groups to allow multiple users to share an iOS device.
Create and manage public device groups.	Create public device groups to manage single-purpose iOS or Android Enterprise devices that are locked to a specific set of apps.
Create and manage shared iPad groups.	Create shared iPad groups to allow multiple users to sign in to and use a shared iPad device.
Manage Chrome OS devices.	Use UEM to perform management actions for Chrome OS devices.
Set up BlackBerry UEM Self-Service.	Allow users to access UEM Self-Service to perform self-service device management tasks.
Create user roles for UEM Self-Service.	Use roles to manage end-user permissions for UEM Self-Service.
Customize the user list.	Modify the list of user accounts in the management console to suit your needs.

Configuring console login options

You can configure how administrators and users authenticate with the BlackBerry UEM consoles, including the required password complexity, login notices, and session timeout limits.

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

Authentication option	Description
Local password-based authentication	Local administrators and users can authenticate with a username and password.
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 Connecting to your company directories in the Configuration content.
Single sign-on	If you connect 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. A password or certificate is not required to log in. See Configure single sign-on for BlackBerry UEM. This feature is not supported by UEM Cloud.
Certificate-based authentication	You can set up certificate-based authentication so that administrators and users can log in using an authentication certificate. See Configure certificate-based console authentication. This feature is not supported by 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, see KB 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.

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. In the management console, on the menu bar, click **Settings > General settings > Console**.
2. In the **Minimum number of characters** field, specify 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.
4. Click **Save**.

Create a login notice for the consoles

You can create a login notice that is displayed to administrators or users in an on-premises environment when they log in to the BlackBerry UEM management console or BlackBerry UEM Self-Service. The notice informs administrators or users about the terms and conditions they must accept to use the consoles. This feature is not supported for UEM Cloud.

1. In the management console, on the menu bar, click **Settings > General settings > Login notices**.
2. Click .
3. Do any of the following:

Task	Steps
Configure a login notice for the UEM 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 log in.
Configure a login notice for 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 log in.

4. Click **Save**.

Set the session timeout limit

1. In the management console, on the menu bar, click **Settings > General settings > Console**.
2. In the **Session timeout** field, specify the amount of time, in minutes, before the session times out and the user is logged out.
3. In the **Session timeout warning** field, specify the amount of time, in minutes, prior to logging out a user that the session timeout warning displays.
4. Click **Save**.

Configure single sign-on for BlackBerry UEM

If you connect BlackBerry UEM to Microsoft Active Directory, you can configure single sign-on authentication to allow 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 UEM automatically. Windows login information can include Active Directory credentials or derived credentials (for example, from CAC readers or digital tokens).

This feature is not supported by UEM Cloud.

Before you begin:

- Do the following to configure constrained delegation for the Active Directory account that UEM uses for the directory connection:
  1. Use the Windows Server ADSI Edit tool or setspn command-line tool to add the following SPNs for UEM to the 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)

2. In Microsoft Active Directory Users and Computers, in the Microsoft Active Directory account properties, on the **Delegation** tab, enable **Trust this user for delegation to specified services only** and **Use Kerberos only**.
3. Add the SPNs to the list of services.

- If you enable single sign-on for multiple Active Directory connections, verify that there are no trust relationships between the Active Directory forests.

1. In the UEM management console, on the menu bar, click **Settings > External integration > Company directory**.
2. In the **Configured directory connections** section, click an Active Directory connection.
3. On the **Authentication** tab, select the **Enable Windows single sign-on** check box.
4. Click **Save**.
5. Click **Save** again.
6. Click **Close**.

After you finish:

- Restart the UEM services on each computer that hosts a UEM instance.
- Instruct administrators and users to use the following URLs:
  - Management console: https://<*host_FQDN_or_pool_name*>:<*port*>/admin
  - UEM Self-Service: https://<*host_FQDN_or_pool_name*>:<*port*>/mydevice

  Single sign-on authentication takes precedence over other authentication methods. If your organization's security standards require that administrators or users use another authentication method, the single sign-on method can be circumvented by appending ?sso=n to the end of the URLs above.
- Instruct administrators and UEM Self-Service users to configure their browsers to support single sign-on for UEM:
  - Microsoft Edge: The management console and UEM Self-Service URLs must be assigned to the local intranet zone. Enable Integrated Windows Authentication.
  - Mozilla Firefox: In the about:config list, Add https://, <*host_FQDN_or_pool_name*> to the "network.negotiate-auth.trusted-uris" preference.
  - Google Chrome: The management console and UEM Self-Service URLs must be assigned to the local intranet zone.

Configure certificate-based console authentication

In an on-premises BlackBerry UEM environment, you can set up certificate-based authentication so that administrators can log in using an authentication certificate. 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 UEM database. This feature is not supported for UEM Cloud.

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

1. In the management console, on the menu bar, click **Settings > General settings > Certificate-based console authentication**.
2. Select the **Enable certificate-based authentication** check box.
3. Click **Browse** and navigate to the CA certificate files.

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

   If the user principal name in the certificate matches a known user, UEM grants access according to the user's permissions.

5. To require UEM to verify that the user email address in the certificate matches a user email address in the UEM database, select the **Check for email address** check box.

   If the user email address in the certificate matches a known user, 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**, 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, UEM denies access.
6. Click **Save**.

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

Creating and managing administrator roles

You can assign pre-configured roles to administrators, or you can create custom roles to meet your organization's requirements. You must be a Security Administrator to create custom roles, view information about a role, change role settings, rank roles, and delete roles.

Permissions for preconfigured administrator roles

BlackBerry UEM includes four preconfigured roles for administrators. The Security Administrator role has full permissions, including creating and managing roles and administrators. You cannot edit or delete this role. At least one administrator must be assigned the Security Administrator role. The Enterprise Administrator role (all permissions except for creating and managing roles and administrators), the Senior HelpDesk role (permissions to perform intermediate administrative tasks), and the Junior HelpDesk role (permissions to perform basic administrative tasks) can be edited or deleted. The following tables list the permissions that are turned on by default for each preconfigured role.

Some permissions are supported only in custom roles.

Roles and administrators

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	√	√	√	

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	√
Lock work space	√	√	√	√
Reset work space password	√	√	√	√
Specify device password	√	√	√	√
Lock device and set message	√	√	√	√
Unlock device and clear password	√	√	√	√
Delete only work data	√	√	√	√

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	√
Update iOS software	√	√	√	√
Update iOS software on multiple devices	√			
Turn off device	√	√	√	√
View device location details	√	√	√	
View device location history	√	√		
View Exchange gatekeeping information	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		

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

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		
View FileVault profiles	√	√	√	√
Create and edit FileVault profiles	√	√		
Delete FileVault profiles	√	√		
View location service profiles	√	√	√	√
Create and edit location service profiles	√	√		

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

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

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	√
Create and edit AirPrint profiles	√	√		
Delete AirPrint profiles	√	√		
View network usage profiles	√	√	√	√
Create and edit network usage profiles	√	√		

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

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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 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	√	√		

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		
Assign Enterprise Identity authentication policy to users and groups	√	√		

Apps

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
View apps and app groups	√	√	√	√

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√	√	√
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 [1]	√	√		
Delete work space backup and restore settings [1]	√	√		
Edit default variables [1]	√	√		

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

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√	√		
Edit Microsoft Intune settings	√	√		
Edit Microsoft Exchange gatekeeping settings	√	√		
Edit Androidwork profile settings	√	√		
Edit certification authority settings	√	√		
Edit Samsung Knox bulk enrollment settings	√	√		

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

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

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
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	√			
View BlackBerry Dynamics server cluster settings [1]	√	√		
Edit BlackBerry Dynamics server cluster settings [1]	√			
View BlackBerry Dynamics reporting	√	√	√	
View BlackBerry Dynamics communication settings [1]	√	√	√	

Permission	Security Administrator	Enterprise Administrator	Senior HelpDesk	Junior HelpDesk
Edit BlackBerry Dynamics communication 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	√			

Create a custom administrator role

If the preconfigured administrator roles do not meet your organization's requirements, you can create custom ones. 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.
- Review the Permissions for preconfigured administrator roles.

1. In the management console, on the menu bar, click **Settings > Administrators > Roles**.
2. Click  .
3. Type a name and description for the role.
4. To copy permissions from another role, in the **Permissions copied from role** drop-down list, click a role.
5. Do one of the following:

Task	Steps
Allow administrators with this role to search all company directories.	Select the **All company directories** option.
Allow administrators with 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**.

6. Do one of the following:

Task	Steps
Allow administrators with this role to manage all users and groups	Select the **All groups and users** option.
Allow administrators with 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**.

7. Configure the permissions for administrators with this role.
8. Click **Save**.

After you finish: To rank roles, change role settings, or delete a role, see Manage administrator roles.

Manage administrator roles

After you create an administrator role, you can rank the role, change the role's permissions, or delete the role. BlackBerry UEM uses ranking to determine which role is assigned to an administrator when they are a member of multiple user groups that have different roles. If a role is assigned directly to a user account, it takes precedence over a role assigned to a user group. If an administrator is a member of multiple user groups that have different roles, UEM assigns the role with the highest ranking.

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

1. In the management console, on the menu bar click **Settings > Administrators > Roles**.
2. Do one of the following:

Task	Steps
Rank a role.	**a.** Use the arrows to change the rank of the role. **b.** Click **Save**.

Task	Steps
Change a role's settings.	**a.** Click the name of the role that you want to change. **b.** Click **Edit**. **c.** Make your changes. **d.** Click **Save**.
Delete a role.	**a.** Click the name of the role that you want to delete. **b.** Click  .

Create an administrator

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

When a role is assigned to a user account or to a user group, UEM sends administrators an email with their username and a link to the management console. UEM also sends administrators a separate email with their password for the management console. If an administrator does not have an account password, UEM generates a temporary password and sends it to the administrator.

Before you begin:

- You must be a Security Administrator to create an administrator.
- If necessary, Create a custom administrator role.

1. In the management console, on the menu bar, click **Settings > Administrators**.
2. Do one of the following:

Task	Steps
Assign a role to a user account.	**a.** Click **Users**. **b.** Click  . **c.** Click the name of the user account that you want to assign the role to.
Assign a role to a user group.	**a.** Click **Groups**. **b.** Click  . **c.** Click the name of the user group that you want to assign the role to.

3. In the **Role** drop-down list, click the role that you want to assign.
4. Click **Save**.

After you finish:

- To change an assigned role, click the name of a user account or user group, click the role that you want to assign, and click **Save**.
- To delete an administrator, select the user account or the user group that you want to remove the role from and click  > **Delete**.

Creating and managing user accounts

You can create user accounts directly in BlackBerry UEM or, if you connected UEM to your company directory, you can add user accounts from your company directory. You can also use a .csv file to add multiple user accounts to UEM at one time.

After you create user accounts, you can enable services for users, add users to groups, activate users' devices on UEM, and send communications to users.

Create a user account

Before you begin:

- If you want to add a directory user, verify that BlackBerry UEM is connected to your company directory. For information about connecting UEM to a company directory and enabling directory-linked groups, see Connecting to your company's directories in the Configuration content.
- If you want to enable the BlackBerry Workspaces service for your users, verify that the Workspaces plug-in for UEM is installed on each instance of UEM in your environment.

1. In the management console, on the menu bar, click **Users > Managed devices > Add user**.
2. Do one of the following:

Task	Steps
Add a directory user.	**a.** On the **Company directory** tab, search for the directory user that you want to add. You can search by first name, last name, display name, username, or email address. **b.** In the search results, select the user account.
Add a local user.	**a.** On the **Local** tab, specify the user's first name and last name. **b.** Optionally, edit the user's display name. **c.** In the **Username** field, type a unique username. **d.** In the **Email address** field, enter a contact email address for the user account. An email address for the user account is required when you enable a service such as Workspaces or device management. **e.** Optionally, click **Additional user details** and fill in the fields as needed.
Add a BlackBerry Online Account user (UEM Cloud only)	**a.** On the **Non-directory** tab, specify the user's first name and last name. **b.** Optionally, edit the user's display name. **c.** In the **Email address** field, enter a contact email address for the user account. An email address for the user account is required when you enable a service such as Workspaces or device management. **d.** Optionally, click **Additional user details** and fill in the fields as needed.

3. If local groups exist in UEM and you want to add the user account to groups, in the **Available groups** list, click one or more groups and click ➡.

   When you create a user account, you can add it to local groups only. If the user account is a member of a directory-linked group, it is automatically associated with that group when the synchronization between UEM and your company directory occurs.

4. In a Cloud environment, under **UEM Self-Service**, select either **BlackBerry Online Account** or **Local UEM user account**. If you select Local UEM user account, create a password for BlackBerry UEM Self-Service. If the user is assigned an administrative role, they can also use the password to access the management console.
5. In an on-premises environment, if you add a local user, in the **Password** field, create a password for UEM Self-Service. If the user is assigned an administrative role, they can also use the password to access the management console.
6. In the **Enabled services** section, select the **Enable user for device management** check box.
7. If the Workspaces plug-in for UEM is installed in the domain, to enable the Workspaces service, do the following:
   a) In the **BlackBerry Workspaces** section, select the **Enable BlackBerry Workspaces** check box. By default, users enabled with the Workspaces service receive the Visitor role.
   b) Select one or more user roles and click ➡.
8. Do one of the following:

Task	Steps
Have users activate devices with the activation profile that is currently assigned to them.	**a.** In the **Activation option** drop-down list, select **Default device activation**. **b.** In the **Activation password** drop-down list, select whether you want to set the password or autogenerate a password. **c.** Optionally, change the activation period expiration. **d.** If you want the activation password to be valid only for one device activation, select **Activation period expires after the first device is activated**. **e.** In the **Activation email template** drop-down list, select the template that you want to use for the activation email.
Pair an activation password with a specific activation profile.	**a.** In the **Activation option** drop-down list, click **Device activation with specified activation profile**. **b.** In the **Activation profile** drop-down list, select the activation profile that you want to pair with a password. **c.** In the **Activation password** drop-down list, select whether you want to set the password or autogenerate a password. **d.** Optionally, change the activation period expiration. **e.** If you want the activation password to be valid for one device activation only, select **Activation period expires after the first device is activated**. **f.** In the **Activation email template** drop-down list, select the template that you want to use for the activation email.
Allow users to activate only BlackBerry Dynamics apps.	**a.** In the **Activation option** drop-down list, select **BlackBerry Dynamics access key generation**. **b.** In the **Number of access keys to generate** drop-down list, select the number of keys. Each key can be used only once to activate a BlackBerry Dynamics app. **c.** Select the number of days that you want the access key to remain valid. **d.** In the **Activation email template** drop-down list, select the template that you want to use for the activation email.
Add the user to UEM only.	In the **Activation option** drop-down list, select **Do not set**.

9. If you use custom variables, expand **Custom variables** and specify the appropriate values for the variables that you defined.

10. Do one of the following:

- To save the user account, click **Save**.
- To save the user account and create another user account, click **Save and new**.

Creating user accounts from a .csv file

You can import user accounts from a .csv file into BlackBerry UEM to create multiple user accounts at one time. You can create the .csv file manually by using a sample .csv file that you can download from the management console (Users > All users > Add user > Import > Download sample .csv file).

Depending on your requirements, you can specify group membership and activation settings for the user accounts by including the following columns in the .csv file:

Column Header	Description
Group membership	Assign one or more user groups to each user account. Use a semicolon (;) to separate multiple user groups. If you do not include the Group membership column, when you import the file, you are given the option to select the group that you want all of the imported user accounts to be added to.
MDM (BlackBerry UEM)	Specify whether the user is enabled for MDM. To enable a user for MDM, type "Enabled".
Activation password	Specify the activation password. This value is required if the “Activation password generation” value is set to “manual.”
Activation template	Specify the name of the activation email template that you want to send to the user. If you do not specify a name, the default email activation template is used.
Activation password expiration	Specify the time, in seconds, that the activation password is valid before it expires.
Activation password generation	Specify one of the following: • Auto: The activation password is automatically created and sent to the user. (Default) • Manual: The activation password is set in the "Activation password" column. • Ignore: No activation password is generated.
Send activation email	Specify one of the following: • True: The activation email is sent to the user. • False: The activation email is not sent to the user. If “Activation password generation” is set to “Auto”, the activation email is sent to the user regardless of the value in this column. If the “Activation password generation” value is "Manual" and this value is empty, then the default is True. If the "Activation password generation" value is "Ignore", the user will not receive a self-service activation email.

Column Header	Description
User type	This column is required whenever the .csv file includes both local and directory user accounts. Specify one of the following: • L: Local user accounts • D: Directory user account
Directory UID	This column is an alternative to entering the email address for directory user accounts. By default, the email address is used to validate the directory user accounts, but you can specify that the directory UID is used instead. If the user account cannot be validated against the directory UID, an error is reported. If you include a Directory UID value for one of your users, the column header must include Directory UID, and all of the rows in the .csv file must include either a Directory UID or have an empty placeholder (,) for the Directory UID column.

Add user accounts to UEM using a .csv file

Before you begin:

- Prepare the .csv file. For more information, see Creating user accounts from a .csv file.
- If the .csv file contains directory user accounts, verify that BlackBerry UEM is connected to your company directory.

1. In the management console, on the menu bar, click **Users**.
2. On the **All users** or **Managed devices** tab, click **Add user**.
3. On the **Import** tab, click **Browse** and navigate to the .csv file.
4. Click **Load**.
5. If the .csv file does not use the "Group membership" column and you want to add user accounts to groups, in the **Available groups** list, select one or more groups and click ➡. Click **Next**.

   When you import the .csv file, all of the user accounts are added to the local groups that you select. If a user account is a member of a directory-linked group, it is automatically associated with that group when the synchronization between UEM and your company directory occurs.
6. Review the list of user accounts and do one of the following:
   - To correct the errors for any invalid directory user accounts, click **Cancel**, make corrections to the file, and upload it again.
   - To add the valid user accounts, click **Import**. Invalid directory user accounts are ignored.

Enable services for a user

If BlackBerry UEM is enabled for one or more services (for example, Workspaces, BBM Enterprise, or Enterprise Identity) you can enable a service for a user.

1. In the management console, on the menu bar, click **Users > All users**.
2. Search for and click a user account.
3. On the user detail page, the available services are listed under the user's name.
4. If a service is not currently enabled, it is listed with a + icon. Click + to add the service.
5. Configure the service as required and save.

After you finish: If you want to remove a service from a user, click . Click on the service that you want to remove. Before you can remove MDM controls, you must remove activated devices from the user. Before you can remove the Enterprise Identity service, you must remove all Enterprise Identity assignments from the user.

Add users to user groups

For more information about user groups, see Creating and managing user groups. Note that you cannot change a user's membership to a directory-linked group.

Before you begin: To add a user that is assigned an administrator role to a user group, you must be a Security Administrator.

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Select the check box beside the users that you want to add to user groups.
3. Click .
4. In the **Available groups** list, select one or more groups and click .
5. Click **Save**.

After you finish:

- To change which user group a user belongs to, click the name of the user account whose membership you want to change. Click and, in the **Group membership** section, use the left and right arrows to add the user to groups or remove the user from groups.
- To remove multiple users from a user groups, on the menu bar, click **Groups**. Click the user group that you want to remove the users from. Select the users that you want to remove and click .

Manage user accounts

Before you begin: Create a user account.

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Do one of the following:
   - To manage an individual user, search for and click a user account, then go to the next step.
   - To perform an action for multiple user accounts at once, select the check box beside each user account that you want to manage. Click an action above the user list (for example, you can add the selected user accounts to user groups) and follow the instructions on the screen.
3. Do any of the following:

Task	Steps
Edit a user's information.	**a.** Click . **b.** Make changes to the user's account. **c.** Click **Save**.
Add a note to a user's account.	**a.** Click . **b.** Type your notes. The notes that you type are automatically saved and stored with the user account and not with an individual device.

Task	Steps
Assign an IT policy, profile, app, or app group to the user	**a.** In the appropriate section, click +. **b.** Select the IT policy, profile, app, or app group that you want to assign. Follow the prompts and select the appropriate settings to complete the assignment. **c.** To remove an IT policy, profile, app, or app group from the user, beside the property that you want to delete, click ×.
Synchronize information for a directory user	Click .
Delete a user account.	**a.** Click . **b.** Click **Delete**.

Send communications to users

You can send an email, including an email message containing a BlackBerry UEM Self-Service password, to one or more users. When you send a password, the passwords are randomly generated and an email message containing a password is sent to each user. In a UEM on-premises environment, you can configure the email address that the email is sent from in the SMTP server settings.

Before you begin: The users that you send the email message to must have an email address associated with their user account.

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Select the check box beside each user that you want to send the message to.
3. Do one of the following:

Task	Steps
Send an email to users.	**a.** Click . **b.** Optionally, to copy the email to yourself or to others, click **CC** and type one or more email addresses. Separate the addresses with commas or semicolons.
Send a BlackBerry UEM Self-Service password to users.	**a.** Click . **b.** Click **Continue**.

Creating and managing user groups

A user group is a collection of related users who share common properties. Administering users as a group is more efficient than administering individual users because properties can be added, changed, or removed for all members of the group at the same time. Users can belong to more than one group at a time. When you create and manage a user group, you can assign IT policies, profiles, and apps in the management console. You can also define one group as a member of another group.

You can create two types of user groups:

- Directory-linked groups: These groups link to groups in your company directory. Only directory user accounts can be members of a directory-linked group.
- Local groups: These groups are created and maintained in BlackBerry UEM and can have both local user accounts and directory user accounts assigned to them.

For directory-linked groups, UEM periodically synchronizes the membership of the group with its associated company directory groups. Users that were added or removed from the company directory are added or removed from the directory-linked group. When users are added into a company directory group that is linked to a directory-linked group, they are assigned the properties that are assigned to the group. When users are removed from the directory-linked group, the properties are removed from the user.

Each directory-linked group can link to a single company directory. For example, if UEM has two Microsoft Active Directory connections (A and B), and you create a directory-linked group that is linked to connection A, you can link only to directory groups from connection A. You must create new directory-linked groups for any other directory connections.

Synchronizing directory-linked groups does not add or delete users in UEM. To allow UEM to create user accounts when new company directory users are created, you must enable onboarding.

Create a directory-linked group

You can create user groups that link to groups in your company directory. BlackBerry UEM periodically synchronizes the membership of a directory-linked group with its associated company directory groups. When a user is added or removed from the company directory, they are added or removed from the directory-linked group. The profiles, policies, and apps that you assign to the directory-linked group are assigned to the users in that group. When users are removed from group, those properties are removed.

Before you begin: Enable directory-linked groups.

1. In the management console, on the menu bar, click **Groups > User**.
2. Click .
3. Type the group name.
4. In the **Linked directory groups** section, do the following:
   a) Click +.
   b) Type the name or partial name of the company directory group that you want to link to.
   c) If you have more than one company directory connection, select the connection that you want to search. After you have made this selection, the directory-linked group is permanently associated with the selected connection.
   d) Click .
   e) Select the company directory group.
   f) Click **Add**.

g) If necessary, to allow the directory settings to control the number of nested groups, select the **Link nested groups** check box. To link to all nested groups, leave the check box unselected.
h) Repeat these steps to link additional groups.

5. Do any of the following:

Task	Steps
Assign a user role to the directory-linked group.	**a.** In the **User role** section, click +. **b.** In the drop-down list, click the name of the user role that you want to assign to the group. **c.** Click **Add**.
Assign an IT policy or profile to the directory-linked group.	**a.** In the **IT policy and profiles** section, click +. **b.** Click **IT policy** or a profile type. **c.** In the drop-down list, click the name of the IT policy or profile that you want to assign to the group. **d.** Click **Assign**.
Assign an app to the directory-linked group.	**a.** in the **Assigned apps** section, click +. **b.** Search for and select the app that you want to assign. **c.** Click **Next**. **d.** In the **Disposition** drop-down list, do one of the following: • To install the app automatically on devices and to prevent users from uninstalling the app, select **Required**. • To require users to install the app and prevent Apple VPP apps from updating automatically, select **Required without updates**. • To allow users to install and uninstall the app, select **Optional**. • To permit users to install and remove the app and prevent Apple VPP apps from updating automatically, select **Optional without updates**. **e.** For iOS devices, to assign per-app VPN settings to an app or an app group, in the **Per app VPN** drop-down list, select the settings to associate with the app or app group. **f.** Click **Assign**.

6. Click **Add**.

Add a company directory group to an existing directory-linked group

Before you begin: Create a directory-linked group.

1. In the management console, on the menu bar, click **Groups > User**.
2. Click the directory-linked group.
3. On the **Settings** tab, click ✎.
4. In the **Linked directory groups** section, click +.
5. Search for and select the company directory group that you want to add to an existing directory-linked group.
6. Click **Add**.
7. If required, select **Link nested groups**.

Create a local group

You can create a local user group in BlackBerry UEM that you can assign IT policies, profiles, and apps to. When you add user accounts to the group, the properties that you assign to the group are assigned to each member of the group. You can add both local user accounts and directory user accounts to a local group.

1. In the management console, on the menu bar, click **Groups > User**.
2. Click  .
3. Type a name and a description for the group.
4. Do any of the following:

Task	Steps
Assign a user role to the local group.	**a.** In the **User role** section, click +. **b.** In the drop-down list, click the name of the user role that you want to assign to the group. **c.** Click **Add**.
Assign an IT policy or profile to the local group.	**a.** In the **IT policy and profiles** section, click +. **b.** Click **IT policy** or a profile type. **c.** In the drop-down list, click the name of the IT policy or profile that you want to assign to the group. **d.** Click **Assign**.

Task	Steps
Assign an app to the local group.	**a.** In the **Assigned apps** section, click +. **b.** Search for and select the app that you want to assign to the group. **c.** Click **Next**. **d.** In the **Disposition** drop-down list, do one of the following: • To install the app automatically on devices and to prevent users from uninstalling the app, select **Required**. This option is not available for BlackBerry apps. • To require users to install the app and prevent Apple VPP apps from updating automatically, select **Required without updates**. • To allow users to install and uninstall the app, select **Optional**. • To permit users to install and remove the app and prevent Apple VPP apps from updating automatically, select **Optional without updates**. If the same app is assigned to a user account and to the user group that the user belongs to, the disposition of the app assigned to the user account takes precedence. **e.** For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list, select the settings to associate with the app or app group. **f.** If available, for iOS and Android devices, select an app configuration to assign to the app. **g.** If you use Android Enterprise and have created tracks for apps in the Google Play console, select a track to assign to the app. **h.** Click **Assign**.

5. Click **Add**.

Add nested groups to a user group

When you nest a group within a user group, members of the nested group inherit the properties of the user group. You create and maintain the nesting structure in BlackBerry UEM and you can nest both directory-linked groups and local groups within each type of user group. When you add a nested group to a user group, any groups that belong to the nested group are also added.

1. In the management console, on the menu bar, click **Groups > User**.
2. Search for and click the name of a user group.
3. In the **Nested groups** tab, click +.
4. Select one or more groups.
5. Click **Add**.

After you finish: To remove nested groups that are assigned directly to a user group, in **Groups**, click the name of the user group that you want to remove a group from. In the **Nested groups** tab, click × beside the nested group that you want to remove.

Manage a user group

Before you begin: Create a local group or Create a directory-linked group.

1. In the management console, on the menu bar, click **Groups > User**.
2. Search for and click the user group that you want to manage.
3. Do any of the following:

Task	Steps
View information about a user group.	**a.** To view the user accounts that are assigned to the group, click **Users**. **b.** To view the nested groups that are assigned to the group, click **Nested groups**. **c.** To view the linked-directory groups (if available) or the assigned properties of the group, click **Settings**.
Change the name or description of a user group.	**a.** Click ✎. **b.** Change the name or the description of the user group. **c.** Click **Save**.
Manage the assigned roles, assigned profiles, or assigned apps of the user group.	**a.** Click the **Settings** tab. **b.** To assign a role, profile, or app to the user group, beside the appropriate section, click +. **c.** To remove a role, profile, or app from the user group, beside the property that you want to remove, click ✕.
Delete a user group.	**a.** Click 🗑. **b.** Click **Delete**.

Creating and managing device groups

A device group is a group of devices that have common attributes, such as device model and manufacturer, OS type and version, service provider, and ownership. Based on the attributes that you define, BlackBerry UEM automatically moves devices into or out of the device group.

You can use device groups to apply different sets of policies, profiles, and apps to specific devices. The properties that you assign to a device group take precedence over those that you assign to a user or a user group. You cannot assign activation profiles or user certificates to device groups.

Create a device group

1. In the management console, on the menu bar, click **Groups > Device**.
2. Click  .
3. Type a name for the device group.
4. Optionally, in the **Scope to user groups** section, select user groups to apply the device group to. If you don't select any user groups, the device group applies to all activated devices.
5. In the **Device query** section, in the first drop-down list, do one of the following:
   - If you want to include devices that match all of the attributes that you define, select **All**.
   - If you want to include devices that match at least one of the attributes that you define, select **Any**.
6. In the **Device query** section, set the parameters for the device group. See Parameters for device groups.
7. Click **Next**.
8. Do any of the following:

Task	Steps
Assign an IT policy or profile to the device group.	**a.** In the **IT policy and profiles** section, click +. **b.** Click **IT policy** or a profile type. **c.** In the drop-down list, click the name of the IT policy or profile that you want to assign to the group. **d.** Click **Assign**.

Task	Steps
Assign an app or an app group to the device group.	**a.** In the **Assigned apps** section, click +. **b.** Search for and select the app that you want to assign to the group. **c.** Click **Next**. **d.** In the **Disposition** drop-down list, do one of the following: • For iOS and Android apps, to require users to follow the actions defined for apps in the compliance profile assigned to them, select **Required**. • To require users to install the app and prevent Apple VPP apps from updating automatically, select **Required without updates**. • To allow users to install and uninstall the app, select **Optional**. This option is not available for app groups that support Android Enterprise. • To permit users to install and remove the app and prevent Apple VPP apps from updating automatically, select **Optional without updates**. **e.** For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list, select the settings to associate with the app or app group. **f.** If available, for iOS and Android devices, select an app configuration to assign to the app. **g.** If you use Android Enterprise and have created tracks for apps in the Google Play console, select a track to assign to the app. **h.** Click **Assign**. Note that you can't add BlackBerry Dynamics apps to device groups because entitlements can be granted only to users. Any BlackBerry Dynamics apps included in app groups that you add to device groups will not be assigned to user. If your environment supports Android Enterprise, you can't add Android apps that have an optional disposition to device groups. Google Play for Work can assign apps only to Google User IDs, not to device IDs. If you add Android apps that have a required disposition to a device group, the apps will be installed, but the apps will not be listed in Google Play for Work.

9. Click **Save**.

Parameters for device groups

When you create a device group, you configure a device query that includes one or more attribute statements. You can specify whether a device belongs to the device group if it matches any attribute statement or only if it matches all the attribute statements. Each attribute statement contains an attribute, an operator, and a value.

Attribute	Operators	Values
Carrier	• = • != • Starts with	Specify the name of a service provider, such as T-Mobile or Bell.
BlackBerry Dynamics	• = • !=	In the drop-down list, select one of the following options: • Disabled • Enabled
Manufacturer	• = • != • Starts with	Specify the name of a device manufacturer (for example, Apple).
Model	• = • != • Starts with	Specify the name of a device model (for example, iPhone 15).
OS	• = • !=	In the drop-down list, select the appropriate OS.
OS version	• = • != • >= • <=	Specify the OS version (for example, 7.1.1 or 10.3). If you use this attribute, you should also specify the OS attribute.
Ownership	• = • !=	In the drop-down list, select one of the following options: • Work • Personal • Not specified
Activation type	• = • !=	In the drop-down list, select an activation type. The list contains the same activation types that are available for assignment in your activation profiles.
Knox Workspace	• = • != • Starts with	Specify a Samsung Knox Workspace version (for example, 3.2.1).

Manage a device group

Before you begin: Create a device group.

1. In the management console, on the menu bar, click **Groups > Devices**.
2. Search for and click the device group that you want to manage.
3. Do one of the following:

Task	Steps
View information about a device group.	**a.** To view the devices that are assigned to the device group, click the **Devices** tab. **b.** To view the user groups, device queries, IT policies, profiles, or apps that are assigned to the device group, click the **Settings** tab.
Edit a device group.	**a.** Click  . **b.** Make your changes. **c.** Click **Save**.
Delete a device group.	**a.** Click  . **b.** Click **Delete**.

Creating and managing shared device groups

If you want to allow multiple users to share an iOS device, you can create a shared device group. You can configure settings for the group that are specific to each user or the same for all users. When you create a shared device group, BlackBerry UEM creates a local user account that owns the shared device group.

To check out a device, users can use either local or Microsoft Active Directory authentication. You can customize the terms of use that users must accept when they check out a shared device. When they check in the device, it is available for the next user. Shared devices are managed by UEM during the check-out and check-in process.

This feature was designed for supervised devices with the following configuration:

- App lock mode enabled
- VPP apps assigned

This feature does not support BlackBerry Dynamics apps. The same BlackBerry Dynamics profile must be assigned to the user account that owns the shared device group and to the shared device group itself. You must verify that the "Enable UEM Client to enroll in BlackBerry Dynamics" option is not selected in the profile.

Create a shared device group

When you create a shared device group, a local user account is created. This local user account owns the shared device group.

1. In the management console, on the menu bar, click **Dedicated devices > Shared device groups**.
2. Click +.
3. Type a name and a description for the shared device group.
4. Type the username for device activation.
5. To require users to accept terms of service when they check out a shared device, select **Enable terms of service** and specify the terms of the service.
6. For each user that you want to add to the group, in the **Granted users** section, search for and click the user.

   Users can belong to multiple shared device groups.
7. To assign an app or app group, in the **Assigned apps** section, click + and do the following:
   a) Search for and select the app that you want to assign to the group.
   b) Click **Next**.
   c) For iOS or Android apps, to require users to follow the actions defined for apps in the compliance profile assigned to them, in the **Disposition** drop-down list, select **Required**.

      If the app group supports Android Enterprise, the disposition can be set to **Required** only.
   d) To allow users to install and uninstall the app, in the **Disposition** drop-down list, select **Optional**.
   e) For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list, select the settings to associate with the app or app group.
   f) If available, for iOS and Android devices, select an app configuration to assign to the app.
   g) If you use Android Enterprise and have created tracks for apps in the Google Play console, select a track to assign to the app.
   h) Click **Assign**.

      You can't add BlackBerry Dynamics apps to device groups because entitlements can only be granted to users. Any BlackBerry Dynamics apps included in app groups that you add to device groups will not be assigned to users.

If your environment supports Android Enterprise, you can't add Android apps that have an optional disposition to device groups. Google Play for Work can assign apps only to Google User IDs, not to device IDs. If you add Android apps that have a required disposition to a device group, the apps will be installed, but the apps will not be listed in Google Play for Work.

8. Click **Save**.

After you finish:

- Activate a shared device.
- To make changes to the shared device group, see Manage a shared device group.

Activate a shared device

Before users can check out shared devices, you must activate them. The User privacy - User enrollment activation type is not supported.

Before you begin: Verify that the BlackBerry Dynamics profile that is assigned to the shared device group does not have the "Enable UEM Client to enroll in BlackBerry Dynamics" option selected. Verify that the same profile is also assigned to the user account that owns the shared device group.

1. In the management console, on the menu bar, click **Dedicated devices > Shared device groups**.
2. Search for and click the name of a shared device group.
3. To get the server address and device activation credentials that you use to activate the device, click **Device activation**.
4. To activate the device, follow the instructions on the screen.

After you finish: Verify that the activated device is displayed in the **Shared devices** section. To generate a device name, BlackBerry UEM adds a number to the group name. For example, if the group name is Example, the first device that you activate is named Example 01.

Manage a shared device group

Before you begin: Create a shared device group.

1. In the management console, on the menu bar, click **Dedicated devices > Shared device groups**.
2. Search for and click the name of the shared device group that you want to manage.
3. Do any of the following:

Task	Steps
Display only the BlackBerry UEM Client login screen when the device is checked in.	a. Click ✎. b. Select the **Enable UEM Client app lock** check box. c. Click **Save**.
Edit the user membership of a shared device group.	a. Navigate to the **Granted users** section. b. To add a user to the group, search for and click the name of the user. c. To remove a user from the group, in the **Action** column, click ✕.

Task	Steps
Assign an IT policy or a profile to a shared device group.	You can assign an IT policy and profiles to a shared device group that apply either when the device is checked in or when the device is checked out by a user. To have the same IT policy or profile apply whether the device is checked in or out, you can assign it for both states. If the assigned IT policy or profile is different for each state, the appropriate policy and profiles are applied whenever the device is checked in or out. **a.** On the **Checked-out settings** tab, in the **Assigned IT policy and profiles** section, click +. **b.** Click **IT policies** or a profile type. **c.** In the drop-down list, click the name of the IT policy or profile that you want to assign to devices when they are checked out. **d.** Click **Assign** or **Replace**. **e.** On the **Checked-in settings** tab, repeat the steps to assign an IT policy and profiles that apply to the shared devices when they are checked in.
Assign an app to a shared device group.	You can assign apps or app groups to a shared device group that are made available either when the device is checked in or when the device is checked out by a user. To have apps remain on the device at all times, you can assign them for both states. Assigned apps available only in one state are added or removed appropriately whenever the device is checked in or out. Before you follow the steps below, add the app to the available app list or create app groups. **a.** On the **Checked-out settings** tab, in the **Assigned apps** section, click +. **b.** Search for and select the app or app group that you want to assign. **c.** Click **Next**. **d.** Configure the app disposition, per app-VPN, app configuration, and track as necessary. **e.** Click **Next**. **f.** Select **Yes** if you want to assign a license to the app and configure the license settings as necessary. Select **No** if you do not want to assign a license or you do not have a license to assign to the app. **g.** Click **Assign**. Users must follow the instructions to enroll in your organization's VPP on their devices before they can install prepaid apps. Users have to complete this task once. **h.** On the **Checked-in settings** tab, repeat the steps to assign apps or app groups that should remain installed on the device when the device is checked in.
Remove a device from a shared device group.	**a.** In the **Shared devices** section, in the **Action** column, click ×. **b.** Click **Delete only work data**.

Task	Steps
Delete a shared device group.	**a.** Remove all the devices from the shared device group. **b.** Click  . **c.** Click **Delete**.

Creating and managing public device groups

A public device is a single-purpose device that is locked to a specific set of applications to perform that purpose. This feature is supported for iOS and Android Enterprise devices.

A public device group must be assigned an app lock mode profile and a supported activation profile. For Android Enterprise, the activation type must be Work space only (Android Enterprise fully managed device). For iOS, the device must be a supervised iOS device with MDM controls.

Create a public device group

1. In the management console, on the menu bar, click **Dedicated devices > Public device groups**.
2. Click +.
3. Type a name and a description for the public device group.
4. Type the username for device activation.
5. To assign an app or app group to the group, in the **Assigned apps** section, click + and do the following:
   a) Search for and select the app that you want to assign to the group.
   b) Click **Next**.
   c) For iOS or Android apps, to require users to follow the actions defined for apps in the compliance profile assigned to them, in the **Disposition** drop-down list, select **Required**.

      If the app group supports Android Enterprise, the disposition must be **Required**.
   d) To allow users to install and uninstall the app, in the **Disposition** drop-down list, select **Optional**.
   e) For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list, select the settings to associate with the app or app group.
   f) If available, for iOS and Android devices, select an app configuration to assign to the app.
   g) If you use Android Enterprise and have created tracks for apps in the Google Play console, select a track to assign to the app.
6. Click **Assign**.

   You can't add BlackBerry Dynamics apps to device groups because entitlements can be granted to users only. Any BlackBerry Dynamics apps included in app groups that you add to device groups will not be assigned to users.

   If you support Android Enterprise, you can't add Android apps that have an optional disposition to device groups. Google Play for Work can assign apps only to Google user IDs, not to device IDs. If you add Android apps that have a required disposition to a device group, the apps will be installed, but the apps will not be listed in Google Play for Work.
7. Click **Save**.

After you finish:

- Create an app lock mode profile and assign it to the public device group.
- Create an activation profile and assign it to the public device group. The activation type for Android Enterprise must be Work space only (Android Enterprise fully managed device). The activation type for iOS must be a supervised iOS device with MDM controls.
- Activate a public device.
- To delete a public device group, select the check box next to the group that you want to delete and click 🗑.

Activate a public device

Before you begin: Create a public device group.

1. In the management console, on the menu bar, click **Dedicated devices > Public device groups**.
2. Search for and click the name of a public device group.
3. To get the server address and activation credentials that you use to activate the device, click **Device activation**.
4. To activate the device, follow the instructions on the screen.

After you finish: Verify that the activated device is displayed in the **Public devices** section. To generate a device name, BlackBerry UEM adds a number to the group name. For example, if the group name is Example, the first device that you activate is named Example 01.

Manage a public device group

Before you begin: Create a public device group.

1. In the management console, on the menu bar, click **Dedicated devices > Public device groups**.
2. Search for and click a public device group.
3. Do any of the following:

Task	Steps
Assign an IT policy, profile, or app to a public device group.	**a.** In the appropriate section, click +. **b.** Select the IT policy, profile, or app that you want to assign. Follow the prompts and select the appropriate settings to complete the assignment. **c.** To remove an IT policy, profile, or app, beside the property that you want to delete, click ×.
Remove a device from a public device group.	In the **Public devices** section, in the **Action** column, click × for the device.

Creating and managing shared iPad groups

When you create a shared iPad group, users can sign in to a shared iPad with their managed Apple ID, allowing them to use common apps and bookmarks while maintaining and synchronizing separate user details.

Note the following requirements:

- The iPad device must be a supervised, MDM enrolled device.
- The iPad device must be enrolled in DEP.
- The iPad device must be using a supported iPadOS version.

This feature does not support BlackBerry Dynamics apps. You must verify that the "Enable UEM Client to enroll in BlackBerry Dynamics" option is not selected in the BlackBerry Dynamics profile.

Create a shared iPad group

1. In the management console, on the menu bar, click **Dedicated devices > Shared iPad groups**.
2. Click +.
3. Type a name and description for the shared iPad group.
4. Type the username for device activation.
5. To assign an app or app group to the group, in the **Assigned apps** section, click + and do the following:
   a) Search for and click the app that you want to assign to the group.
   b) Click **Next**.
   c) To require users to follow the actions defined for apps in their assigned compliance profile, in the **Disposition** drop-down list, select **Required** or **Required without updates**.
   d) To assign per-app VPN settings to the group, in the **Per app VPN** drop-down list for the group, select the settings to associate with the group.
   e) If available, select an app configuration to assign to the app.
   f) Click **Assign**.
6. Click **Save**.

After you finish:

- Optionally, Create a shared iPad profile.
- Activate a shared iPad device.
- To make changes to a shared iPad group, see Manage a shared iPad group.

Create a shared iPad profile

Optionally, you can create and assign a shared iPad profile to configure how users can use a shared iPad device.

Before you begin: Create a shared iPad group.

1. In the management console, on the menu bar, click **Policies and profiles > Policy > Shared iPad**.
2. Click +.
3. Type a name and description for the shared iPad profile.
4. In the **Quota size** field, specify, in MB, the size of the quota for each user on the shared device. This setting takes precedence over the "Resident users" setting.
5. In the **Resident users** field, specify the number of users to partition the remaining device space for.

6. If you want the device to use guest mode only, select the **Temporary session only** option.
7. In the **Temporary session timeout** field, specify, in seconds, the timeout for a temporary session.
8. In the **User session timeout** field, specify, in seconds, the timeout for a regular session.
9. Click **Save**.

After you finish:

- Assign the profile to the shared iPad group.
- Activate a shared iPad device.

Activate a shared iPad device

Before you begin:

- Create a shared iPad group. Optionally, Create a shared iPad profile.
- Create a DEP configuration with the "Enable Shared iPad mode" option selected and assign it to a DEP activated iPad device.
- Wipe the iPad device.
- Verify that the BlackBerry Dynamics profile that is assigned to the shared iPad group does not have the **Enable UEM Client to enroll in BlackBerry Dynamics** option selected. Verify that the same profile is also assigned to the user account that owns the shared iPad group.

1. In the management console, on the menu bar, click **Dedicated devices > Shared iPad groups**.
2. Search for and click the name of a shared iPad group.
3. To get the activation credentials that you use to activate the device, click **Device activation**.
4. To activate the device, follow the device activation instructions on the screen.

After you finish: To remove a device from a shared iPad group, click the name of the group that you want to remove the device from. On the **Device details** screen, click **Remove device** or **Delete all device data**.

Manage a shared iPad group

Before you begin: Create a shared iPad group.

1. In the management console, on the menu bar, click **Dedicated devices > Shared iPad groups**.
2. Search for and click a shared iPad group.
3. Do any of the following:

Task	Steps
Assign an IT policy or profile to a shared iPad group.	a. In the **Assigned IT policy and profiles** section, click +. b. Click **IT policies** or a profile type. c. In the drop-down list, click the name of the IT policy or profile that you want to assign. d. Click **Assign** or **Replace**.

Task	Steps
Assign an app to a shared iPad group.	You can't add BlackBerry Dynamics apps to shared iPad groups because entitlements can be granted to users only. Any BlackBerry Dynamics apps included in app groups that you add to shared iPad groups will not be assigned to users. Only app store VPP or internal iOS apps are supported, as well as iOS app shortcuts. Non-VPP store apps are not supported. **a.** In the **Assigned apps** section, click +. **b.** Search for and select the app or app group that you want to assign. **c.** Click **Next**. **d.** Click **Next** again. **e.** Assign a VPP app license to the device for each app. **f.** Click **Assign**.

Managing Chrome OS devices in BlackBerry UEM

You can integrate Chrome OS with the BlackBerry UEM management console to extend the ability to perform some administrative tasks in UEM. You continue to enroll Chrome OS devices and perform some administrative tasks in your Google admin console. When you integrate Chrome OS with UEM, it sorts the organizational units from Google Admin console into UEM organizational unit groups. When a change to an organizational unit, a user, or a device is made in the Google domain, UEM updates its database accordingly.

For more information about configuring UEM to support Chrome OS devices, see Extending the management of Chrome OS devices to BlackBerry UEM.

Manage Chrome OS devices

Before you begin: Extend the management of Chrome OS devices to BlackBerry UEM.

Do any of the following:

Task	Steps
View Org units for Chrome OS users.	**a.** In the management console, on the menu bar, click **Users > All users**. **b.** Search for and click a Chrome OS user. **c.** The Org unit that the user belongs to is displayed at the top of the page. You can click the name of the Org unit to view its current settings.
Edit an Org unit.	The information that is displayed for Org units replicates what you have configured in the Google admin console. You can edit certain fields in an Org unit, but many of the settings can be changed only in the Google admin console. **a.** In the management console, on the menu bar, click **Groups > Org unit**. **b.** Click the Org unit that you want to edit. **c.** Make the necessary changes. **d.** Click **Save**.

Task	Steps
Send commands to Chrome OS devices.	**a.** In the management console, on the menu bar, click **Users > All users**. **b.** Search for and click a Chrome OS user. **c.** In the **Manage device** section, click one of the following commands: • View device report: This command displays detailed information about the device. • View device actions: This command displays any actions that are in progress on the device. • Disable device: This command disables the device. Note that the user cannot re-enable the device after an administrator has disabled it. • Enable device: This command enables the device. • Delete all device data: This command deletes all user information and app data and returns the device to factory default settings. • Delete only work data: This command deletes work data and deprovisions the device. • Remove device: This command deprovisions the device.

Set up BlackBerry UEM Self-Service

BlackBerry UEM Self-Service is a web-based application that allows device users to perform management tasks such as creating activation passwords, remotely locking their devices, or deleting data from their devices. To use UEM Self-Service, you must provide the web address and login information to users.

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

After you finish:

- Provide the BlackBerry UEM Self-Service web address and login information to users.
- To create and manage user roles for UEM Self-Service, see Managing user roles for BlackBerry UEM Self-Service.

Managing user roles for BlackBerry UEM Self-Service

User roles allow you to specify the capabilities that are available to users in BlackBerry UEM Self-Service. BlackBerry UEM includes one preconfigured Default user role. The Default user role is set up to allow all UEM Self-Service features, and it is assigned to the "All users" group.

Note: Renaming, deleting, or removing the Default user role from the "All users" group can cause issues with the Work Apps app on iOS devices.

If you want to restrict certain features for users, you can create new user roles or edit an existing user role. You can assign user roles to groups or directly to users.

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

BlackBerry UEM Self-Service capabilities

Feature	Description
Specify an activation password	Users can create a password that they can use to activate their devices with BlackBerry UEM. You can configure the default password expiration period and the required password complexity at Settings > Self-Service > Self-Service settings.
Specify access key	Users can create access keys that they can use to activate BlackBerry Dynamics apps.
Delete only work data	Users can send the "Delete only work data" command to a device. The command deletes work data including the IT policy, profiles, apps, and certificates.
Delete all device data	Users can send the "Delete all device data" command to a device. The command deletes all user information and app data that the device stores, including information in the work space. It returns the device to factory default settings and deletes the device from UEM.
Locate device	Users can view the location of their iOS or Android devices on a map. This feature requires that a location service profile is assigned to the user. For more information, see Using location services on devices.
Manage user certificates	Users can upload user certificates for their devices. You can provide instructions to users about the certificates they need and where to upload the certificates from.
Lock and unlock BlackBerry Dynamics apps	If users' devices are enabled for BlackBerry Dynamics, users can lock BlackBerry Dynamics apps that are installed on their devices and can generate unlock keys to unlock the apps. When a user locks an app, it prevents anyone from opening it.
Delete BlackBerry Dynamics app data	If users' devices are enabled for BlackBerry Dynamics, users can delete all data from a BlackBerry Dynamics app that is installed on a device. The command removes all data stored by the app but the app is not deleted.

Create a user role for UEM Self-Service

You can create a custom user role and assign it to users or groups to specify the capabilities that users have in BlackBerry UEM Self-Service.

1. In the management console, on the menu bar, click **Settings > Self-Service > User roles**.
2. Click  .
3. Type a name and description for the user role.
4. To copy permissions from another role, in the **Permissions copied from role** drop-down list, click a role.
5. Select the capabilities that you want the user role to have.
6. Click **Save**.

After you finish:

- Rank user roles as appropriate and save your changes.
- Assign user roles to user groups (Groups > search for and click a group > Managed devices) or to individual users (Users > Managed devices > search for and click a user > Direct role assignment).

Customize the user list

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Do any of the following:

Task	Steps
Set the default or advanced view.	In the upper-right corner, click **Default** or **Advanced**. In larger environments, the advanced view might take longer to display than the default view.
Select the information to display in the user list.	**a.** At the top of the user list, click  . **b.** Choose the columns that you want to include or exclude. To sort the user list by a column, click the column header. To reorder the columns, click and drag a column header.
Filter the user list.	If turn on multiple selection, you can select multiple filters before you apply them, and you can select multiple filters in each category. If multiple selection is off, each filter is applied when you select it, and you can select only one filter in each category. **a.** Click  to turn multiple selection on or off. **b.** Under **Filters**, expand one or more categories. Each category includes only filters that display results and each filter indicates the number of results to display when you apply it. **c.** Select the filters that you want to apply.
Export the user list to a .csv file.	When you export the user list, the file includes all columns that are currently displayed. **a.** Select the user accounts that you want to include in the export. You can select the check box at the top of the user list to select all users. **b.** Click and save the file.
Change the device ownership label.	Each activated device has a label that indicates whether the device is owned by your organization, the user, or not specified. The default value comes from the device ownership setting in the activation profile. You can filter the user list by the device ownership label. Follow the steps below to change the device ownership label for a specific user. If you want to change the label for multiple users, you can send a bulk command. **a.** Search for and click the name of a user account. **b.** In the **Activated devices** section, beside the ownership setting, click **Edit**. **c.** Set the appropriate device ownership label. **d.** Click **Save**.

Legal notice

©2023 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.

Patents, as applicable, identified at: www.blackberry.com/patents.

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