BlackBerry UEM

Managing users and groups

Administration

12.13

Contents

Users and groups

You can create user accounts and create groups of users to help manage users efficiently. The BlackBerry UEM management console manages users for device management, and for other BlackBerry enterprise products, including the following products:

- BlackBerry 2FA
- BlackBerry Enterprise Identity
- BlackBerry Workspaces
- BBM Enterprise
- BlackBerry Org Connect

Creating and managing user accounts

You can add user accounts directly to BlackBerry UEM or, if you connected BlackBerry UEM to your company directory, you can add user accounts from your company directory. For information about connecting BlackBerry UEM to a company directory and enabling directory-linked groups, see the on-premises Configuration content or the Cloud Configuration content.

You can also use a .csv file to add multiple user accounts to BlackBerry UEM at the same time.

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 BlackBerry UEM to a company directory and enabling directory-linked groups, see the on-premises Configuration content or the Cloud Configuration content.
- If you want to enable the BlackBerry Workspaces service for your users, verify that the Workspaces plug-in for BlackBerry UEM is installed on each instance of BlackBerry UEM in your environment. For more information about installing the Workspaces service, contact your Workspaces account representative.

1. On the menu bar, click **Users > Managed devices**.
2. Click **Add user**.
3. Perform one of the following tasks:

Task	Steps
Add a directory user	**a.** On the **Company directory** tab, in the search field, specify the search criteria 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.** In an on-premises environment, click the **Local** tab. In a Cloud environment, click the **Non-directory** tab. **b.** Type the **First name** and **Last name** for the user account. **c.** In the **Display name** field, make changes if necessary. The display name is automatically configured with the first and last name that you specified. **d.** In the **Username** field, enter a unique username for the user account. **e.** 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. **f.** Optionally, click **Additional user details** and fill in the fields as needed.
Add a BlackBerry Online Account user (This option is available only in Cloud environments.)	**a.** Click the **Non-directory** tab. **b.** Type the **First name** and **Last name** for the user account. **c.** In the **Display name** field, make changes if necessary. The display name is automatically configured with the first and last name that you specified. **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.

4. If local groups exist in BlackBerry UEM and you want to add the user account to groups, in the **Available groups** list, select one or more groups and click ➔.

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

   To add a user account to groups that are assigned an administrative role, you must be a Security Administrator.
5. 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.
6. In an on-premises environment, if you add a local user, in the **Account password** field, 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.
7. In the **Enabled services** section, select the **Enable user for device management** option.
8. If the Workspaces plug-in for BlackBerry UEM is installed in the domain, to enable the Workspaces service, perform the following actions:
   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. Click ➔.
9. Perform one of the following tasks:

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. The activation period expiration specifies how long the activation password remains valid. **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 a template to use for the activation email.
Pair an activation password with a specific activation profile.	**a.** In the **Activation option** drop-down list, select **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. The activation period expiration specifies how long the activation password remains valid. **e.** If you want the activation password to be valid only for one device activation, select **Activation period expires after the first device is activated**. **f.** In the **Activation email template** drop-down list, click a template to use for the activation email.

Task	Steps
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, click a template to use for the activation email.
Add user to BlackBerry UEM only.	**a.** In the **Activation option** drop-down list, select **Do not set**.

10. If you use custom variables, expand **Custom variables** and specify the appropriate values for the variables that you defined.
11. Perform one of the following actions:
    - 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 in a .csv file into BlackBerry UEM to create many user accounts at the same time. You can create the .csv file manually using the BlackBerry UEM sample .csv file, which is available for download from the Import tab in the Add a user window.

Depending on your requirements, you can also 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 added to. If you want to assign each user account to a specific user group, you use this column before you import the file.
MDM (BlackBerry UEM)	Specify whether the user is enabled for MDM. To enable a user for MDM, type "Enabled".
Activation password	Enter the activation password. This value is required if the “Activation password generation” value is set to “manual.”
Activation template	Enter 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.

Column Header	Description
Activation password expiration	Enter the number of seconds the activation password exists before it expires.
Activation password generation	Enter one of the following: • Auto. The activation password is automatically created and sent to the user. • Manual. The activation password is set in the "Activation password" column. • Ignore. No activation password is generated. If the value is left blank, the default is Auto.
Send activation email	Enter one of the following: • True. The activation email is sent to the user. • False. The activation email is not sent to the user. If the “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.
User type	This column is required whenever the .csv file includes both local and directory user accounts. Enter one of the following: • L for local user accounts • D for directory user accounts The entries are not case-sensitive.
Directory UID	(Optional) An alternative to entering the email address for directory user accounts. By default, the email address is used to validate the directory user accounts; however, you can specify that the directory UID be 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.

To see an example of the .csv file, in the UEM administration console, click **Users > All users > Add user > Import > Download sample .csv file**.

Add user accounts using a .csv file

Before you begin:

- If the .csv file contains directory user accounts, verify that BlackBerry UEM is connected to your company directory.
- Verify that the number of columns match the number of headers in the .csv file.
- Verify that the required columns are included.
- Verify that the information in the columns is correct.

1. On the menu bar, click **Users**.
2. Select the **All users** or **Managed devices** tab.

3. Click **Add user**.
4. Click the **Import** tab.
5. Click **Browse** and navigate to the .csv file that contains the user accounts that you want to add.
6. Click **Load**.
7. If errors are reported, perform the following actions:
   a) Correct the errors in the .csv file.
   b) Click **Browse** and navigate to the .csv file.
   c) Click **Load**.
   d) Repeat step 6 until all errors are corrected.
8. If the .csv file does not use the "Group membership" column and local groups exist in BlackBerry UEM, perform the following actions if you want to add user accounts to groups:
   a) In the **Available groups** list, select one or more groups and click ➔.
   b) Click **Next**.

   When you import the .csv file, all 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 BlackBerry UEM and your company directory occurs.

   To add user accounts to groups that are assigned an administrative role, you must be a Security Administrator.
9. Review the list of user accounts and perform one of the following actions:
   - To correct the errors for any invalid directory user accounts, click **Cancel** and go to step 6.
   - To add the valid user accounts, click **Import**. Any invalid directory user accounts are ignored.

How BlackBerry UEM validates the user accounts .csv file

BlackBerry UEM validates the user accounts .csv file before, during, and immediately after it loads the .csv file and reports any errors that it encounters.

The following are some of the errors that will prevent BlackBerry UEM from loading the .csv file:

- An invalid file format or file extension
- No data in the file
- The number of columns does not match the number of headers in the file

When BlackBerry UEM encounters an error, it stops loading the file and displays an error message. You must correct the error and then reload the .csv file.

After the .csv file is loaded, BlackBerry UEM displays a list of user accounts that will be imported and, if applicable, any directory user accounts that will not be imported as a result of an error (for example, a duplicate entry or invalid email address). You can do one of the following:

- Cancel the operation, correct the errors, and then reload the .csv file.
- Continue and load the valid user accounts. The directory user accounts with errors are not loaded. You must copy and correct the directory user accounts that were not loaded in a separate .csv file. Otherwise, reloading the same .csv file will result in duplication errors for the user accounts that were successfully loaded.

BlackBerry UEM performs a final validation on the imported user accounts just before it creates the user accounts to ensure that no errors have been introduced as the file was being imported (for example, another administrator created a user account just as a .csv file containing that same user account was being imported).

View a user account

You can view information about a user account on the Summary tab. For example, you can view the following information:

- Activated devices
- User groups that a user account belongs to
- Assigned IT policy, profiles, and apps
- Client certificates added to user accounts directly and through user credential profiles

1. On the menu bar, click **Users**.
2. Search for a user account using one of the following options:
   - Click **All users**, and type in the **Search** field.
   - Click **Managed devices > User search** and type in the search field.
3. In the search results, click the name of the user account.

Add notes to a user account

You can add notes to keep track of any information related to a specific user account. The note information is stored with the user account and not with an individual device. If the user is removed, the information in the notes field is also removed. Using the notes feature is controlled by the "Edit users" permission for administrators.

1. On the menu bar, click **Users**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. Click the **Add note** icon in the upper right hand corner.
5. Type notes in the dialog box that opens. The notes that you type are automatically saved and the icon changes to indicate that there are notes saved.

Manage multiple user accounts at one time

You can complete certain actions for multiple users at one time. For example, you can send an email to a selected group of users.

1. On the menu bar, click **Users > Managed devices**.
2. If necessary, Filter the user list.
3. Perform one of the following actions:
   - Select the check box at the top of the user list to select all users.
   - Select the check box for each user that you want to include in the file. You can use Shift+click to select multiple users.
4. From the menu, click one of the following icons:

Icon	Description
	Send an email to users

Icon	Description
	Send an activation email to multiple users
	Add users to user groups
	Export the user list to a .csv file
	Send a BlackBerry UEM Self-Service password to multiple users

Send an email to users

You can send an email to one or more users directly from the management console. The users must have an email address associated with their account.

If you have an on-premises environment, you can configure the email address that the email is sent from in the SMTP server settings.

Before you begin: To send an email to multiple users, you must be assigned an administrative role that has the "Send email to users" permission.

1. On the menu bar, click **Users**.
2. Select the **All users** or **Managed devices** tab.
3. Perform one of the following tasks:

Task	Steps
Send an email to one user	**a.** Search for a user account. **b.** In the search results, click the name of the user account. **c.** Click  . **d.** Optionally, click **CC** and enter one or more email addresses (separated by commas or semicolons) to copy the email to yourself or others.
Send an email to multiple users	**a.** Select the check box for each user that you want to send an email to. **b.** Click  . **c.** Optionally, click **To** or **CC** and enter one or more email addresses (separated by commas or semicolons) to send or copy the email to yourself or others.

4. Enter a subject and message.
5. Click **Send**.

Send a BlackBerry UEM Self-Service password to multiple users

You can send a UEM Self-Service password to multiple users at one time. The passwords are randomly generated, and an email message containing a password is sent to each user.

If you have an on-premises environment, you can configure the email address that the email is sent from in the SMTP server settings.

1. On the menu bar, click **Users > Managed devices**.
2. Select the users that you want to send the UEM Self-Service password to. Note that users must have an email address associated with their accounts.
3. Click .
4. Click **Continue**.

Edit user account information

You can edit the following user information:

- Name, username, display name, and email address
- Group membership (membership to directory-linked groups cannot be changed)
- Account password for local user accounts
- User role
- If you defined custom variables, you can edit the variable information

Note: You cannot edit the user details for the default administrative user or for users that use their BlackBerry Online account credentials.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Click .
5. Edit the user account information.
6. Click **Save**.

Synchronize information for a directory user

If you have added a user account from your company directory, you can manually synchronize that user's information with your company directory at any time instead of waiting for the automatic synchronization time.

1. On the menu bar, click **Users**.
2. Select the **All users** or **Managed devices** tab.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click .

Remove services from a user

If BlackBerry UEM is enabled for one or more value-added services, and a user is enabled for a service, you can remove the service from a user. You can also remove MDM controls, without deleting the user account from BlackBerry UEM.

Before you begin:

- Before you can remove MDM controls, you must remove activated devices from a user.
- Before you can remove the Enterprise Identity service, you must remove all Enterprise Identity assignments.

1. On the menu bar, click **Users > All users**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Click ⛔.
5. Perform any of the following tasks:

Task	Steps
Remove MDM services	**a.** Click ⛔ on Managed devices. **b.** Click **Save**.
Remove Workspaces servi	**a.** Click ⛔ on Workspaces. **b.** Select one of the following options: • Delete all files owned by this user and revoke memberships from all workspace groups and distribution lists • Transfer this user's files and membership in workspace groups and distribution lists to a different email address. In the **Email address** field, type a contact email address. A new user account is created if the email address is not associated with an existing user account. **c.** Click **Remove**.
Remove Enterprise Identity service	**a.** Click ⛔ on Enterprise Identity. **b.** Click **Save**.

After you finish: To enable a service, see Enable services for a user.

Enable services for a user

If BlackBerry UEM is enabled for one or more value-added services, you can enable a service for a user.

1. On the menu bar, click **Users > All users**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Perform any of the following tasks:

Task	Steps
Enable MDM services	**a.** Click + on Managed devices. **b.** If local groups exist in BlackBerry UEM and you want to add the user account to groups, in the **Available groups** list, select one or more groups and click ➔. **c.** Choose an option for the device activation password. **d.** Click **Save**.

Task	Steps
Enable the Workspaces service	**a.** Click + on Workspaces. **b.** Assign Workspaces roles. **c.** Click **Save**.
Enable the Enterprise Identity service	**a.** Click + on Enterprise Identity. **b.** Select app groups. **c.** Click **Assign**.

Delete a user account

When you delete a user account, the work data is also deleted from all of the user's devices.

Before you begin:

- Deactivate any devices that are associated with the user account that you want to delete.
- Remove any services that are associated with the user account that you want to delete. For more information, see Remove services from a user.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, select the name of a user account.
4. Click .
5. Click **Delete**.

Add users to user groups

Note: To add a user that is assigned an administrative role to a user group, you must be a Security Administrator.

1. 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 .

   Note: Membership to directory-linked groups cannot be changed.
5. Click **Save**.

Remove a user from a user group

You cannot remove a user from a directory-linked group.

Note: To remove a user that is assigned an administrative role from a user group, you must be a Security Administrator.

1. On the menu bar, click **Groups**.
2. Search for the user group you want to edit.

3. Click the user group.
4. Search for the user you want to remove.
5. Select the user.
6. Click  .

Change which user groups a user belongs to

Note: To change which user groups a user that is assigned an administrative role belongs to, you must be a Security Administrator.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. In the **Group membership** section, click  .
5. Perform any of the following actions:
   - To add the user to user groups, in the **Available groups** list, select one or more groups and click  .
   - To remove the user from user groups, in the **Member of groups** list, select one or more groups and click  .

   Note: Membership to directory-linked groups cannot be changed.
6. Click **Save**.

Assign a profile or IT policy to a user account

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. In the **IT policy and profiles** section, click  .
5. Click **IT policy** or a profile type.
6. In the drop-down list, click the name of the profile or IT policy that you want to assign to the user.
7. For IT policies and ranked profile types, if the profile type that you selected in step 5 is already assigned directly to the user, click **Replace**. Otherwise, click **Assign**.

Assign an app to a user account

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

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

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

Before you begin:

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

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. In the **Apps** section, click +.
5. Select the check box beside the apps or app group that you want to assign to the user account.
6. Click **Next**.
7. In the **Disposition** drop-down list for the app, perform one of the following actions:
   - To require users to install the app, select **Required**.
   - To permit users to install and remove the app, select **Optional**.

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

Assign an app group to a user account

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

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

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

Before you begin: Add the apps to an app group.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. In the **Apps** section, click +.
5. Select the check box beside the apps or app group that you want to assign to the user account.
6. Click **Next**.
7. In the **Disposition** drop-down list for the app, perform one of the following actions:
   - To require users to install the app, select **Required**.
   - To permit users to install and remove the app, select **Optional**.

   Note: If the same app is assigned to a user account, a user group that the user belongs to, and the device group the device belongs to, the disposition of the app assigned in the device group takes precedence.
8. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
9. If you are adding an iOS app, perform one of the following tasks:

Task	Steps
If you have not added a VPP account or you are not adding an iOS app	**a.** Click **Assign**.
If you are adding an iOS app and you have added at least one VPP account	**a.** Click **Next**. **b.** Select **Yes** if you want to assign a license to the iOS app. Select **No**, if you do not want to assign a license or you do not have a license to assign to the app. **c.** If you have assigned a license to the app, in the **App license** drop-down list, select the VPP account to associate with the app. **d.** In the **Assign license to** drop-down list, assign the license to the **User** or **Device**. If no value is specified in the **App license** drop-down list, the **Assign license to** drop-down list is not available. **e.** 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 **Note:** If you grant access to more licenses than you have available, the first users who access the available licenses can install the app. If the app is a required app that does not have an available license, you must obtain the license before the user can install the app or be subject to any compliance rules that you have assigned to the user.

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. You can assign an IT policy, profiles, and apps in the management console when you create or update the settings for a user group.

You can create two types of user groups:

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

After you create user groups, you can define a group as a member of another group. For more information, see Add nested groups to a user group.

Creating directory-linked groups

You can create groups in BlackBerry UEM that are linked to one or more groups in your company directory. These BlackBerry UEM groups are called "directory-linked groups." Only directory user accounts can be members of a directory-linked group.

At a scheduled interval, BlackBerry UEM automatically synchronizes the membership of a directory-linked group with its associated company directory group (or groups). Users that were added or removed from the company directory group are added or removed from the directory-linked group.

Note: When users are moved into a company directory group that is linked to a directory-linked group, they are assigned the policies, profiles, and apps that are assigned to the group. When users are removed from a company directory group that is linked to a directory-linked group, the policies, profiles, and app are removed from the user.

Each directory-linked group can link to only a single company directory. For example, if BlackBerry 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.

To enable this feature, see "Enable directory-linked groups" in the on-premises Configuration content or the cloud Configuration content.

Synchronizing directory-linked groups does not add or delete users in BlackBerry UEM. To allow BlackBerry UEM to create user accounts when new company directory users are created, you must enable and configure onboarding. For more information, see "Enabling onboarding" in the on-premises Configuration content or the cloud Configuration content.

Create a directory-linked group

Before you begin: Enable directory-linked groups. For instructions, see "Enable directory-linked groups" in the on-premises Configuration content or the cloud Configuration content.

1. On the menu bar, click **Groups**.
2. Click  .
3. Type the group name.
4. In the **Linked directory groups** section, perform the following actions:
   a) Click +.

b) Type the name or partial name of the company directory group 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 in the search results list.
f) Click **Add**. The company directory group displays in the list and the company directory connection the group is linked to displays beside the section title.
g) If necessary, select the **Link nested groups** check box. You can leave the check box unselected to link to all nested groups, or you can select the check box to allow the directory settings to control the number of nested groups.
h) Repeat these steps to link additional groups.

5. To assign a user role to the directory-linked group, perform the following actions:
   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**.
6. To assign an IT policy or profile to the directory-linked group, perform the following actions:
   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**.
7. To assign an app to the directory-linked group, in the **Assigned apps** section, click +.
8. Search for the app.
9. In the search results, select the app.
10. Click **Next**.
11. In the **Disposition** drop-down list for the app, perform one of the following actions:
    - To install the app automatically on devices, and to prevent users from removing the app, select **Required**. This option is not available for BlackBerry apps.
    - To permit users to install and remove the app, select **Optional**.
12. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
13. Click **Assign**.
14. Click **Add**.

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

1. On the menu bar, click **Groups**.
2. Click the directory-linked group.
3. Click the **Settings** tab.
4. Click .
5. In the **Linked directory groups** section, click +.
6. Type the company directory group name.
7. Click **Search**.
8. Select the company directory group in the search results list.
9. Click **Add**.

10. If required, select **Link nested groups**.

Create a local group

1. On the menu bar, click **Groups**.
2. Click  .
3. Type a name for the user group.
4. Optionally, type a description for the user group.
5. To assign a user role to the local group, perform the following actions:
   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**.
6. To assign an IT policy or profile to the local group, perform the following actions:
   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**.
7. To assign an app to the user group, in the **Assigned apps** section, click +.
8. Search for the app.
9. In the search results, select the app.
10. Click **Next**.
11. In the **Disposition** drop-down list for the app, perform one of the following actions:
    - To install the app automatically on devices, and to prevent users from removing the app, select **Required**. This option is not available for BlackBerry apps.
    - To permit users to install and remove the app, select **Optional**.

      Note: 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.
12. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
13. Click **Assign**.
14. When you are finished specifying the user group properties, click **Add**.

View a user group

1. On the menu bar, click **Groups**.
2. Search for a user group.
3. In the search results, click the name of the user group.
4. To view the members of a user group, perform the following actions:
   a) Click **Users** to view the assigned user accounts.
   b) Click **Nested groups** to view the assigned nested groups.
5. Click **Settings** to view the following information about a user group:
   - Linked directory groups (available for a directory-linked group)

- Assigned IT policy, profiles, and apps

Change the name of a user group

1. On the menu bar, click **Groups**.
2. Search for the user group you want to view.
3. Click the user group.
4. Click .
5. Change the name of the user group.
6. Optionally, change the description of the user group.
7. Click **Save**.

Delete a user group

When you delete a user group, the users in the group are not deleted. The group properties that are assigned to the user are removed or changed.

1. On the menu bar, click **Groups**.
2. Search for the user group that you want to delete.
3. Click the user group.
4. Click .
5. Click **Delete**.

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.vWhen you add a nested group to a user group, any groups that belong to the nested group are also added.

1. On the menu bar, click **Groups**.
2. Search for a user group.
3. In the search results, click the name of the user group.
4. Click the **Nested groups** tab.
5. Click .
6. Select one or more available groups.
7. Click **Add**.

Remove nested groups from a user group

You can remove nested groups that are assigned directly to a user group.

1. On the menu bar, click **Groups**.
2. Search for a user group.

3. In the search results, click the name of the user group.
4. Click the **Nested groups** tab.
5. Click ✕ beside each nested group that you want to remove.

Assign a profile or IT policy to a user group

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

Assign an app to a user group

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

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

Before you begin:

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

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

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

Assign an app group to a user group

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

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

Before you begin:

- Add the apps to an app group.

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

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

Task	Steps
If you have not added a VPP account or you are not adding an iOS app	**a.** Click **Assign**.

Task	Steps
If you are adding an iOS app and you have added at least one VPP account	**a.** Click **Next**. **b.** Select **Yes** if you want to assign a license to the iOS app. Select **No**, if you do not want to assign a license or you do not have a license to assign to the app. **c.** If you have assigned a license to the app, in the **App license** drop-down list, select the VPP account to associate with the app. **d.** In the **Assign license to** drop-down list, assign the license to the **User** or **Device**. If no value is specified in the **App license** drop-down list, the **Assign license to** drop-down list is not available. **e.** 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. **Note:** If you grant access to more licenses than you have available, the first users who access the available licenses can install the app. If the app is a required app that does not have an available license, you must obtain the license before the user can install the app or the user will be subject to any compliance rules that you have assigned to the user.

Creating 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 whether the device is owned by your organization or by the user. BlackBerry UEM automatically moves devices into or out of the device group based on the device attributes that you define.

You can use device groups to apply different sets of policies, profiles, and apps to specific devices assigned to various individual users. For example, you can use a device group to apply a specific IT policy to all devices running BlackBerry 10 OS, or to all HTC EVO devices running Android OS 7.0 or later on the T-Mobile network.

Policies, profiles, and apps assigned to a device group take priority over those assigned to a user or a user group. However, you cannot assign activation profiles or user certificates to device groups.

Create a device group

1. On the menu bar, click **Groups > Device**.
2. Click  .
3. Type a name for the device group.
4. In the **Scope to user groups** section, you can select one or more 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, click **Any** or **All**.

   If you select **All**, devices must match all the attributes you define to be included in the device group. If you select **Any**, devices need to match only one of the attributes you define to be included in the device group.
6. In the **Device query** section, perform the following actions:
   - In the **Attribute** drop-down list, click an attribute.
   - In the **Operator** drop-down list, click an operator.
   - In the **Value** drop-down list, click or type a value.

   You can add or remove rows to focus your query.
7. Click **Next**.
8. To assign an IT policy or profile to the device group, perform the following actions:
   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**.
9. To assign an app or app group to the device group, in the **Assigned apps** section, click +.

   Note: 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.

   Note: You can't add Android apps that have an optional disposition to device groups in a BlackBerry UEM environment that supports Android Enterprise. Google Play for Work cannot assign apps to device IDs. Google Play for Work can assign apps only to Google User 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.
10. Search for the app.

11. In the search results, select the app.
12. Click **Next**.
13. In the **Disposition** drop-down list for the app or app group, perform one of the following actions:
    - If the app is an iOS or Android app: To require users to follow the actions defined for apps in the compliance profile assigned to them, select **Required**.
    - If the app is an internal BlackBerry 10 app: To automatically install an internal app on assigned devices, select **Required**. This option is only available for internal BlackBerry 10 apps. Apps added from the BlackBerry World storefront can only be optional.
    - If the app group supports Android Enterprise, the disposition can only be set as required.
    - To permit users to install and remove the app, select **Optional**.

      Note: The same app can be assigned directly to the user account, or inherited from user groups or device groups. The settings for the app (for example, whether the app is required) are assigned based on priority: device groups take precedence over user accounts and user groups.
14. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
15. For iOS and Android devices, if there is an available app configuration, select the app configuration to assign to the app.
16. Click **Assign**.
17. When you are finished specifying the device group properties, click **Save**.

Edit a device group

1. On the menu bar, click **Groups > Device**.
2. Click the name of a device group that you want to edit.
3. Click .
4. Make the necessary edits.
5. Click **Save**.

Defining 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	In the text field, type the name of a service provider, such as T-Mobile or Bell.
BlackBerry Dynamics	• = • !=	In the drop-down list, choose one of the following options: • Disabled • Enabled

Attribute	Operators	Values
Manufacturer	• = • != • Starts with	In the text field, type the name of a device manufacturer, such as Apple or BlackBerry.
Model	• = • != • Starts with	In the text field, type the name of a device model, such as iPhone 5S or BlackBerry Classic.
OS	• = • !=	In the drop-down list, choose one of the following options: • Android • BlackBerry 10 • Chrome • iOS • macOS • Windows
OS version	• = • != • >= • <=	In the text field, type an OS version, such as 7.1.1 or 10.3. If you use this attribute, you should also specify the OS attribute.
Ownership	• = • !=	In the drop-down list, choose one of the following options: • Work • Personal • Not specified
Activation type	• = • !=	In the drop-down list, choose an activation type. The list contains the same activation types that are available for assignment in your activation profiles.
Knox Workspace	• = • != • Starts with	In the text-field, type a Samsung Knox Workspace version, such as 2.2.

View a device group

1. On the menu bar, click **Groups > Devices**.
2. Search for the device group you want to view.
3. Click the device group.
4. Perform one of the following actions:
   - To view the devices assigned to the device group, click the **Devices** tab.
   - To view the user groups, device queries, IT policies, profiles, or apps assigned to the device group, select the **Settings** tab.

Change the name of a device group

1. On the menu bar, click **Groups > Device**.
2. Search for the device group that you want to view.
3. Click the device group.
4. Click .
5. Change the name of the device group.
6. Click **Next**.
7. Click **Save**.

Delete a device group

To be able to delete a device group, you must have permission to manage all of the user groups that the device group has been applied to.

1. On the menu bar, click **Groups > Device**.
2. Search for the device group that you want to view.
3. Click the device group.
4. Click .
5. Click **Delete**.

Creating and managing shared device groups

You can allow multiple users to share an iOS device and configure settings that are specific to each user or the same for all users. You can customize terms of use that users must accept to check out shared devices. A user can check out a device using local or Microsoft Active Directory authentication. When they are done using it, they can check it in and the device is available for the next user. Shared devices remain managed by BlackBerry 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

Note: 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 also to the shared device group. 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. On the menu bar, click **Dedicated devices > Shared device groups**.
2. Click + beside the search bar.
3. Type a name for the shared device group.
4. Optionally, type a description for the shared device group.
5. Type the username for device activation.
6. To require users to accept terms of service when they check out a shared device, perform the following actions:
   a) Select **Enable terms of service**.
   b) Type the terms of service text.
7. In the **Granted users** section, search for a user and click their name in the list of search results.
8. Repeat step 7 for each user that you want to add.
9. Click **Save**.

After you finish: To enable UEM Client app lock, edit the shared device group information.

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. On the menu bar, click **Dedicated devices > Shared device groups**.
2. Search for a shared device group.
3. In the search results, click the name of the shared device group.

4. Click **Device activation** to view the server address and activation username and password.
5. Use the device activation information to activate the device. For more information, see Activating iOS devices.

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

View the check-out history for a user

You can view the list of shared devices that a user has used. Each record indicates the time a device was checked out and checked in and the list displays the last 50 records for a user. The check-out history for a user is updated when they check in a device.

1. On the menu bar, click **Dedicated devices > Shared device groups**.
2. Search for a shared device group.
3. In the search results, click the name of the shared device group.
4. In the **Granted users** section, click **View** in the **Checkout history** column for the user.

Edit the user membership for a shared device group

User membership for a shared device group specifies the list of users granted access to the shared devices activated for the group. Users can belong to one or more shared device groups.

1. On the menu bar, click **Dedicated devices > Shared device groups**.
2. Search for a shared device group.
3. In the search results, click the name of the shared device group.
4. In the **Granted users** section, perform any of the following actions:
   - To add a user to the group, search for the user and click their name in the list of search results.
   - To remove a user from the group, click ✕ in the **Action** column for the user and click **Submit**.
5. Repeat step 4 for each user that you want to add or remove.

Remove a device from a shared device group

When you remove a device from a shared device group, BlackBerry UEM sends the Delete only work data command to the device.

1. On the menu bar, click **Dedicated devices > Shared device groups**.
2. Search for a shared device group.
3. In the search results, click the name of the shared device group.
4. In the **Shared devices** section, perform the following actions:
   a) Click ✕ in the **Action** column for the device.
   b) Click **Delete only work data**.
5. Repeat step 4 for each device that you want to remove.

Delete a shared device group

Before you begin: Remove all devices in the shared device group.

1. On the menu bar, click **Dedicated devices > Shared device groups**.
2. Search for a shared device group.
3. In the search results, click the name of the shared device group.
4. Click  .
5. Click **Delete**.

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 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.

Before you begin:

- If necessary, Create an IT policy.
- If necessary, create profiles. For more information, see the Profiles reference and Using variables in profiles.

1. On the menu bar, click **Dedicated devices > Shared device groups**.
2. Search for a shared device group.
3. In the search results, click the name of the shared device group.
4. Click the **Checked-out settings** tab.
5. In the **Assigned IT policy and profiles** section, click +.
6. Click **IT policies** or a profile type.
7. 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.
8. Perform any of the following tasks:

Task	Steps
Assign an IT policy	**a.** If an IT policy is already assigned directly to the group, click **Replace**. Otherwise, click **Assign**.
Assign a ranked profile type	**a.** If the profile type that you selected in step 5 is already assigned directly to the group, click **Replace**. Otherwise, click **Assign**.
Assign a non-ranked profile type	**a.** Click **Assign**.

9. Click the **Checked-in settings** tab.
10. Repeat steps 5 to 8 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 assign it 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 begin:

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

1. On the menu bar, click **Dedicated devices > Shared device groups**.
2. Search for a shared device group.
3. In the search results, click the name of the shared device group.
4. Click the **Checked-out settings** tab.
5. In the **Assigned apps** section, click +.
6. In the search field, type the app name, vendor, or URL of the app that you want to be available to users when the device is checked out.
7. Select the check box beside the apps or app group that you want to assign to the user group.
8. Click **Next**.
9. In the **Disposition** drop-down list for the app, perform one of the following actions:
   - To require users to install the app, select **Required**.
   - To permit users to install and remove the app, select **Optional**.
10. To assign per-app VPN settings to an app or app group, in the **Per-app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
11. If there is an available app configuration, select the app configuration to assign to the app.
12. Click **Next**.
13. Select **Yes** if you want to assign a license to the app. Select **No** if you do not want to assign a license or you do not have a license to assign to the app.
14. If you have assigned a license to the app, in the **App license** drop-down list, select the VPP account to associate with the app.
15. In the **Assign license to** drop-down list, assign the license to the **User** or **Device**. If no value is specified in the **App license** drop-down list, the **Assign license to** drop-down list is not available.
16. 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.

    Note: If you grant access to more licenses than you have available, the first users who access the available licenses can install the app. If the app is a required app that does not have an available license, you must obtain the license before the user can install the app or the user will be subject to any compliance rules that you have assigned to the user.
17. Click the **Checked-in settings** tab.
18. Repeat steps 5 to 16 to assign apps that should remain installed on the device when the device is checked in.

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. On the menu bar, click **Dedicated devices > Public device groups**.
2. Click + beside the search bar.
3. Type a name for the public device group.
4. Optionally, type a description for the public device group.
5. Type the username for device activation.
6. Click **Save**.

After you finish:

- Create an app lock mode profile and assign it to the public device group.
- Assign the required apps 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.

Note: Android devices must be running Android 9 or later.

Activate a public device

1. On the menu bar, click **Dedicated devices > Public device groups**.
2. Search for a public device group.
3. In the search results, click the name of the public device group for which you want to activate the device.
4. Click **Device activation** to view the server address and activation username and password.
5. Use the device activation information to activate the device. For help with activation, see Activating Android devices or Activating iOS devices.

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

Remove a device from a public device group

1. On the menu bar, click **Dedicated devices > Public device groups**.
2. Search for a public device group.
3. In the search results, click the name of the public device group from which you want to remove a device.
4. In the **Public devices** section, click ✕ in the **Action** column for the device.

5. Repeat step 4 for each device that you want to remove.

Delete a public device group

Before you begin: Remove all devices from the public device group.

1. On the menu bar, click **Dedicated devices > Public device groups**.
2. Search for a public device group.
3. In the search results, select the check box next to the group that you want to delete.
4. Click 🗑
5. Click **Delete**.

Assign an IT policy or a profile to a public device group

Before you begin:

- If necessary, Create an IT policy.
- If necessary, create profiles. For more information, see Profiles reference and Using variables in profiles.

1. On the menu bar, click **Dedicated devices > Public device groups**.
2. Search for a public device group.
3. In the search results, click the name of the public device group to which you want to add an IT policy or profile.
4. In the **Assigned IT policy and profiles** section, click +.
5. Click **IT policies** or a profile type.
6. In the drop-down list, click the name of the IT policy or the profile that you want to assign to the group.
7. Perform any of the following tasks:

Task	Steps
Assign an IT policy	If an IT policy is already assigned directly to the group, click **Replace**. Otherwise, click **Assign**.
Assign a ranked profile	If the profile type that you selected is already assigned directly to the group, click **Replace**. Otherwise, click **Assign**.
Assign a non-ranked profile	Click **Assign**.

Assign an app to a public device group

Before you begin:

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

1. On the menu bar, click **Dedicated devices > Public device groups**.
2. Search for a public device group.
3. In the search results, click the name of the public device group to which you want to assign an app.

4. In the **Assigned apps** section, click +.
5. In the search field, type the app name, vendor, or URL of the app that you want to add.
6. Select the check box next to the app or app group that you want to assign to the group.
7. Click **Next**.
8. In the **Disposition** drop-down list for the app, perform one of the following actions:
   - To require users to install the app, select **Required**.
   - To permit users to install and remove the app, select **Optional**.
   - To prevent users from installing the app, select **Denied**

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 BlackBerry UEM Self-Service capabilities, 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 BlackBerry UEM Self-Service capabilities 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 user group. If a user is a member of multiple user groups that have different user roles, BlackBerry UEM assigns the role with the highest ranking.

BlackBerry UEM Self-Service capabilities

The following table lists the BlackBerry UEM Self-Service capabilities:

Capability	Description
Specify an activation password	This capability allows users to create activation passwords that they can use to activate their devices in 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	This capability allows users to create access keys that they can use to activate BlackBerry Dynamics apps.
Delete only work data	This capability allows users to 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	This capability allows users to 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 BlackBerry UEM.
Locate device	This capability allows users to view the location of their iOS, Android, or Windows 10 Mobile devices on a map. This capability requires that a location service profile is assigned to the user. For more information, see Create a location service profile.
Manage user certificates	This capability allows users to 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, this capability allows users to lock BlackBerry Dynamics apps that are installed on their devices and to generate unlock keys to unlock the apps. When a user locks an app, it prevents anyone from opening it.

Capability	Description
Delete BlackBerry Dynamics app data	If users' devices are enabled for BlackBerry Dynamics, this capability allows users to 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

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

After you finish: Rank user roles.

Rank user roles

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

1. On the menu bar, click **Settings > Self-Service**.
2. Click **User roles**.
3. Use the arrows to move roles up or down the ranking.
4. Click **Save**.

Assign a user role to a user

A user role specifies the capabilities available to users in BlackBerry UEM Self-Service.

Before you begin: Create a user role.

1. On the menu bar, click **Users**.
2. Select the **All users** or **Managed devices** tab.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click  .
6. In the **Direct role assignment** drop-down list, select the role that you want to assign. If you select **None**, the user's role will be assigned by a group. If there is no group assignment, the user will not have access to BlackBerry UEM Self-Service.
7. Click **Save**.

Assign a user role to a group

A user role specifies the capabilities available to users in BlackBerry UEM Self-Service.

Before you begin: Create a user role.

1. On the menu bar, click **Groups**.
2. Search for a user group.
3. In the search results, click the name of the user group.
4. Click the **Managed devices** tab.
5. In the **User role** section, click +.
6. In the drop-down list, click the name of the role that you want to assign to the group.
7. Click **Add** or **Replace**.

Viewing and customizing the user list

You can view and customize the user list by setting the default or advanced view and then selecting the information to display in the user list. You can select and reorder the columns in the user list.

You can use filters to view only the information that is relevant to your task. You can filter the user list by selecting one filter at a time or by selecting multiple filters. In the default view, you can filter the user list by OS, wireless service provider, group, assigned IT policy, ownership, and compliance violation. More categories are available in the advanced view. For example, you can filter the user list by model, OS version, and activation type.

For further analysis or reporting purposes, you can export the user list to a .csv file.

Set the default or advanced view

You can set the view that your browser uses to display the user list in BlackBerry UEM. More columns and filter categories are available in the advanced view.

Note: In larger environments, the advanced view might take longer to display than the default view.

1. On the menu bar, click **Users > Managed devices**.
2. In the upper-right corner, click **Default** or **Advanced**.

After you finish: Select the information to display in the user list.

Select the information to display in the user list

Before you begin: Set the default or advanced view.

1. On the menu bar, click **Users > Managed devices**.
2. Click + at the top of the user list and perform any of the following actions:
   - Click **Select all** or select the check box for each column that you want to display.
   - Clear the check box for each column that you want to remove.
   - Click **Reset** to return to the default selections.
3. To sort the user list, click a column header.
4. To reorder the columns, click a column header and drag it to the left or right.

Filter the user list

When you turn on multiple selection, you can select multiple filters before you apply them, and you can select multiple filters in each category. When you turn off multiple selection, each filter is applied when you select it, and you can select only one filter in each category.

Before you begin: Set the default or advanced view.

1. On the menu bar, click **Users**.
2. Click  to turn multiple selection on or off.
3. 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.

4. Perform one of the following actions:
   - If you turned on multiple selection, select the check box for each filter that you want to apply and click **Submit**.
   - If you turned off multiple selection, click the filter that you want to apply.
5. Optionally, in the right pane, click **Clear all** or click ✕ for each filter that you want to remove.

Sort the user list

You can sort the user list alphabetically by any of the categories displayed in the column headers.

Before you begin: Set the default or advanced view.

1. On the menu bar, click **Users** and select the tab you want to view.
2. If necessary, filter the user list.
3. Click a column header. Click the column header again to sort in reverse order.

Export the user list to a .csv file

When you export the user list to a .csv file, the file includes all columns available in the current view.

Before you begin: Set the default or advanced view.

1. On the menu bar, click **Users > Managed devices**.
2. If necessary, filter the user list.
3. Perform one of the following actions:
   - Select the check box at the top of the user list to select all users.
   - Select the check box for each user that you want to include in the file. You can use Shift+click to select multiple users.
4. Click  and save the file.

Change the device ownership label

Each activated device in BlackBerry UEM has a label that indicates whether the device is owned by your organization, the user, or not specified. The default value for this label comes from the device ownership setting in the activation profile. You can edit the ownership label at any time. To change this setting for multiple devices at a time, see Send a bulk command.

The device ownership label is useful if you want to filter the user list using the device ownership setting. For more information, see Filter the user list.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Click the device tab.
5. In the activated device section, beside the ownership setting, click **Edit**.
6. From the drop-down list, select one of the following options:
   - Work

- Personal
- Not specified

7. Click **Save**.

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada