BlackBerry UEM

Activating devices

Administration

12.22

Contents

Activating devices with BlackBerry UEM

When you or a user activates a device, the device is associated with BlackBerry UEM. This allows you to manage and assign configurations to devices, and it gives users access to work data on their devices.

When a device is activated, you can send IT policies and profiles to control and configure features and manage the security of work data. You can also assign apps for the user to install. Depending on how much control the selected activation type allows, you may also be able to protect the device by restricting access to certain data, remotely setting passwords, locking the device, or deleting data.

You can assign activation types to accommodate the requirements of devices that are owned by your organization and devices that are owned by users. Different activation types give you different degrees of control over the work and personal data on devices, ranging from full control over all data to specific control over work data only.

To set up UEM to allow users to activate devices, perform the following actions:

Step	Action
1	For each device that you want to activate, verify that a UEM license is available. For iOS, iPadOS, and Android devices, verify that the latest version of the BlackBerry UEM Client is installed on the device from the appropriate app store.
2	Configure default activation settings.
3	Review the information that is relevant for your UEM environment and device users: • Supporting Android Enterprise and Android Management activations • Supporting Windows 10 activations • Supporting Apple User Enrollment for iOS and iPadOS devices • Supporting Samsung Knox DualDAR • Configure support for Android zero-touch enrollment • Activate multiple devices using Knox Mobile Enrollment • Activating iOS devices that are enrolled in DEP • Activating iOS devices using Apple Configurator 2
4	Update the template for the activation email.
5	Create an activation profile and assign it to user accounts or user groups.
6	Send an activation email to multiple users, send an activation email to a specific user, or allow users to set their own activation password in UEM Self-Service.
7	Send users activation instructions: • Activating Android devices • Activating iOS devices • Activating a macOS or Apple TV device with BlackBerry UEM Self-Service • Activate a Windows 10 tablet or computer

Activation types: iOS devices

Activation type	Description
MDM controls	This activation type provides basic device management using device controls made available by iOS and iPadOS. A separate work space is not installed on the device and there is no added security for work data. You can control the device using commands and IT policies. During activation, users must install a mobile device management profile on the device. To specify whether BlackBerry UEM can limit activation by device ID, select "Allow only approved device IDs".
User privacy	This activation type provides basic control of devices while making sure that users' personal data remains private. A separate container is not installed on the device, and no added security for work data is provided. Devices can use services such as Find my Phone and Root Detection, but administrators cannot control device policies. **Note:** For SIM-based licensing, you must select "Allow access to SIM card and device hardware information to enable SIM-based licensing" in the activation profile. Users must install an MDM profile that can access only the SIM card and device hardware information that is required to check if an appropriate SIM license is available (for example, ICCID and IMEI). This activation type is not supported for Apple TV devices. When you allow User privacy activations, you select the profiles that you want manage on the device based on the needs of your organization. You can choose any of the following: • Allow access to SIM card and device hardware information to enable SIM-based licensing: This option specifies whether UEM can access SIM card and device hardware information, such as ICCID and IMEI, to check if an appropriate SIM license is available. • Allow App management: This option specifies whether you want to install or remove work apps on the device and display a list of installed work apps in the user details screen. You can also specify whether to allow app shortcuts. • Allow IT Policy management: This option specifies whether you want to apply a limited set of IT policy rules to the device (password policies, allow screenshots, allow documents from managed sources in unmanaged destinations, and allow documents from unmanaged sources in managed destinations). • Allow Email profile management: This option specifies whether to apply the Email profile settings that are assigned to the user to the device. • Allow Wi-Fi profile management: This option specifies whether to apply the Wi-Fi profile settings that are assigned to the user to the device. • Allow VPN profile management: This option specifies whether to apply the VPN profile settings that are assigned to the user to the device.

Activation type	Description
User privacy - User enrollment	This activation type can be used for iOS and iPadOS devices to ensure that user data is kept private and separated from work data. A separate work space is installed on the device for work apps and the native Notes, iCloud Drive, Mail (attachments and full email bodies), Calendar (attachments), and iCloud Keychain apps. This activation type enables app management, IT policy management, email profiles, Wi-Fi profiles, and per-app VPN. Administrators can manage work data (for example, delete work data) without affecting personal data. This activation type is supported on unsupervised iPhone and iPad devices. **Note:** The User privacy - User enrollment activation type is not supported for iOS 18 and later.
Device registration for BlackBerry 2FA only	This activation type supports the BlackBerry 2FA solution for devices that UEM does not manage. This activation type does not provide any device management or controls, but it allows devices to use the BlackBerry 2FA feature. To use this activation type, you must also assign the BlackBerry 2FA profile to users. When a device is activated, you can view limited device information in the management console, and you can deactivate the device using a command. This activation type is supported only for Microsoft Active Directory users. It is not supported for Apple TV devices. For more information, see the BlackBerry 2FA content.

Activation types: Android devices

For Android devices, you can select multiple activation types and rank them to ensure that BlackBerry UEM assigns the most appropriate activation type for the device. For example, if you rank Work and personal - user privacy (Samsung Knox) first and Work and personal - user privacy (Android Enterprise) second, devices that support Samsung Knox Workspace receive the first activation type and devices that don't support Samsung Knox Workspace receive the second.

Android Management devices

Before activating devices with Android Management activation types, review the Considerations for Android Management activation types.

Activation type	Description
Work and personal - user privacy (Android Management with work profile)	This activation type maintains privacy for personal data but allows you to manage work data using commands and IT policy rules. A work profile is created on the device that separates work and personal data. Work and personal data are both protected using encryption and password authentication.

Activation type	Description
Work and personal - full control (Android Management fully managed device with work profile)	This activation type allows you to manage the entire device using commands and IT policy rules. A work profile is created on the device that separates work and personal data. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. This activation type supports logging of device activity (SMS, MMS, and phone calls) in UEM log files. Following activation, Work and personal - full control devices have only a limited set of the standard pre-installed apps, such as Camera, Phone, and Settings, in the personal space. The list of retained pre-installed apps depends on the device vendor and OS version. This activation type requires the device to be reset to factory default settings before it is activated. If the BlackBerry UEM Client is deleted or the work profile is removed from the device, it is automatically reset to factory default settings.
Work space only (Android Management fully managed device)	This activation type allows you to manage the entire device using commands and IT policy rules. This activation type requires the user to reset the device to factory settings before activating. The activation process installs a work profile and no personal profile. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password. During activation, the device installs the UEM Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app. Following activation, Work space only devices have only a limited set of the standard pre-installed apps, such as Camera, Phone, and Settings, plus any apps you have assigned with a required disposition. The list of retained pre-installed apps depends on the device vendor and OS version. This activation type requires the device to be reset to factory default settings before it is activated. If the UEM Client is deleted or the work profile is removed from the device, it is automatically reset to factory default settings.

Android Enterprise devices

Activation type	Description
Work and personal - user privacy (Android Enterprise with work profile)	This activation type maintains privacy for personal data but allows you to manage work data using commands and IT policy rules. A work profile is created on the device that separates work and personal data. Work and personal data are both protected using encryption and password authentication. To allow Google Play app management for Android Enterprise devices, select "Add Google Play to the workspace" in the activation profile (enabled by default). If the device does not have access to Google Play, the user must download the latest UEM Client from a different source. To download the .apk file of the latest UEM Client, see KB 42607. To enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise support, you must select the "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus" option in the activation profile. Users do not have to grant Administrator permissions to the UEM Client.
Work and personal - full control (Android Enterprise fully managed device with work profile)	This activation type allows you to manage the entire device using commands and IT policy rules. A work profile is created on the device that separates work and personal data. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. This activation type supports logging of device activity (SMS, MMS, and phone calls) in UEM log files. To allow Google Play app management for Android Enterprise devices, select "Add Google Play account to the work space" in the activation profile (enabled by default). Following activation, Work and personal - full control devices have only a limited set of the standard pre-installed apps, such as Camera, Phone, and Settings, in the personal space. The list of retained pre-installed apps depends on the device vendor and OS version. To enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise support, you must select the "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus" option in the activation profile. To specify whether UEM can limit activation by device ID, select "Allow only approved device IDs" in the activation profile. This activation type requires the device to be reset to factory default settings before it is activated. If the UEM Client is deleted or the work profile is removed from the device, it is automatically reset to factory default settings. During activation users must grant Administrator permissions to the UEM Client.

Activation type	Description
Work space only (Android Enterprise fully managed device)	This activation type allows you to manage the entire device using commands and IT policy rules. It requires the user to reset the device to factory settings before activation. The activation process installs a work profile and no personal profile. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password. To allow Google Play app management for Android Enterprise devices, select "Add Google Play to the workspace" in the activation profile (enabled by default). If the device does not have access to Google Play, the user can download the UEM Client using an .apk file of the app. You can configure and include a QR Code that contains the location of the UEM Client source file in the activation email message that you send to users. When a user scans the QR Code code, the UEM Client automatically downloads. To configure and include a QR Code in the activation email message, you must select the “Allow QR codes for device activation” check box in the Activation defaults page (Settings > General settings > Activation defaults). You must also select the “Allow QR code to contain location of UEM Client app source file” check box and specify the location of the UEM Client app source file. To get the .apk file of the latest version of the UEM Client, see KB 42607. During activation, the device installs the UEM Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app. Following activation, Work space only devices have only a limited set of the standard pre-installed apps, such as Camera, Phone, and Settings, plus any apps you have assigned with a required disposition. The list of retained pre-installed apps depends on the device vendor and OS version. To enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise support, you must select the "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus" option in the activation profile. To specify whether UEM can limit activation by device ID, select "Allow only approved device IDs" in the activation profile. This activation type requires the device to be reset to factory default settings before it is activated. If the UEM Client is deleted or the work profile is removed from the device, it is automatically reset to factory default settings.

Android devices without a work profile

The following activation types apply to all Android devices.

Activation type	Description
User privacy	You can use the User privacy activation type to provide basic control of devices, including work app management, while making sure that users' personal data remains private. A separate container is not created on the device. To provide security for work data you can install BlackBerry Dynamics apps. Devices activated with User privacy can use services such as Find my Phone and Root Detection, but administrators cannot control device policies. You can also use the User privacy activation type to activate Chrome OS devices so that you can install and manage Android BlackBerry Dynamics apps.
Device registration for BlackBerry 2FA only	This activation type supports the BlackBerry 2FA solution for devices that UEM does not manage. This activation type does not provide any device management or controls, but it allows devices to use the BlackBerry 2FA feature. To use this activation type, you must also assign the BlackBerry 2FA profile to users. When a device is activated, you can view limited device information in the management console, and you can deactivate the device using a command. This activation type is supported only for Microsoft Active Directory users. For more information, see the BlackBerry 2FA content.

Samsung Knox Workspace devices

Note: Samsung Knox activation types will be deprecated in a future release. Devices that support Knox Platform for Enterprise can be activated using the Android Enterprise activation types. For more information, see KB 54614.

Activation type	Description
Work and personal - user privacy - (Samsung Knox)	This activation type maintains privacy for personal data but allows you to manage work data using commands and IT policy rules. This activation type does not support the Knox MDM IT policy rules. A separate work space is created on the device, and the user must create a password to access the work space. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. The user must also create a screen lock password to protect the entire device and will not be able to use USB debugging mode. During activation, users must grant Administrator permissions to the UEM Client.
Work and personal - full control (Samsung Knox)	This activation type allows you to manage the entire device using commands and the Knox MDM and Knox Workspace IT policy rules. A separate work space is created on the device and the user must create a password to access the work space. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. During activation users must grant Administrator permissions to the UEM Client.

Activation types: macOS devices

Activation type	Description
MDM controls	This activation type provides basic device management using device controls that macOS makes available. When a user activates a macOS device, the device and the user are set up as separate entities on BlackBerry UEM. Separate communication channels are established between UEM and the device and UEM and the user account, allowing you to manage the device and the user separately. Some profiles are assigned to the user only (for example, email profiles). Some profiles are assigned to the device only (for example, proxy profiles). Some profiles allow you to choose whether to apply the profile to the device or the user (for example, Wi-Fi profiles). You can control the device using commands and IT policies. Users activate macOS devices using BlackBerry UEM Self-Service.

Activation types: Windows 10 devices

Note: Windows 10 Mobile devices are no longer supported by Microsoft and have only limited support on UEM.

Activation type	Description
MDM controls	This activation type provides basic device management using device controls made available by Windows 10 devices. A separate work space is not installed on the device and there is no added security for work data. You can control the device using commands and IT policies. Windows 10 users activate devices through the Windows 10 Work access app.

Managing activation settings

You can manage how users activate devices, including whether users need to type an activation password or scan a QR Code, the length of time that an activation password or QR Code is valid, and whether users can activate multiple devices with the same password or QR Code.

Configure default activation settings

1. In the management console, on the menu bar, click **Settings > General settings > Activation defaults**.
2. In the **Device activation defaults** section, specify the activation password and QR Code options.
3. If you want BlackBerry UEM to notify a user with an email message each time a device is activated on their account, select the **Send device activated notification** check box.
4. To allow users to activate BlackBerry Dynamics apps with a QR Code, in the **Default BlackBerry Dynamics app control** section, select the **Use QR codes to unlock BlackBerry Dynamics apps** check box. For more information, see Generate access keys, activation passwords, or QR Codes for BlackBerry Dynamics apps.
5. To simplify the way that users activate their mobile devices, in the **BlackBerry Infrastructure** section, select the **Turn on registration with the BlackBerry Infrastructure** check box. If you clear this option, users will be asked to provide the server address for UEM when they activate their devices.
6. To import or export a list of approved device IDs, in the **Import or export device IDs** section, click **Browse**. Navigate to and select the .csv file that contains a list of approved device IDs. For more information see Import or export a list of approved device IDs.
7. Click **Save**.

Set an activation password and send an activation email message

You can set an activation password and send a user an activation email with instructions to activate one or more devices. In on-premises environments, the email message is sent from the email address that you configured in the SMTP server settings.

Before you begin: Create an activation email template.

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Search for and click the name of a user account.
3. In the **Activation details** section, click **Set activation password**.
4. In the **Activation option** drop-down list, do one of the following:
   - If you want the user to activate their device with the activation profile that is currently assigned to them, select **Default device activation**.
   - If you want to pair an activation password with a specific activation profile, select **Device activation with specified activation profile**. For more information, see Allowing users to activate multiple devices with different activation types.
5. In the **Activation password** drop-down list, do one of the following:
   - If you want to automatically generate a password, select **Autogenerate device activation password and send email with activation instructions**. When you select this option, you must select an email template to send the information to the user.
   - If you want to set an activation password for the user and, optionally, send an activation email, select **Set device activation password** and type a password.

6. Optionally, to specify how long the activation password remains valid, change the activation period expiration.
7. If you want the activation password to be valid only for one device activation, select **Activation period expires after the first device is activated**.
8. In the **Activation email template** drop-down list, select the email template that you want to use.
9. Click **Submit**.

Send an activation email to multiple users

You can send activation email messages to multiple users at once. When you send an activation email to multiple users, the activation password is autogenerated. The email is sent from the email address that you configured in the SMTP server settings.

Before you begin: Create an activation email template.

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 an activation email to.
3. Click  .
4. In the **Activation option** drop-down list, do one of the following :
   - If you want users to activate their devices with the activation profile that is currently assigned to them, select **Default device activation**.
   - If you want to pair an activation password with a specific activation profile, select **Device activation with specified activation profile**. For more information about pairing activation passwords with activation profiles, see Allowing users to activate multiple devices with different activation types.
5. In the **Activation password** drop-down list, select **Autogenerate device activation password and send email with activation instructions**.
6. To specify how long the activation password remains valid, change the activation period expiration.
7. If you want the activation password to be valid only for one device activation, select **Activation period expires after the first device is activated**.
8. In the **Activation email template** drop-down list, select the email template that you want to use.
9. Click **Send**.

Allow users to set activation passwords in BlackBerry UEM Self-Service

You can allow users with iOS, Android, and Windows devices to create their own activation passwords using BlackBerry UEM Self-Service.

1. In the management console, on the menu bar, click **Settings > Self-Service > Self-Service settings**.
2. Select the **Allow users to activate devices in the self-service console** check box and do the following:
3. Specify how long 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 required level of complexity.
6. To automatically send an activation email to users when they create an activation password, select the **Send activation email** check box. In the **Activation email template** drop-down list, select an email template.
7. To send custom activation messages to users, select the **Send custom activation messages** check box. Select a message template for each device type from the appropriate drop-down list.

8. To send login notification emails to users each time they log in to UEM Self-Service, select the **Send self-service login notification** check box.
9. Click **Save**.

Allowing users to activate multiple devices with different activation types

You can create multiple activation passwords for a user and pair the activation passwords with specific activation profiles so that users can activate devices with different activation types.

For example, you might want users to activate work devices with an activation type that allows you to have full control of devices, but activate their personal devices with an activation type that allows user privacy. By pairing one activation password with an activation profile that allows full device control and a second activation password with the user privacy activation profile, users can activate each device with different results. You can create email templates that describe the intended use for each password.

To pair an activation password with a specific activation profile, when you create a user account or send an activation email message, select the "Device activation with specified activation profile" option.

You can have a maximum of two activation passwords that are paired with specific activation profiles. Each password can be used to activate multiple devices. Note that, for activation passwords that are paired with activation profiles, the "Number of devices that a user can activate" option in the activation profile is not enforced.

If you delete an activation profile that an activation password is paired with, the activation password is automatically expired. If necessary, you can expire activation passwords for a user at any time.

Users cannot create activation passwords that are paired with specific activation profiles in BlackBerry UEM Self-Service.

This option is not supported by iOS devices that are enrolled in DEP.

Force activation password expiry

You can manually force an activation password that was generated for a user to expire.

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Search for and click the name of a user account.
3. In the **Activation details** section, under the activation password that you want to expire, click **Expire**.

The activation password expires immediately. If you force a regular activation password to expire, the date and time that the password expired is displayed. If you force an activation password that was paired with a specific activation profile to expire, the details of the device activation password are no longer displayed.

Supporting Android Enterprise and Android Management activations

The way that you activate users' Android Enterprise and Android Management devices can depend on several factors, including the device's Android OS version and the amount of control that your organization wants to have over users' devices. It can also depend on whether your organization interacts with Google services by using managed Google Play accounts, Google Workspace domains or Google Cloud domains, or whether it does not use Google services.

Support Android Enterprise and Android Management activations using managed Google Play accounts

If your organization doesn't have a Google domain or you don't want to connect BlackBerry UEM to your Google domain, you can activate Android Enterprise and Android Management devices using managed Google Play accounts. Managed Google Play accounts allow you to add internal apps to Google Play that Android Enterprise device users can download.

To use managed Google Play accounts with UEM, you use any Google or Gmail account to connect UEM to Google. No personally identifiable information about your users is sent to Google. After you connect UEM to Google, you can allow users to activate Android Enterprise and Android Management devices and to download work apps using Google Play. For information about configuring UEM to support Android Enterprise and Android Management devices, see Configuring BlackBerry UEM to support Android Enterprise devices and Configuring BlackBerry UEM to support Android Management devices.

Support Android Enterprise activations with a Google Workspace domain

If you have configured BlackBerry UEM to connect to your organization's Google Workspace domain, perform the following tasks before users activate Android Enterprise devices.

Before you begin: Configure BlackBerry UEM to support Android Enterprise devices.

1. In your Google Workspace domain, create user accounts for your Android users.
2. Select the **Enforce EMM Policy** setting.

   This setting is required for devices that will be assigned the Work space only and Work and personal - full control activation types, and it is strongly recommended for devices with other activation types. If this setting is not selected, users can add a managed Google account to the device that can access work apps outside of the work profile.
3. In UEM, create local user accounts for your Android users. Each account's email address must match the email address in the corresponding Google Workspace account.
4. In UEM, assign an email profile and productivity apps to users, user groups, or device groups.

Support Android Enterprise activations with a Google Cloud domain

If you have configured BlackBerry UEM to connect to a Google Cloud domain, you must perform the following tasks before users can activate devices using Android Enterprise.

Before you begin: Configure BlackBerry UEM to support Android Enterprise devices. When you configure UEM to connect to a Google Cloud domain, you must select whether UEM can create user accounts in the domain. This selection affects the tasks that you must perform before users can activate Android Enterprise devices.

1. In UEM, add directory user accounts for your Android Enterprise users.
2. If you choose not to allow UEM to create user accounts in your Google Cloud domain, you must create user accounts in your Google Cloud domain and in UEM. Do one of the following:
   - In your Google Cloud domain, create user accounts for your Android Enterprise users. Each email address must match the email address in the corresponding UEM user account. Make sure that your Android Enterprise users know the password for their Google Cloud accounts.
   - Use the Google Apps Directory Sync tool to synchronize your Google Cloud domain with your company directory. If you do this, you don't need to create user accounts manually in your Google Cloud domain.
3. If you intend to assign the Work space only or Work and personal - full control activation types, select the **Enforce EMM Policy** setting in the Google Cloud domain.

   This setting is required for devices with the Work space only and Work and personal - full control activation types and strongly recommended for devices with other activation types. If this setting is not selected, users can add a managed Google account to the device that can access work apps outside of the work profile.
4. In UEM, assign an email profile and productivity apps to users, user groups, or device groups.

Support Android Enterprise devices without access to Google Play

To activate devices that don’t have access to Google Play, users must download the latest BlackBerry UEM Client from a different source. The available methods to download the UEM Client depend on the OS version and activation type:

- For devices that will be activated with the Work space only or Work and personal - full control activation types, the device must be set to factory default settings before installing the UEM Client. You can include a specified download location in a QR Code.
- Devices that will be activated with the Work and personal - user privacy activation type don't need to be reset to their factory default settings. For these devices, after the out-of-box setup is complete, users can install the UEM Client.

To download the .apk file of the latest UEM Client, see KB 42607.

If you want to activate devices that don’t have access to Google Play, verify the following:

Requirement	Description
BlackBerry UEM environment	If you only want to support devices that don't have access to Google Play, you aren't required to integrate your UEM environment with Android Enterprise. If you want to support a mixture of devices that do and don't have access to Google Play, you must integrate your environment with Android Enterprise.
Default activation settings	If you want to include the UEM Client location in a QR code, in the default activation settings, select "Allow QR code to contain location of UEM Client app source file" and "Use default location". These options allow users to scan the QR code in the activation email to download the UEM Client from the BlackBerry download site. These options are available only if your UEM environment is integrated with Android Enterprise.

Requirement	Description
Activation profile settings	Verify the following settings in the activation profile: • Clear the "Add Google Play account to workspace" option. • If you want to enable BlackBerry Secure Connect Plus, select the "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus" option. You must upload the BlackBerry Connectivity app as an internal app and assign it to users.
IT policy rules	For users that are assigned the Work and personal - user privacy (Android Enterprise) activation type, to allow the installation of apps outside of Google Play, enable the "Allow installation of non Google Play apps" IT policy rule.
Non-BlackBerry Dynamics apps	For non-BlackBerry Dynamics apps, add the apps to UEM as internal apps and assign them to users. **1.** Get the .apk files of the apps that you want to assign. **2.** In the management console, on the menu bar, click **Apps**. **3.** Click > **Internal apps**. **4.** Click **Browse** and select the .apk file. **5.** In the **Send to** field, select **All Android devices**. **6.** Deselect **Publish app in Google domain**. **7.** Click **Add**. **8.** Repeat the previous steps for each app that you want to add. **9.** Assign the apps to users. The app disposition must be set to **Required**.
BlackBerry Dynamics apps	For BlackBerry Dynamics apps, upload the internal app source file and assign the app to users. To install or update internal apps on devices that don't have access to Google Play, do the following: **1.** Get the .apk files of the BlackBerry Dynamics apps that you want to assign. **2.** In the management console, on the menu bar, click **Apps**. **3.** Click a BlackBerry Dynamics app. **4.** Click the **Android** tab. **5.** Click **Add internal app source file**. **6.** Click **Browse** and select the .apk file. **7.** Click **Add**. **8.** Click **Save**. **9.** Repeat the previous steps for each app that you want to add. **10.** Assign the apps to users. The app disposition must be set to **Required**.
BlackBerry UEM Client app update	To update the UEM Client app on devices, users must manually download the latest version of the .apk file and install it.

Supporting Windows 10 activations

You can help users activate Windows 10 devices in the following ways:

- Create or edit an activation email template to provide Windows 10 activation information. For more information, see Create an activation email template.
- Integrate UEM with Entra ID join: When Entra ID join is configured, users can activate their devices using only their Entra ID username and password.
- Configure Windows Autopilot: When you configure Windows Autopilot, the enrollment is part of the out-of-box setup experience and the device is automatically activated when the user completes it using only their Entra ID username and password.
- Deploy a discovery service: You can use a Java web application from BlackBerry as a discovery service to simplify the activation process for users with Windows 10 devices. If you use the discovery service, users don't need to type a server address during the activation process.

Supporting Apple User Enrollment for iOS and iPadOS devices

You can use the User privacy - User enrollment activation type for iOS and iPadOS devices to ensure that user data is kept private and separated from work data. With this activation type, a separate work space is installed on the device for work apps and the native Notes, iCloud Drive, Mail (attachments and full email bodies), Calendar (attachments), and iCloud Keychain apps. This activation type enables app management, IT policy management, email profiles, Wi-Fi profiles, and per-app VPN. Administrators can manage work data (for example, wipe work data) without affecting personal data. This activation type is supported on unsupervised iPhone and iPad devices that run supported versions of iOS or iPadOS.

Note: The User privacy - User enrollment activation type is not supported for iOS 18 and later.

If you want to support Apple User Enrollment, do the following:

- Verify that the devices that you will activate using this activation type are not supervised.
- Create a managed Apple ID account for each user. The managed Apple ID email address must match the user's email address in BlackBerry UEM.
- When you set the device activation password for a user, select the Apple User Enrollment activation email template.
- If you want to allow users to easily activate other BlackBerry Dynamics apps, import certificates, use BlackBerry 2FA features, use CylancePROTECT, and check their compliance status, assign the BlackBerry UEM Client using a VPP license. If you set the disposition to Required, the user is prompted to install the app. If you set the disposition to Optional, the user must manually download the app from Work Apps.

Supporting Samsung Knox DualDAR

Devices that support Samsung Knox DualDAR encryption can have work data secured using two layers of encryption. The outer layer of Knox DualDAR is built on Android file-based encryption and enhanced by Samsung to meet MDFPP requirements. In the activation profile, you can specify whether to use the default built-in encryption app or an internal encryption app that you want to use for the inner layer of encryption in the work profile.

If you choose to use the default app, the work profile is secured using a FIPS 140-2 certified cryptographic module that is included in the Samsung Knox framework. The internal encryption app is a purpose-built cryptographic module that is developed by your organization or a third party and is expected to be FIPS 140-2 certified. When the user is not using the device, all data in the work profile is locked and can't be accessed by apps running in the background.

Requirement	Description
Supported devices	Samsung flagship models are supported.
Encryption app	If you have an encryption app that you want to use for Knox DualDAR encryption, you must add it as an internal app in the management console. You select this encryption app when you create an activation profile for devices that support Knox DualDAR. You can also choose to use the default encryption app instead.
Activation profile	If you enable Knox DualDAR encryption in the activation profile, you should only assign the profile to devices that support it. If your organization supports a mixture of devices that may or may not support Knox DualDAR, you should assign the activation profile to a device group. If you enable Knox DualDAR activation for an unsupported device, the activation will not complete successfully. To support Knox DualDAR encryption, create an activation profile with the following settings for Android devices: • Select the Work and personal - full control (Android Enterprise fully managed device with work profile) activation type • Select the "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus" option. • Select the "Enable Samsung Knox DualDAR Workspace" option. • To use the default encryption app, select the "Default built-in encryption app" option. To use another encryption app, select the "Select an internal app for encryption" option and choose the encryption app that you want from the app list.
BlackBerry UEM Client	The latest version of the BlackBerry UEM Client for Android is recommended.

Creating activation profiles

You can control how devices are activated and managed using activation profiles. An activation profile specifies the number of devices and the types of devices that a user can activate, as well as the activation type to use for each device type. The activation type determines how much control you have over activated devices.

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

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

Create an activation profile

1. In the management console, on the menu bar, click **Policies and profiles > Policy > Activation**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Number of devices that a user can activate** field, specify the maximum number of devices that a user can activate.
5. In the **Device ownership** drop-down list, select one of the following:
   - If some users activate personal devices and some users activate work devices, select **Not specified**.
   - If most users activate work devices, select **Work**.
   - If most users activate personal devices, select **Personal**.
6. Optionally, in the **Assign organization notice** drop-down list, select an organization notice.

   If you assign an organization notice, users activating iOS, iPadOS, macOS, or Windows 10 devices must accept the notice to complete the activation process.
7. In the **Device types that users can activate** section, select the device OS types that users can activate.
8. For each device type that you include in the activation profile, perform the following actions:
   a) Click the tab for the device type.
   b) In the **Device model restrictions** drop-down list, select one of the following options:
      - **No restrictions**: Users can activate any device model.
      - **Allow selected device models**: Users can activate only the device models that you specify.
      - **Do not allow selected device models**: Users can't activate the device models that you specify.

      If you restrict the device models users can activate, click **Edit** to select the devices you want to allow or restrict and click **Save**.
   c) In the **Minimum allowed version** drop-down list, select the minimum allowed OS version.
   d) Select the supported activation types.

      For Android devices, you can select multiple activation types and rank them. For all other device types, you can select only one activation type.

      You must create separate activation profiles for Android Enterprise and Android Management. If Android Enterprise and Android Management activation types are specified in the same profile, the Android Management type will take precedence, even if it is ranked lower than Android Enterprise. Only the password and activation information for the Android Management activation type will be embedded in the QR Code.
9. For iOS and iPadOS devices, perform the following actions:

a) If you selected the User privacy activation type and you want to enable SIM-based licensing, select **Allow access to SIM card and device hardware information to enable SIM-based licensing**.
b) If you selected the User privacy activation type and you want to manage specific features, select the appropriate check boxes.
c) If you selected the MDM controls or User privacy (with SIM-based licensing) activation types and you only want to activate supervised devices, select **Do not allow unsupervised devices to activate**.
d) If you selected the MDM controls activation type and you want to allow UEM to restrict activation by device ID, select **Allow only approved device IDs**. See Import or export a list of approved device IDs.
e) If you have enabled CylancePROTECT Mobile for BlackBerry UEM and you want to perform iOS app integrity checks, select one of the following attestation methods:

- **Perform app integrity check on BlackBerry Dynamics app activation**: Use this method to send challenges to devices when they are activated to check the integrity of iOS work apps.
- **Perform periodic app integrity checks**: Use this method to send challenges to devices to check the integrity of iOS work apps.

f) Optionally, if you want to perform managed device attestation for iOS devices, in the **Managed device attestation** section, select one of the following attestation methods:

- **Perform Managed device attestation on device activation**: Use this method to send challenges to devices when they are activated to check the integrity of the device properties.
- **Perform periodic Managed device attestation**: Use this method to send challenges periodically to check the integrity of the device properties.

Managed device attestation applies to the MDM controls and the User privacy activation types, but not the User privacy - User enrollment activation type. When you select the User privacy activation type, you must select at least one of the management options (such as "Allow VPN management").

10. For iOS and macOS devices, if you want to use SCEP or ACME to send client certificates to devices, in the **Identity certificate** section, select the certificate type (SCEP or ACME).

- If you selected SCEP, in the **Key strength** drop-down list, select the appropriate value.
- If you selected ACME, in the **RSA strength** drop-down list, select the appropriate value.

11. For Android devices, perform the following actions:

a) If you selected more than one activation type, click the arrows to rank them. Devices receive the highest ranked profile that they support.
b) If you selected a Samsung Knox activation type and you want to use Google Play to manage work apps, select **Google Play app management for Samsung Knox Workspace devices**. This option is available only if you have configured a connection to a Google domain.

Samsung Knox activation types will be deprecated in a future release. Devices that support Knox Platform for Enterprise can be activated using the Android Enterprise activation types.

c) If you selected an Android Enterprise activation type, select the appropriate Android Enterprise options:

- To enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise features (for devices that support Samsung Knox) on devices with an appropriate license, select **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus**.
- To enable Samsung Knox DualDAR encryption for devices that support it, select **Enable Samsung Knox DualDAR Workspace**.
- To allow Google Play app management in the work space, select **Add Google Play account to work space**.
- To allow UEM to restrict activation by device ID, select **Allow only approved device IDs** This option is supported only for Work space only and Work and personal - full control devices. See Import or export a list of approved device IDs.

- To specify the network type that users can activate a device over, in the **QR Code enrollment** drop-down list, select a network. This option is supported only for Work space only and Work and personal - full control devices.

d) Optionally, in the **SafetyNet or Play Integrity attestation options** section, select one of the following attestation methods:

- **Perform SafetyNet or Play Integrity attestation for device**: Use this method to send challenges to test the authenticity and integrity of devices.
- **Perform SafetyNet attestation on device activation (Applies only to UEM Client versions that do not support Play Integrity)**: Use this method to send challenges to test the authenticity and integrity of devices when they are activated.
- **Perform SafetyNet or Play Integrity attestation on BlackBerry Dynamics app activation**: Use this method to send challenges to test the authenticity and integrity of BlackBerry Dynamics apps when they are activated.

e) If you want UEM to send challenges to devices when they are activated to ensure the required security patch level is installed, in the **Hardware attestation options** section, select **Enforce attestation compliance rules during activation**.

12. For Windows 10 devices, select one or both form factor options.

13. Click **Add**.

After you finish:

- If necessary, rank activation profiles.
- Assign the profile to user accounts and groups.

Activating Android devices

The steps that users follow to install the BlackBerry UEM Client and activate Android devices depend on several factors, including the Android OS version, the device manufacturer, how your organization uses Google services, the activation type specified in the device activation profile, and your organization's preferences. You can provide device activation instructions in the activation email that you send to users. For more information about creating an activation email template, see Create an activation email template.

Android Management devices support the following activation methods:

Activation method	Description
Activation for Android Management user privacy	For devices that will be activated with the Work and personal - user privacy activation type, users can set up a work profile and use a provided QR code to download the UEM Client from Google Play and activate the device on UEM. For more information, see Activate an Android Management device with the Work and personal - user privacy activation type.
Activation for Android Management full control and work space only	For devices that will be activated with the Work and personal - full control and Work space only activation types, the user must reset the device to factory default settings and use a provided QR code to download the UEM Client from Google Play and activate the device on UEM. For more information, see Activate an Android Management device using a managed Google Play account.

Android Enterprise devices support the following activation methods:

Activation method	Description
Install the UEM Client from Google Play.	Devices that will be activated with the Work and personal - user privacy activation type don't need to be reset to factory default settings before activation. To activate these devices, users can download the UEM Client from Google Play. For more information, see Activate an Android Enterprise device with the Work and personal - user privacy activation type.
Download the UEM Client .apk file from the BlackBerry download site.	If Android users don't have access to Google Play, for devices that will be activated with the Work and personal - user privacy activation type, users can download the UEM Client .apk file from the BlackBerry download site. You can also download the file from BlackBerry and put the file in a location that your users can access. To get the .apk file of the latest version of the UEM Client, see KB 42607.
Use Google domain credentials during device setup.	If BlackBerry UEM is connected to your organization's Google Workspace or Google Cloud domain, to activate devices that are assigned the Work space only or Work and personal - full control activation type, when users enter their work Google credentials during device setup the device downloads the UEM Client and begins the activation process. For more information, see Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain.

Activation method	Description
Scan a QR code that contains the UEM Client download location.	BlackBerry UEM allows you to include the download location for the UEM Client in a QR code that you can include in the activation email email that you send to users. Users that are assigned the Work space only or Work and personal - full control can scan the QR code to download the UEM Client. For more information, see Activate an Android Enterprise device using a managed Google Play account.
Android zero-touch enrollment or Samsung Knox Mobile Enrollment.	Android zero-touch enrollment allows you to deploy a large number of Android Enterprise devices at one time. Knox Mobile Enrollment allows you to deploy large numbers of Samsung Knox devices with Android Enterprise activations. To use this option, devices must be provisioned for zero-touch enrollment or Knox Mobile Enrollment when they are purchased from an authorized reseller. For more information, see Configure support for Android zero-touch enrollment or Activate multiple devices using Knox Mobile Enrollment.

For Android Enterprise devices, each activation option is supported only by certain activation types. For the Work space only and Work and personal - full control activation types, the supported options also depend on how your organization uses Google services.

Activation type	AE User privacy	AE full control			AE Work space only		
Method		Google domain	Managed Google Play	No Google access	Google domain	Managed Google Play	No Google access
Install UEM Client from Google Play or user download	Yes	No	No	No	No	No	No
Google domain credentials	Yes	Yes	No	No	Yes	No	No
Scan QR code	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Android zero-touch enrollment / Samsung Knox Mobile Enrollment	No	Yes	Yes	Yes	Yes	Yes	Yes

Activate an Android Enterprise device with the Work and personal - user privacy activation type

To activate devices with the Work and personal - user privacy (Android Enterprise) activation type, send the following activation instructions to device users. Devices with this activation type don't need to be reset to factory default settings before activation.

Before you begin: Your device administrator sent you one or more email messages with the information that you need to activate your device. If the email message includes an activation QR code, you can use it to activate your device. If you did not receive a QR code, make sure you have the following information:

- Your work email address
- Your UEM username (usually your work username)
- Your UEM activation password
- The UEM server address (if required)

1. On the device, install the BlackBerry UEM Client from Google Play.

   If the device doesn't have access to Google Play, you can manually download the UEM Client using an .apk file. To get the .apk file of the latest version of UEM Client, see KB 42607.
2. Open the UEM Client.
3. Read the license agreement and tap the **I accept the License Agreement** check box.
4. Do one of the following:

Task	Steps
Scan a QR code to activate the device.	**a.** Tap . **b.** To allow the UEM Client to take pictures and to record video, tap **Allow**. **c.** Scan the QR code that your administrator provided in the activation email.
Manually activate the device.	**a.** Type your work email address and tap **Next**. **b.** Type your activation password and tap **Activate My Device**. **c.** If necessary, type the server address and tap **Next**. **d.** If necessary, type your username and activation password and tap **Next**.

5. To allow the UEM Client to make and manage phone calls, tap **Allow**.
6. On the **Set up your profile** screen, tap **Set up**. It may take a moment to set up the work profile.
7. If you are prompted log in to your Google account, enter your Google email address and password.
8. Choose a screen unlock method.
9. If you are prompted by the **Secure start-up** screen to require a password when the device starts, tap **Yes**.
10. Type a device password and type it again to confirm it. Tap **OK**.
11. Select how you want your notifications to display. Tap **Done**.
12. Create a UEM Client password and tap **OK**. If you are using BlackBerry Dynamics apps, you will also use this password to sign in to all of your BlackBerry Dynamics apps.
13. Tap **Enroll**.
14. If you want to set up fingerprint authentication for the UEM Client and BlackBerry Dynamics apps, follow the instructions on the screen. Otherwise, tap **Cancel**.

15. If you are signed out of your device, unlock your device to complete the UEM activation.
16. If you are prompted to allow the connection to BlackBerry Secure Connect Plus, tap **OK** and wait for the connection to turn on.
17. If you are prompted to install work apps on your device, follow the instructions on the screen.

After you finish: To verify that the activation process completed successfully, do one of the following:

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

Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain

These steps apply to devices that are assigned the Work space only (Android Enterprise) or Work and personal - full control (Android Enterprise) activation type when BlackBerry UEM is connected to a Google Workspace or Google Cloud domain. To activate devices that are connected to a Google domain with the Work and personal - user privacy activation type, see Activate an Android Enterprise device with the Work and personal - user privacy activation type.

Send the following activation instructions to the device user.

Before you begin: Your device administrator sent you one or more email messages with the information that you need to activate your device. If the email message includes an activation QR Code, you can use it to activate your device and you don't need to type any information. If you did not receive a QR Code, make sure you received the following information:

- Your work email address
- Your UEM username (usually your work username)
- Your UEM activation password
- Your UEM server address (if required)

1. If you do not see the device setup Welcome screen, reset your device to the factory default settings.
2. During the device setup, in the Google account login screen, enter your work Google email address and password.
3. On the device, tap **Install** to install the BlackBerry UEM Client.
4. Read the license agreement and tap the **I accept the License Agreement** check box.
5. Do one of the following:

Task	Steps
Use a QR Code to activate the device.	**a.** Tap . **b.** Tap **Allow** to allow the UEM Client to take pictures and record video. **c.** Scan the QR Code in the activation email message that you received.

Task	Steps
Manually activate the device.	a. Type your work email address. Tap **Next**. b. Type your activation password. Tap **Activate My Device**. c. If necessary, type the server address. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service. Tap **Next**. d. If necessary, type your username and activation password. Tap **Next**.

6. Wait while the profiles and settings are pushed to your device.
7. On the **Set up your profile** screen, tap **Set up**. It may take a moment to set up the work profile.
8. If you are prompted, log in to your Google account with your Google email address and password.
9. On the unlock selection screen, choose a screen unlock method.
10. If you are prompted with the **Secure start-up** screen, tap **Yes** to require a password when the device starts.
11. Type a device password and type it again to confirm it. Tap **OK**.
12. Select one of the options for how you want your notifications to show. Tap **Done**.
13. Create a UEM Client password and tap **OK**. If you are using BlackBerry Dynamics apps, you will also use this password to sign in to all of your BlackBerry Dynamics apps.
14. On the next screen, tap **Enroll** and follow the instructions on the screen if you want to set up fingerprint authentication for the UEM Client and any BlackBerry Dynamics apps that you have. Otherwise, tap **Cancel**.
15. If you are signed out of your device, unlock your device to complete the UEM activation.
16. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.
17. If you are prompted, follow the instructions on the screen to install work apps on your device.

After you finish: To verify that the activation process completed successfully, do one of the following:

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

Activate an Android Enterprise device using a managed Google Play account

The following activation instructions apply to supported Android devices that are assigned the Work space only (Android Enterprise) or Work and personal - full control (Android Enterprise) activation type. To activate devices that are connected to a managed Google Play account with the Android Enterprise Work and personal - user privacy activation type, see Activate an Android Enterprise device with the Work and personal - user privacy activation type.

You can configure and include a QR Code that contains the location of the UEM Client app source file in the activation email message that you send to users. When a user scans the QR Code code, the UEM Client is downloaded automatically. To configure and include a QR Code in the activation email message, you must select the “Allow QR codes for device activation” check box in the Activation defaults page (Settings > General settings > Activation defaults). You must also select the “Allow QR code to contain location of UEM Client app source file” check box and specify the location of the UEM Client app source file. To get the .apk file of the latest version of the UEM Client, see KB 42607.

Send the following activation instructions to the device user.

Before you begin: Your device administrator sent you one or more email messages with the information that you need to activate your device. The email message includes a QR Code with the information needed to install the UEM Client and activate the device.

1. On the device that you want to activate, if you don't see the device setup screen, reset your device to its factory default settings.
2. To open the device's QR Code reader, tap the device screen seven times.
3. To download the UEM Client, scan the QR Code that your administrator provided in the activation email.
4. Open the UEM Client.
5. Read the license agreement and tap the **I accept the License Agreement** checkbox.
6. On the **Set up your profile** screen, tap **Set up**. It may take a moment to set up the work profile.
7. Choose a screen unlock method.
8. If you are prompted by the **Secure start-up** screen to require a password when the device starts, tap **Yes**.
9. Type a device password and type it again to confirm it, then tap **OK**.
10. Select how you want your notifications to display. Tap **Done**.
11. Create a UEM Client password and tap **OK**. If you are using BlackBerry Dynamics apps, you will also use this password to sign in to all of your BlackBerry Dynamics apps.
12. Tap **Enroll**.
13. If you want to set up fingerprint authentication for the UEM Client and BlackBerry Dynamics apps, follow the instructions on the screen. Otherwise, tap **Cancel**.
14. If you are signed out of your device, unlock your device to complete the UEM activation.
15. If you are prompted to allow the connection to BlackBerry Secure Connect Plus, tap **OK** and wait for the connection to turn on.
16. If you are prompted to install work apps on your device, follow the instructions on the screen.

After you finish: To verify that the activation process completed successfully, do one of the following:

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

Activate an Android Enterprise device without access to Google Play

The following activation instructions apply to devices that are assigned the Work space only (Android Enterprise) and Work and personal - full control (Android Enterprise) activation types and that don't have access to Google Play. The user can download the BlackBerry UEM Client using an .apk file of the app. You can configure and include a QR Code that contains the location of the UEM Client source file in the activation email message that you send to users. When a user scans the QR Code code, the UEM Client automatically downloads.

To configure and include a QR Code in the activation email message, you must select the “Allow QR codes for device activation” check box in the Activation defaults page (Settings > General settings > Activation defaults). You must also select the “Allow QR code to contain location of UEM Client app source file” check box and specify the location of the UEM Client app source file. To get the .apk file of the latest version of the UEM Client, see KB 42607.

Send the following activation instructions to device users.

Before you begin: Your device administrator sent you one or more email messages with the information that you need to activate your device. If you received an activation QR Code from your administrator, you can use it to activate your device. If you did not receive a QR Code, make sure that you have the following information:

- Your work email address
- Your UEM username (usually your work username)
- Your UEM activation password
- Your UEM server address (if required)

1. On the device that you want to activate, if you don't see the device setup screen, reset your device to its factory default settings.
2. To open the device's QR Code reader, tap the device screen seven times.
3. To download the UEM Client, scan the QR Code that your administrator provided in the activation email message.
   The UEM Client automatically downloads on to the device.
4. Open the UEM Client.
5. Read the license agreement and tap the **I accept the License Agreement** check box.
6. Do one of the following:

Task	Steps
Use a QR Code to activate the device.	**a.** In the UEM Client, tap . **b.** To allow the UEM Client to take pictures and record video, tap **Allow**.
Manually activate the device.	**a.** Type your work email address and tap **Next**. **b.** Type your activation password and tap **Activate My Device**. **c.** If necessary, type the server address and tap **Next**. **d.** If necessary, type your username and activation password and tap **Next**.

7. On the **Set up your profile** screen, tap **Set up**. It may take a moment to set up the work profile.
8. Choose a screen unlock method.
9. If you are prompted by the **Secure start-up** screen to require a password when the device starts, tap **Yes**.
10. Type a device password and type it again to confirm it. Tap **OK**.
11. Select how you want your notifications to display. Tap **Done**.
12. Create a UEM Client password and tap **OK**. If you are using BlackBerry Dynamics apps, you will also use this password to sign in to all of your BlackBerry Dynamics apps.
13. On the next screen, tap **Enroll**.
14. If you want to set up fingerprint authentication for the UEM Client and BlackBerry Dynamics apps, follow the instructions on the screen. Otherwise, tap **Cancel**.
15. If you are signed out of your device, unlock your device to complete the UEM activation.
16. If you are prompted to allow the connection to BlackBerry Secure Connect Plus, tap **OK** and wait while the connection turns on.
17. If you are prompted to install work apps on your device, follow the instructions on the screen.
18. If necessary, to set up email on your phone, open the email app that your organization wants you to use and follow the instructions.

Activate an Android Management device with the Work and personal - user privacy activation type

You can include a QR Code in the activation email message that you send to users. When a user scans the QR Code code, the UEM Client is downloaded automatically. To configure and include a QR Code in the activation email message, you must select the “Allow QR codes for device activation” check box in the Activation defaults page (Settings > General settings > Activation defaults). Use the default Android Management activation email template (or a custom equivalent).

Send the following activation instructions to the device user.

Before you begin: Your device administrator sent you one or more email messages with the information that you need to activate your device. The email message includes a QR Code with the information needed to install the UEM Client and activate the device.

1. On your device, go to **Settings > Google Services & Preferences**.
2. Tap **Set up & Restore**.
3. Tap **Set up your work profile**.
4. Tap **Next**.
5. In the **Allow Device Policy to take pictures and record video** dialog box, tap **Only this time**.
6. Scan the QR code that you received from your administrator.
7. Tap **Agree**.
8. Tap **Next**.
9. Depending on how your administrator configured the activation, you may be prompted to set a lock for your device or for the work space.
10. On the **Your work checklist** screen, below **Install work apps**, tap **Install**.
11. After the UEM Client is installed, tap **Done**.
12. Tap **Setup BlackBerry UEM**.
13. Read the license agreement and tap **Agree**.

Your device will finish setting up your work profile.

After you finish: If you ever want to deactivate your device and remove it from UEM, you can do so from the UEM Client.

Activate an Android Management device using a managed Google Play account

The following activation instructions apply to Android devices that are assigned the Work and personal - full control (Android Management) or Work space only (Android Management) activation type. To activate devices that are connected to a managed Google Play account with the Android Management Work and personal - user privacy activation type, see Activate an Android Management device with the Work and personal - user privacy activation type.

You can include a QR Code in the activation email message that you send to users. When a user scans the QR Code code, the UEM Client is downloaded automatically. To configure and include a QR Code in the activation email message, you must select the “Allow QR codes for device activation” check box in the Activation defaults page (Settings > General settings > Activation defaults). Use the default Android Management activation email template (or a custom equivalent).

Send the following activation instructions to the device user.

Before you begin: Your device administrator sent you one or more email messages with the information that you need to activate your device. The email message includes a QR Code with the information needed to install the UEM Client and activate the device.

1. On the device that you want to activate, if you don't see the device setup screen, reset your device to its factory default settings.
2. To open the device's QR Code reader, tap the device screen seven times.
3. To download the UEM Client, scan the QR Code that your administrator provided in the activation email message.
   The UEM Client is automatically downloaded.
4. Open the UEM Client.
5. Read the license agreement and tap the **I accept the License Agreement** checkbox.
6. On the **Set up your profile** screen, tap **Set up**. It may take a moment to set up the work profile.
7. Choose a screen unlock method.
8. If you are prompted by the **Secure start-up** screen to require a password when the device starts, tap **Yes**.
9. Type a device password and type it again to confirm it, then tap **OK**.
10. Select how you want your notifications to display, then tap **Done**.
11. Create a UEM Client password and tap **OK**. If you are using BlackBerry Dynamics apps, you will also use this password to sign in to all of your BlackBerry Dynamics apps.
12. On the next screen, tap **Enroll**.
13. If you want to set up fingerprint authentication for the UEM Client and BlackBerry Dynamics apps, follow the instructions on the screen. Otherwise, tap **Cancel**.
14. If you are signed out of your device, unlock your device to complete the BlackBerry UEM activation.
15. If you are prompted to allow the connection to BlackBerry Secure Connect Plus, tap **OK** and wait for the connection to turn on.
16. If you are prompted to install work apps on your device, follow the instructions on the screen.

After you finish: To verify that the activation process completed successfully, do one of the following:

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

Activating iOS devices

The steps that users follow to install the BlackBerry UEM Client and activate iOS and iPadOS devices depends on the device's OS version and whether the activation type includes MDM controls. You can provide device activation instructions in the activation email that you send to users. For more information about creating an activation email template, see Create an activation email template.

Activate an iOS or iPadOS device with the MDM controls activation type

To activate devices with the MDM controls activation type or the User privacy with MDM options enabled activation type, send the following activation instructions to device users.

During activation, users must leave the BlackBerry UEM Client to manually install the MDM profile.

Before you begin: If Lockdown Mode is enabled on your device (iOS and iPadOS 16 or later), you must disable it to activate the device. Lockdown Mode prevents the installation of configuration profiles which are required for activation. If necessary, you can enable Lockdown Mode after activation.

1. On your device, install the UEM Client from the App Store.
2. Open the UEM Client and accept the license agreement.
3. Do one of the following:

Task	Steps
Scan a QR Code to activate the device.	a. Tap . b. To allow the UEM Client to take pictures and record video, tap **Allow**. c. Scan the QR Code in the activation email that you received.
Manually activate the device.	a. Type your work email address and activation password. b. If necessary, type the server address. You can find the server address in the activation email that you received or in BlackBerry UEM Self-Service. c. Tap **Next**.

4. To allow the UEM Client to send you notifications, tap **Allow**. Choosing **Don't Allow** will prevent the device from activating.
5. When you are prompted to install a configuration profile, tap **OK**.
6. When you are prompted to download the configuration profile, tap **Allow**.
7. After the download is complete, open **Settings**.
8. Tap **General** and navigate to **VPN & Device Management**.
9. To install the profile, tap **BlackBerry UEM Profile** and follow the instructions on the screen.
10. After the installation is complete, to complete the activation, return to the UEM Client.
11. If you are prompted to install work apps on your device, follow the instructions on the screen.

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

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

Activate an iOS or iPadOS device with Apple User Enrollment

Apple User Enrollment is supported on devices running supported versions of iOS and iPadOS. To activates devices with Apple User Enrollment, send the following activation instructions to device users.

Before you begin:

- Verify that you received an activation email that has the QR Code for Apple User Enrollment. If you didn't receive the email, contact an administrator.
- If your device is already activated with BlackBerry UEM, you must deactivate your device.
- Uninstall the BlackBerry UEM Client.
- You must have an Apple ID account that is managed through your organization.
- Your device must not be a supervised device. If your device is supervised, it is noted in the Settings app near your Apple ID.
- If Lockdown Mode is enabled on your device (iOS and iPadOS 16 or later), you must disable it to activate the device. Lockdown Mode prevents the installation of configuration profiles which are required for activation. If necessary, you can enable Lockdown Mode after activation.

1. Open the activation email that contains the QR Code for Apple User Enrollment. If the QR Code has expired, you can request a new activation code from BlackBerry UEM Self-Service or you can contact your administrator.
2. On your device, open the Camera app and scan the QR code in the activation email. When you are prompted, tap the notification to open the URL in Safari.
3. When you are prompted to download the UEM configuration profile, tap **Allow**.
4. After the download is complete, tap **Close**.
5. Go to **Settings > General > Profile**.
6. Tap **UEM profile**.
7. On the User Enrollment screen, tap **Enroll my iPhone** or **Enroll my iPad**.
8. Type your passcode.
9. Log in to Apple ID using your managed Apple ID credentials.
10. If your administrator assigned the UEM Client to you, tap **Install** when prompted, or open Work Apps.
11. To set up the UEM Client, open it and accept the license agreement. Follow the instructions on the screen to complete the activation process.

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

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

Activating a macOS or Apple TV device with BlackBerry UEM Self-Service

Users activate macOS and Apple TV devices using BlackBerry UEM Self-Service. For details and instructions, see the UEM Self-Service User Guide.

Activate a Windows 10 tablet or computer

To activate Windows 10 devices, send the following activation instructions to device users. Note that if you want to manage Windows 10 devices with the MDM controls activation type, the devices can't be managed by Microsoft System Center Configuration Manager.

Send the following activation instructions to the device user.

Before you begin: Verify that you received an activation email that contains a certificate server address. If you didn't receive the email, contact your administrator.

1. In the browser on your device, type or paste the certificate server address.
2. Click **Save**.
3. In the certificate download notification, click **Open**.
4. Click **Open**.
5. Click **Install Certificate**.
6. Select the **Current User** option and click **Next**.
7. Select the **Place all certificates in the following store** option and click **Browse**.
8. Select **Trusted Root Certification Authorities** and click **OK**.
9. Click **Next > Finish > OK > OK**.
10. Click the **Start** button.
11. Do one of the following:

Device OS version	Steps
Windows 10 version 1607 or later	**a.** Tap **Settings > Accounts > Access work or school**. **b.** Tap **Enroll only in device management**.
Windows 10 version earlier than 1607	**a.** Tap **Settings > Accounts > Work access**. **b.** Tap **Connect**.

12. In the **Email address** field, type your email address, and tap **Continue**.
13. If you are prompted, in the **Server** field, type the server name and tap **Continue**. You can find the server name in the activation email that you received from your administrator or in BlackBerry UEM Self-Service when you set your activation password.
14. In the **Activation password** field, type your activation password and tap **Continue**. You can find your activation password in the activation email that you received from your administrator, or you can set your own activation password in UEM Self-Service.
15. Tap **Done**.

After you finish:

- To verify that the activation process completed successfully, perform on of the following actions:
  - On your device, click Settings > Accounts > Access work or school (or Work access) to confirm that your device is connected to UEM.
  - In UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.
- If requested by your administrator, add your work account to Accounts used by other apps so that you can access required online apps.

- For Windows 10 version 1607 or later, click Settings > Accounts > Access work and school > Connect. Type your work email address and password.
- For Windows 10 version earlier than 1607, click Settings > Accounts > Your email and accounts. Under Accounts used by other apps, click Add a work or school account, and type your work email address and password.

Configure support for Android zero-touch enrollment

You can use Android zero-touch enrollment in BlackBerry UEM to deploy a large number of Android Enterprise devices at one time. The devices must support zero-touch enrollment.

When your organization purchases supported devices from an authorized enterprise reseller, they set up a zero-touch enrollment account and add the devices to the account. When a user set ups one of these devices for the first time or resets a device to its factory settings, the device automatically downloads the BlackBerry UEM Client and starts the UEM activation process.

Note that if the user restarts the device before the activation completes, cancels the activation, or allows the battery to drain before the activation completes, the device automatically resets to its factory settings and the activation process restarts.

1. In the management console, on the menu bar, click **Settings > External integration**.
2. Click **Android Enterprise**.
3. Click **Launch zero-touch console**.
4. If this is the first time you have connected to Android zero-touch with UEM, click **Next** and sign in to Google using the address associated with your organization's zero-touch account.
5. Create or manage enrollment configurations and assign them to the devices.

   You can also use the Android zero-touch portal to manage enrollment configurations.

After you finish:

- In UEM, verify that the appropriate profiles and IT policies are assigned to users. To use zero-touch enrollment, you must assign an activation profile with the Work and personal - full control (Android Enterprise) or Work space only (Android Enterprise) activation type enabled.
- Distribute the devices to users.

Activate multiple devices using Knox Mobile Enrollment

You can use Samsung Knox Mobile Enrollment to deploy a large number of Samsung Knox devices at one time. Your organization purchases devices from an authorized reseller or from a reseller that is willing to share the device IMEIs directly with Samsung so that the device can use Knox Mobile Enrollment. When a user sets up one of these devices for the first time, or resets a device to its factory settings, the device automatically downloads the BlackBerry UEM Client and starts the BlackBerry UEM activation process.

Note that if the user restarts the device before the activation completes, cancels the activation, or allows the battery to drain before activation the activation completes, the device automatically resets to factory settings and the activation process restarts.

Note: Knox Mobile Enrollment does not support Device Admin based enrollment on devices running Android 11 or later. For more information, see the Knox Mobile Enrollment 1.36 Release Notes.

1. In the management console, on the menu bar, click **Settings > External integration > KNOX Mobile Enrollment**.
2. Download the UEM JSON file.
3. Complete the steps on the screen.

Activating iOS devices that are enrolled in DEP

You can enroll iOS and iPadOS devices in the Apple Device Enrollment Program (DEP) and assign enrollment configurations to devices using the BlackBerry UEM management console. The enrollment configurations include extra rules that are assigned to devices during MDM enrollment.

You can use an Apple Business Manager account to synchronize UEM with DEP. Apple Business Manager is a web-based portal that allows you to enroll and manage iOS devices in DEP and manage Apple VPP accounts.

Note that you can activate DEP devices on UEM without using the BlackBerry UEM Client, but the UEM Client is required to support the following:

- BlackBerry Secure Connect Plus
- User credential profiles configured for Entrust smart credentials or app-based PKI solutions such as Purebred
- Intercede user credential profiles

To activate devices that are enrolled in DEP, perform the following actions:

Step	Action
1	Register iOS devices in DEP and assign them to the BlackBerry UEM server.
2	Assign a DEP enrollment configuration.
3	Optionally, to add the BlackBerry UEM Client to the app list and assign it to user accounts or user groups, see Add an iOS app to the app list.
4	If you do not want to use the default activation profile, create an activation profile and assign it to DEP devices (Users > Apple DEP Devices).
5	Choose how you want users to activate their devices: • Send an activation email to multiple users or send an activation email to a specific user using the Apple DEP email template. • If you connected UEM to your company directory, users can use their company directory usernames and passwords. Users must enter their usernames in the format domain \username (the credentials match your organization's domain and username variables (“%UserDomain%\%UserName%”). • You can Assign a user to an iOS device. When you assign a user to the device in UEM, they are not prompted for a username or password during device activation.
6	Distribute devices to users and have them complete the activation. If you want to support features that require the UEM Client, instruct users to install and open the UEM Client.

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

To register iOS devices in the Apple Device Enrollment Program (DEP), you must enter the device serial numbers in the Apple Business Manager and assign the devices to the BlackBerry UEM server. To enter the serial numbers, you can type in each number, select the order number that Apple assigned to the devices when you purchased them, or upload a .csv file that contains the serial numbers.

Before you begin:

- Configure BlackBerry UEM for DEP.
- Add your devices to Apple Business Manager.

1. Log in to the Apple Business Manager.
2. Click **Devices**.
3. Do the following for each device that you want to add:
   a) Search for the device serial number.
   b) Click the device.
   c) In the options menu, click **Edit Device Management Service**.
   d) Assign the device to the UEM server.

After you finish: Assign a DEP enrollment configuration.

Assign a DEP enrollment configuration

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

Before you begin: Register iOS devices in DEP and assign them to the BlackBerry UEM server.

When you configured UEM for DEP, if you selected **Automatically assign new devices to this configuration** check box, any DEP devices you add will automatically receive the DEP enrollment configuration. If you did not select this option, do the following to assign the appropriate enrollment configuration to devices:

a) In **Users > Apple DEP devices**, select the devices registered to the same DEP account.
b) Click .
c) Select and assign the enrollment configuration.

After you finish:

- If you do not want to use the default activation profile, create an activation profile and assign it to devices registered in Apple DEP. In **Users > Apple DEP devices**, select the devices registered to the same DEP account and click . Select and assign the profile.
- During device activation, users may be prompted for a username and password. Choose how you want users to activate their devices:
  - Send an activation email to multiple users or send an activation email to a specific user using the Apple DEP email template.
  - If you connected UEM to your company directory, users can use their company directory usernames and passwords. Users must enter their usernames in the format domain\username (the credentials match your organization's domain and username variables (“%UserDomain%\%UserName%”).
  - You can Assign a user to an iOS device. When you assign a user to the device in UEM, they are not prompted for a username or password during device activation.

- Distribute devices to users and have them complete the activation. If you want to support features that require the UEM Client, instruct users to install and open the UEM Client.

Assign a user to an iOS device

You can assign a user directly to a device registered in Apple DEP before the device is activated. When you assign a user directly to the device, they are not prompted for a username or password during device activation.

1. On the menu bar, click **Users > Apple DEP devices**.
2. In the **User Association** column for the device that you want to assign, click **Select**.
3. In the **Select user** search box, search for the user that you want to assign to the device.
4. In the list of search results, click the user account.
5. Click **Save**.

After you finish:

- To view the owner of an activated device, in the **User Association** column, click the username link.
- To remove a user from an iOS device, in the **User Association** column, click the username link for the device that you want to remove the user from. Click **Unassign**.

Activating iOS devices using Apple Configurator 2

If you have BlackBerry UEM on-premises, you can use Apple Configurator 2 to prepare iOS and iPadOS devices for activation. Users can activate the prepared devices without using the BlackBerry UEM Client. Users require only their username and activation password.

Apple Configurator is not supported by UEM Cloud.

Note: Certain UEM features require you to assign the UEM Client to users. Users must start the UEM Client after they activate the device. For more information, see KB 39313.

To activate iOS devices using Apple Configurator 2, perform the following the actions:

Step	Action
1	Optionally, add the UEM Client to the app list and assign it to user accounts or user groups. See Add an iOS app to the app list.
2	Add BlackBerry UEM server information to Apple Configurator 2.
3	Prepare iOS devices using Apple Configurator 2.
4	Create an activation profile and assign it to a user account or group.
5	Send an activation email to multiple users or send an activation email to a specific user.
6	Distribute devices to users and have them complete the activation. To enforce a compliance profile, users must install and open the UEM Client after the activation completes.

Add BlackBerry UEM server information to Apple Configurator 2

Before you begin: Download and install the latest version of Apple Configurator 2 from Apple.

1. In the Apple Configurator 2 menu, select **Preferences > Servers**.
2. Click + > **Next**.
3. In the **Name** field, type a name for the server.
4. In the **Hostname or URL** field, type the UEM server URL using the format *<http or https>://<servername>:<port>*, where the default port number is 8885.
5. Click **Next**.
6. Close the **Server** window.

After you finish: Prepare iOS devices using Apple Configurator 2.

Prepare iOS devices using Apple Configurator 2

When you prepare a device, Apple Configurator 2 wipes the device and upgrades the device OS to the latest version.

Before you begin: Add BlackBerry UEM server information to Apple Configurator 2.

1. Open Apple Configurator 2.
2. Connect one or more iOS devices to your computer.
3. Click **Prepare**.
4. In the **Configuration** drop-down list, select **Manual**. Click **Next**.
5. In the **Server** drop-down list, select the BlackBerry UEM server. Click **Next**.
6. Optionally, select the **Supervise devices** check box. Click **Next**.
7. If you selected **Supervise devices**, complete the organization information.
8. Click **Prepare** and wait while the device is prepared. The process can take up to 15 minutes.

After you finish: Distribute the devices to users for activation.

Import or export a list of approved device IDs

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

Before you begin: To import a list, make sure that you have a .csv file that contains a list of unique device identifiers.

1. In the management console, on the menu bar, click **Settings > General settings > Activation defaults**.
2. In the **Import or export device IDs** section, beside the **Upload approved device IDs (.csv)** field, click **Browse**.
3. Navigate to the .csv file.
4. Click **Open**.
5. Click **Save**.

After you finish: To export the list, click **Export approved device IDs (.csv)**.

Deactivating devices

When a device is deactivated, the connection between the device and the user account in BlackBerry UEM is removed. You can't manage the device and the device is no longer displayed in the management console. The user can't access work data on the device.

A device can be deactivated using any of the following methods:

- Administrators can deactivate a device from the UEM management console using the "Delete only work data" or "Delete all device data" command.
- UEM can deactivate a device if it violates the rules in the assigned compliance profile and the configured enforcement action is to deactivate the device.
- Users can deactivate a device from UEM Self-Service using the "Delete only work data" or "Delete all device data" command.
- Users can use the UEM Client to deactivate iOS and Android devices.
- Users can deactivate Windows 10 devices from Settings > Accounts > Work access > Delete.

Note the following considerations when you deactivate devices with the specified activation types:

Activation type	Considerations
Android Enterprise devices with a work profile only	You have the option to delete all data from the SD card and remove factory reset protection.
Android Enterprise devices with Work and personal - full control activations	• The "Delete all device data" command is supported for Android 10 only. UEM will no longer support Android 10 as of January 2024. • The "Delete only work data" command is supported for Android 11 and later. This command removes all work data and apps but allows the user to keep personal data and apps and continue using the unmanaged device.
Android Enterprise devices with Work and personal - user privacy and Work and personal - full control activations	If you use the "Delete only work data" command, you can specify a reason that appears in the notification on the user's device. If the device is deactivated for violating compliance rules, the notification specifies the reason the device was out of compliance.
Knox MDM	• Internal apps are uninstalled. • The uninstall option becomes available for any public apps that were installed from the app list as required.
Samsung Knox Workspace devices with Work and personal - full control	Deactivating the device deletes all data from the device. You can specify which data is wiped using the "Data wipe on deactivation" IT policy rule.

Troubleshooting device activation

When you troubleshoot activation for any device type, always check the following:

- Verify that licenses are available for the device type and the activation type.
- Verify that the activation profile that is assigned to the device supports the device type.
- Check network connectivity on the device.
  - Verify that the mobile or Wi-Fi network is active and has sufficient coverage.
  - If on work Wi-Fi, verify that the device network path is available.
  - If the user must manually configure a VPN or work Wi-Fi profile to access content behind your organization's firewall, verify that the user's profiles are configured correctly on the device.
- If you have configured compliance rules for devices with a jailbroken or rooted OS, restricted OS versions, or restricted device models, verify that the device is compliant.
- If UEM is installed on-premises and the device is trying to connect with UEM or the BlackBerry Infrastructure through your organization's firewall, verify that the proper firewall ports are open.
- Gather device logs. For more information on retrieving device logs see KB 36986 for iOS and KB 32516 for Android.

Android Management devices

- You must create separate activation profiles for Android Enterprise and Android Management. If Android Enterprise and Android Management activation types are specified in the same profile, the Android Management type will take precedence, even if it is ranked lower than Android Enterprise. Only the password and activation information for the Android Management activation type will be embedded in the QR code.
- On some devices, an unnecessary "Setup and restore" screen may display after the device successfully completes the activation process.

Knox Workspace and Android Enterprise devices

When you troubleshoot activation of Samsung devices that use Samsung Knox Workspace, verify that the Knox container version is supported. Knox Workspace requires Knox Container 2.0 or later.

When you troubleshoot activation of Android Enterprise devices, verify that the UEM user account has the same email address as in the Google domain. If the email addresses do not match, the device will show the error "Unable to activate device - Unsupported activation type".

Troubleshooting: Activation errors and issues

Activation errors

Error	Possible solution
Device activation can't be completed because the server is out of licenses. For assistance, contact your administrator.	In the UEM management console, verify that licenses are available. If necessary, activate licenses or purchase additional licenses.

Error	Possible solution
Profile failed to install. The certificate "AutoMDMCert.pfx" could not be imported.	This error is displayed on an iOS device when a profile already exists on the device. Go to **Settings > General > Profiles** on the device and verify that a profile already exists. Remove the profile and try to activate again. If the issue persists, you might have to reset the device because data might be cached.
Profile Installation Failed: The new MDM payload does not match the old payload.	This error is displayed on an iOS device when a profile already exists on the device. Go to **Settings > General > Profiles** on the device and verify that a profile already exists. Remove the profile and try to activate again. If the issue persists, you might have to reset the device because data might be cached.
Error 3007: Server is not available.	This error can occur if the certificate that UEM uses to sign the MDM profile that it sends to an iOS device is not trusted by the device (the user is prompted to trust this certificate when they activate the device). In an on-premises environment, install the root certificate for the CA that issued the certificate. See Changing the certificates that BlackBerry UEM uses for authentication in the Configuration content. This error can also occur if you configure a transparent proxy such as Blue Coat that monitors port 443 for non-standard traffic and the UEM Client cannot make the required HTTP CONNECT and HTTP OPTIONS calls to UEM. Verify that your proxy configuration is not blocking the UEM Client from making these calls.
Unable to contact server, please check connectivity or server address.	This error can occur if the username (or customer address if registration with the BlackBerry Infrastructure was disabled) was not entered correctly or if the activation password has not been set or has expired. Verify that the username, password, and customer address (if applicable) is accurate, or set a new activation password with UEM Self-Service and try again.

Activation issues

Issue	Possible solution
iOS or macOS device activations fail with an invalid APNs certificate.	The APNs certificate may not be registered correctly. Perform one or more of the following actions: • In the management console, on the menu bar, click **Settings > External integration > Apple Push Notification**. Verify that the APNs certificate status is "Installed." If the status is not correct, try to register the APNs certificate again. • To test the connection between UEM and the APNs server, click **Test APNS certificate**. • If necessary, obtain a new signed CSR from BlackBerry, and request and register a new APNs certificate. For more information, see Obtaining an APNs certificate to manage iOS and macOS devices in the Configuration content.
Users do not receive the activation email.	If users are using a third-party mail server, email messages from UEM can be marked as spam and end up in the spam email folder or the junk mail folder.
The user details screen in UEM is showing more activated Windows devices than expected.	When a user installs BlackBerry Access and BlackBerry Work for Windows on a computer, these apps display as a Windows device on the user details screen. This is expected behavior.

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