BlackBerry UEM

Activating devices

Administration

12.11

Contents

Device activation

When you activate a device, you associate the device with BlackBerry UEM so that you can manage devices and users can access work data on their devices.

When a device is activated, you can send IT policies and profiles to control the available 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 owned by your organization and devices 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.

Activation types: iOS devices

Activation type	Description
MDM controls	This activation type provides basic device management using device controls made available by iOS. 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.

Activation type	Description
User privacy	You can use the User privacy activation type to provide basic control of devices while making sure that users' personal data remains private. With this activation type, no separate container is installed on the device, and no added security for work data is provided. Devices activated with User privacy are activated on BlackBerry UEM and 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 in the iOS activation profile, 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 BlackBerry 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.
Device registration for BlackBerry 2FA only	This activation type supports the BlackBerry 2FA solution for devices that BlackBerry UEM does not manage. This activation type does not provide any device management or controls, but 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. This activation type is not supported for Apple TV devices. For more information, see the BlackBerry 2FA content.

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 BlackBerry UEM and the device and BlackBerry 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: Android devices

For Android devices, you can select multiple activation types and rank them to make sure that BlackBerry UEM assigns the most appropriate activation type for the device. For example, if you rank "Work and personal - user privacy (Android Enterprise)" first and "MDM controls" second, devices that support Android Enterprise receive the first activation type.

The Android activation types are organized in the following tables:

- Android Enterprise devices
- Android devices without a work profile
- Samsung KNOX Workspace devices

Android Enterprise devices

The following activation types apply only to 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 lets you manage work data using commands and IT policy rules. This activation type creates a work profile 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**. This setting is enabled by default. If the device does not have access to Google Play, then this setting must be deselected and the BlackBerry UEM Enroll app must be used from a secondary device during the activation process. 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. Users do not have to grant Administrator permissions to the BlackBerry UEM Client.
Work and personal - full control (Android Enterprise fully managed device with work profile)	This activation type lets you manage the entire device using commands and IT policy rules. This activation type creates a work profile 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 the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files. To allow Google Play app management for Android Enterprise devices, select **Add Google Play to the workspace**. This setting is enabled by default. If the device does not have access to Google Play, then this setting must be deselected and the BlackBerry UEM Enroll app must be used from a secondary device during the activation process. 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. During activation users must grant Administrator permissions to the BlackBerry UEM Client. This activation type is supported only for Android 8.0 and later.

Activation type	Description
Work space only (Android Enterprise fully managed device)	This activation type lets you 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. To allow Google Play app management for Android Enterprise devices, select **Add Google Play to the workspace**. This setting is enabled by default. If the device does not have access to Google Play, then this setting must be deselected and the BlackBerry UEM Enroll app must be used from a secondary device during the activation process. During activation, the device installs the BlackBerry UEM Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app. 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.

Android devices without a work profile

The following activation types apply to all Android devices.

Activation type	Description
MDM controls	This activation type lets you manage the device using commands and IT policy rules. A separate work space is not created on the device, and there is no added security for work data. If the device supports KNOX MDM, this activation type applies the KNOX MDM IT policy rules. If you do not want to apply KNOX MDM policy rules, clear the **Activate Samsung KNOX on Samsung devices that have the MDM controls activation type assigned** check box. During activation, users must grant Administrator permissions to the BlackBerry UEM Client. **Note:** This activation type is deprecated for devices with Android 10. Attempts to activate Android 10 and later devices with the MDM controls activation type will fail. For more information, visit https://support.blackberry.com/community to read article 48386.
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. With this activation type, no separate container is installed 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.

Activation type	Description
Device registration for BlackBerry 2FA only	This activation type supports the BlackBerry 2FA solution for devices that BlackBerry UEM does not manage. This activation type does not provide any device management or controls, but 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

The following activation types apply only to Samsung devices that support KNOX Workspace.

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, visit https://support.blackberry.com/community to read article 54614.

Activation type	Description
Work and personal - user privacy - (Samsung KNOX)	This activation type maintains privacy for personal data, but lets you manage work data using commands and IT policy rules. This activation type does not support the KNOX MDM IT policy rules. This activation type creates a separate work space 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 BlackBerry UEM Client.
Work and personal - full control (Samsung KNOX)	This activation type lets you manage the entire device using commands and the KNOX MDM and KNOX Workspace IT policy rules. This activation type creates a separate work space 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. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files. During activation users must grant Administrator permissions to the BlackBerry UEM Client.

Activation type	Description
Work space only - (Samsung KNOX)	This activation type lets you manage the entire device using commands and the KNOX MDM and KNOX Workspace IT policy rules. This activation type removes the personal space and installs a work space. 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, PIN, pattern, or fingerprint. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files. During activation, users must grant Administrator permissions to the BlackBerry UEM Client.

Activation types: Windows devices

Activation type	Description
MDM controls	This activation type provides basic device management using device controls made available by Windows 10 and Windows 10 Mobile 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 and Windows 10 Mobile users activate devices through the Windows 10 Work access app.

Activation types: BlackBerry 10 devices

Activation type	Description
Work and personal - Corporate	This activation type provides control of work data on devices, while making sure that there is privacy for personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted. You can control the work space on the device using commands and IT policies, but you cannot control any aspects of the personal space on the device.
Work space only	This activation type provides full control of the device and does not provide a separate space for personal data. When a device is activated, the personal space and all work data from any previous activation is removed, a work space is installed, and the user must create a password to access the device. Work data is protected using encryption and password authentication. You can control the device using commands and IT policies.

Activation type	Description
Work and personal - Regulated	This activation type provides control of both work and personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted. You can control both the work space and the personal space on the device using commands and IT policies.

Steps to activate devices

When you activate devices, you perform the following actions.

Step	Action
1	Verify that all activation requirements are met.
2	Configure the default activation settings.
3	If applicable, review the following information: • If you plan to support Android Enterprise devices, see Supporting Android Enterprise activations. • If you plan to support Windows 10 devices, see Supporting Windows 10 activations.
4	Update the template for the activation email.
5	Create an activation profile and assign it to a user account or to a group that the user belongs to.
6	Set an activation password for the user.

Requirements: Activation

For all devices:

- An available license in BlackBerry UEM for the device that you want to activate.
- A working wireless connection

For iOS and Android devices:

- The latest version of the BlackBerry UEM Client app installed on the device

For Windows 10 and Windows 10 Mobile devices:

- A BlackBerry Enterprise Server Root RSA certificate installed on the device
- For devices that use a proxy configuration, a proxy that does not require authentication. For more information, see https://docs.microsoft.com/en-us/windows/client-management/mdm/new-in-windows-mdm-enrollment-management
- For computers, Windows 10 Home has only limited support.

For BlackBerry OS (version 5.0 to 7.1) devices:

- A user account in a directory on the work mail server that the BlackBerry OS mail server connects to
- BlackBerry OS device activation enabled for the user account

Note: Users can watch a video on how to activate their devices.

Turn on user registration with the BlackBerry Infrastructure

Registration with the BlackBerry Infrastructure simplifies the way users activate their mobile devices. With registration turned on, users do not need to enter the server address when they activate devices. Registration is enabled by default. If you change this setting, you might need to update the activation email with the steps that users must take to activate their devices.

Devices running Windows 10 and Windows 10 Mobile do not use the same method for contacting the BlackBerry Infrastructure, so turning user registration on or off does not change the activation process for these devices.

Devices running BlackBerry OS (version 5.0 to 7.1) do not contact the BlackBerry Infrastructure, so turning user registration on or off does not change the activation process for these devices.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **General settings**.
3. Click **Activation defaults**.
4. Make sure the **Turn on registration with the BlackBerry Infrastructure** check box is selected.
5. Click **Save**.

Managing activation passwords

You can have some control over the number of devices that users can activate by managing the activation passwords that are sent to users.

The following are examples of how you can manage activation passwords:

- When you set activation passwords for users, you can do the following:
  - Have BlackBerry UEM autogenerate an activation password or you can specify an activation password.
  - Specify how long the activation password is valid (in minutes or days).
  - Specify that the activation period expires as soon as the user activates a device, effectively limiting the number of devices that a user can activate with that password to one.

  For more information, see Set an activation password and send an activation email message.
- You can create multiple passwords for a user and pair the passwords with specific activation profiles. For more information, see Allowing users to activate multiple devices with different activation types.
- If you allow users to set activation passwords in BlackBerry UEM Self-Service, users can create activation passwords whenever needed, but they can activate only the number of devices that are specified in the the activation profile. For more information, see Allow users to set activation passwords in BlackBerry UEM Self-Service.
- You can expire activation passwords for a user at any time. For more information, see Manually expire an activation password.
- If you are deploying devices using Samsung KNOX Mobile Enrollment, you can allow users of those devices to use their Microsoft Active Directory credentials to activate their devices. Instead of managing activation passwords for each user, you can instruct users to use their Active Directory credentials. This option applies only to devices that are enrolled in your organization's KNOX Mobile Enrollment account. For more information, see Specify the default settings for activation passwords.

Specify the default settings for activation passwords

You can specify the default time an activation password remains valid before it expires. You can also specify the length of automatically generated passwords that are sent to users in one of the activation email messages and you can specify whether or not the activation period expires after the first device is activated.

The value that you enter for the activation password expiration appears as the default setting in the Activation password expiration field in the Set device activation password and Add a user windows.

For devices that are activated using Samsung KNOX Mobile Enrollment, you can also specify whether to allow users to use their Microsoft Active Directory credentials to activate their devices.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **General settings**.
3. Click **Activation defaults**.
4. In the **Activation period expiration** field, enter the default time that an activation password (or QR Code) remains valid before it expires. The time can be from 1 minute to 30 days.
5. If necessary, select the **Activation period expires after the first device is activated** check box.
6. Select or clear the **Allow QR codes for device activation** check box. If selected, you can choose to send a QR Code to users instead of an activation password. If you don't select this option, the option to send a QR Code is not available in the activation email template.
7. If necessary, for devices that are activated using KNOX Mobile Enrollment, select **Allow use of Microsoft Active Directory username and password**.

8. Select or clear the **Send device activated notification** check box. If selected, the user receives an email message when a device is activated.
9. In the **Autogenerated activation password length** field, specify the length of the automatically generated activation password. The value can be from 4 to 16.
10. In the **Autogenerated password complexity** section, select one or more of the following options:
    - Lowercase letters
    - Uppercase letters
    - Numbers
    - Special characters or symbols
11. Select or clear the **Turn on registration with the BlackBerry Infrastructure** check box to modify how users activate their mobile devices. If you don't select this option, users will be asked to provide the server address for BlackBerry UEM when they activate devices. For more information, see Turn on user registration with the BlackBerry Infrastructure.
12. 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.

Select the "Device activation with specified activation profile" option when you create a user account or send an activation email message.

At a given time, 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: For activation passwords that are paired with specific activation profiles, the "Number of devices that a user can activate" setting 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 particular user at any time. For more information, see Manually expire an activation password.

Unlike regular activation passwords, 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.

Manually expire an activation password

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

1. On the menu bar, click **Users > Managed devices**.

2. Search for a user account.
3. In the search results, click the name of the user account.
4. In the **Activation details** section, locate the activation password that you want to expire. Click **Expire**. The activation password is expired immediately.

   If you expire a regular activation password, the date and time that you expire the password is displayed.

   If you expire an activation password that was paired with a specific activation profile, the details of the device activation password are no longer displayed.

Set an activation password and send an activation email message

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

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

Send an activation email to multiple users

You can send activation email messages to multiple users at one time. When you send an activation email to multiple users, the activation password is autogenerated. If you want to set the activation password, see Set an activation password and send an activation email message.

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. On the menu bar, click **Users > Managed devices**.
2. Select the check box for each user that you want to send an activation email to.
3. Click  .
4. In the **Activation option** drop-down list, perform one of the following tasks:
   - 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. Optionally, change the activation period expiration. The activation period expiration specifies how long the activation password remains valid.
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 BlackBerry 10, iOS, Android, and Windows devices to create their own activation passwords using BlackBerry UEM Self-Service.

Note: BlackBerry OS (version 5.0 to 7.1) device users can create activation passwords using BlackBerry Web Desktop Manager.

1. On the menu bar, click **Settings > General settings > Self-Service**.
2. Verify that **Allow users to access the self-service console** is selected.
3. Select **Allow users to activate devices in the self-service console** and complete the following tasks:
   a) Specify the number of minutes, hours, or days that a user can activate a device before the activation password expires.
   b) Specify the minimum number of characters required in an activation password.
   c) In the **Minimum password complexity** drop-down list, select the level of complexity required for activation passwords.
4. Click **Save**.

Supporting Android Enterprise activations

Organizations that use Android Enterprise devices have several options for connecting to Google services. How your organization uses Google services determines how you connect BlackBerry UEM to Google services and how you activate devices. For more information on configuring BlackBerry UEM to connect to a Google domain or use managed Google Play accounts, see the Configuration content.

Your organization may interact with Google services in the following ways:

Google services connection	Description	More information
Managed Google Play accounts	BlackBerry UEM is not connected to a Google domain. You can use managed Google Play accounts to allow users to download and install work apps using Google Play.	Support Android Enterprise activations using managed Google Play accounts Activate an Android Enterprise device with the Work and personal - user privacy activation type Activate an Android Enterprise device using a managed Google Play account
G Suite domain	Your organization has a G Suite domain, which supports all G Suite services such as Gmail, Google Calendar, and Google Drive.	Support Android Enterprise activations with a G Suite domain Activate an Android Enterprise device with the Work and personal - user privacy activation type Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain
Google Cloud domain	Your organization has a Google Cloud domain, which provides managed Google accounts to users. Your organization doesn't use G Suite services such as Gmail, Google Calendar, and Google Drive for your organization's email, calendar, and data management.	Support Android Enterprise activations with a Google Cloud domain Activate an Android Enterprise device with the Work and personal - user privacy activation type Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain
No Google services	Your organization's security policies do not allow you to use Google services.	Support Android Enterprise devices without access to Google Play Activate an Android Enterprise device without a Google Play account

If you support Android Enterprise activations, you can provide users with BlackBerry Hub which allows them to manage both work and personal email messages and calendar data in a unified view. For more information, see Enable a unified BlackBerry Hub.

Support Android Enterprise activations using managed Google Play accounts

If you don't have or don't want to connect BlackBerry UEM to a Google domain, you can activate Android Enterprise devices to use managed Google Play accounts. When you use managed Google Play accounts you can use any Google or Gmail account to connect BlackBerry UEM to Google and no personally identifiable information about your users is sent to Google. For more information on managed Google Play accounts, see https://support.google.com/googleplay/work/.

Once you have connected BlackBerry UEM to Google you can allow users to activate Android Enterprise devices and download work apps using Google Play. For information about configuring BlackBerry UEM to support Android Enterprise devices, see the Configuration content.

Support Android Enterprise activations with a G Suite domain

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

Before you begin: Configure BlackBerry UEM to support Android Enterprise devices. For information about configuring BlackBerry UEM to support Android Enterprise devices, see the Configuration content.

1. In your G Suite domain, create user accounts for your Android users.
2. Select the **Enforce EMM Policy** setting in the G Suite 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.
3. If you intend to assign the Work space only or Work and personal - full control activation type, select the **Enforce EMM Policy** setting in the G Suite domain.
4. In BlackBerry UEM, create local user accounts for your Android users. Each account's email address must match the email address in the corresponding G Suite account.
5. Make sure that your users know the passwords for their G Suite accounts.
6. In BlackBerry 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. When you configure BlackBerry UEM to connect to a Google Cloud domain, you must select whether BlackBerry UEM can create user accounts in the domain. This selection affects the tasks that you must perform before users can activate Android Enterprise devices. For information about configuring BlackBerry UEM to support Android Enterprise devices, see the Configuration content.

1. In BlackBerry UEM, add directory user accounts for your Android Enterprise users.
2. If you choose not to allow BlackBerry UEM to create user accounts in your Google Cloud domain, you must create user accounts in your Google Cloud domain and in BlackBerry UEM. Perform one of the following actions:

- In your Google Cloud domain, create user accounts for your Android Enterprise users. Each email address must match the email address in the corresponding BlackBerry 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 BlackBerry 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 (for example, due to local restrictions) with UEM, you must install the latest BlackBerry UEM Client on the device that you want to activate. The method that you use to download the UEM Client depends on the activation type:

- **Work space only (Android Enterprise) and Work and personal - full control (Android Enterprise)**: You must manually download the BlackBerry UEM Enroll app from BlackBerry and install it on a secondary device. The device that you want to activate must be reset to default factory settings and, before you complete the out-of-box device setup on the device, you use the UEM Enroll app on the secondary device to download the UEM Client using NFC.
- **Work and personal - user privacy (Android Enterprise)**: After the out-of-box device setup is completed on the device that you want to activate, you must manually download the UEM Client from BlackBerry and install it.

To download the .apk file of the latest UEM Enroll or UEM Client app, visit support.blackberry.com/community to read article 42607.

For more information about supporting Android Enterprise devices without access to Google Play, visit support.blackberry.com/community to read article 57492.

Requirements

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

Requirement	Description
BlackBerry UEM environment	Verify the following: • BlackBerry UEM server version 12.11 or later • **Integration with Android Enterprise**: You are not required to integrate UEM with Android Enterprise if you want to support only devices that don’t have access to Google Play. If you want to support a mix of devices that do and don’t have access to Google Play, you must integrate the UEM environment with Android Enterprise.

Requirement	Description
Activation profile settings	The following activation types are supported for devices that don't have access to Google Play: • Work space only (Android Enterprise) • Work and personal - full control (Android Enterprise) • Work and personal - user privacy (Android Enterprise) Verify the following settings in the activation profile: • Deselect the **Add Google Play account to workspace** option. This option is available only if your UEM environment is integrated with Android Enterprise. • 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 settings	Only for users that are assigned the Work and personal - user privacy (Android Enterprise) activation type, verify the following in the IT policy: • Enable the **Allow installation of non Google Play apps** IT policy rule to allow the installation of apps outside of Google Play.
Non-BlackBerry Dynamics apps	For non-BlackBerry Dynamics apps, add the apps to UEM as internal apps and assign them to users. 1. Obtain the .apk files of the apps that you want to assign. For example, to download the latest version of the BlackBerry Connectivity app, visit the BlackBerry myAccount portal. 2. In the BlackBerry UEM 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**.

Requirement	Description
BlackBerry Dynamics apps	For BlackBerry Dynamics apps, upload the internal app source file and assign the app to users. Perform the following steps to install or update internal apps on devices that don't have access to Google Play: 1. Obtain the .apk files of the BlackBerry Dynamics apps that you want to assign. For example, to download BlackBerry Work, visit support.blackberry.com/community and read article 42607. 2. In the BlackBerry UEM management console, on the menu bar, click **Apps**. 3. Click a BlackBerry Dynamics app (for example, BlackBerry Work). 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**.
Activating the devices	For devices assigned the Work space only (Android Enterprise) and Work and personal - full control (Android Enterprise) activation types, use the UEM Enroll app to initiate the download of the UEM Client. For more information, see the BlackBerry UEM Enroll documentation. For devices assigned the Work and personal - user privacy (Android Enterprise) activation type, manually download and install the UEM Client app. For more information, visit support.blackberry.com/community and read article 42607. **Note:** • The device on which you install UEM Enroll must be running Android 9 or earlier. • The device that you want to activate must be running Android 9 or earlier.
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. For more information, visit support.blackberry.com/community and read article 42607.

Enable a unified BlackBerry Hub

BlackBerry Hub is an app that allows users to view messages, notifications, and events in one spot.

To allow users with Android Enterprise devices to view both work and personal messages in BlackBerry Hub, you need to verify some settings in BlackBerry UEM.

1. For the IT policy that is assigned to users, in the BlackBerry Productivity Suite section, verify that the "Allow unified account view in BlackBerry Hub" IT policy rule is selected.
2. Perform one of the following tasks:

- If you configure the settings for BlackBerry Hub in an email profile, on the Android tab of the email profile, verify that the following items are selected:
  - Allow data to be shared between work and personal profiles
  - Allow personal app access to the work data
- If you configure the settings for BlackBerry Hub in an app configuration, verify that the following items are selected:
  - IPC across profiles
  - Access work content

After you finish:

For information about using the BlackBerry Hub on devices, such as adding an email account or customizing the BlackBerry Hub settings, see the BlackBerry Hub content.

For troubleshooting information, visit http://support.blackberry.com/community to read article 37721.

Supporting Windows 10 activations

You can help users activate Windows 10 devices in two ways:

- Deploy a discovery service to simplify Windows 10 activations. For more information, see the Configuration content.
- Create or edit an activation email template to provide Windows 10 activation information. For more information, see "Create an activation email template."

Enable user notification when a device has been activated

You can enable UEM to notify a user each time a device is activated on their account. The email notification is sent to the email address of the user account that was used to activate the device. By default, the email includes the device model, serial number, and IMEI. If the user receives a notification that they were not expecting, they should contact an administrator.

1. On the menu bar, click **Settings** > **General settings**.
2. Click **Activation Defaults**.
3. Select **Send device activated notification**.
4. Click **Save**.

Creating activation profiles

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

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

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

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

Activation profiles do not apply to BlackBerry OS (version 5.0 to 7.1) devices.

Create an activation profile

Note: If you enable attestation for your organization's BlackBerry UEM instance, during Android device activation, the authenticity and integrity of the device is checked. Ensure that users have BlackBerry UEM Client for Android version 12.9 MR1 or later installed on their devices before you enable this feature.

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

- For Android devices, you can select multiple activation types and rank them to meet your organization's requirements.
- The "MDM controls" activation type is deprecated for devices with Android 10 and later.
- For Android devices, if you select an Android Enterprise activation type, you can select the **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus.** option to enable BlackBerry Secure Connect Plus and KNOX Platform for Enterprise features (for devices that support Samsung KNOX).
- For Android devices, if you select the "MDM controls" activation type and you do not want KNOX MDM policy rules to be applied to the devices, clear the **Activate Samsung KNOX APIs on MDM Controls activations** check box. This setting applies only to devices that support KNOX MDM.
- For Android devices, if you select one of the Samsung KNOX activation types and want to use Google Play to manage work apps, select **Google Play app management for Samsung Knox Workspace devices**. This option is available only if you have configured a connection to a Google domain. For more information, see the Configuration content.
- For iOS devices, if you select the "User privacy" activation type and you want to enable SIM-based licensing, you must select the **Allow access to SIM card and device hardware information to enable SIM-based licensing** option.
- For iOS devices, if you select the "MDM controls" or User privacy (with SIM-based licensing) activation types, you can restrict unsupervised devices by selecting "Do not allow unsupervised devices to activate."

10. For Android devices, in the **SafetyNet attestation options** section, you can optionally select an attestation method. The choices are:
    - Perform SafetyNet attestation for device: BlackBerry UEM sends challenges to test the authenticity and integrity of devices.
    - Perform SafetyNet attestation on device activation: BlackBerry UEM sends challenges to test the authenticity and integrity of devices when they are activated.
    - Perform SafetyNet attestation on BlackBerry Dynamics app activation: BlackBerry UEM sends challenges to test the authenticity and integrity of BlackBerry Dynamics apps when they are activated.
11. For Android devices, in the **Hardware attestation options** section, you can optionally select an attestation method.
    - Perform hardware attestation on device activation: BlackBerry UEM sends challenges to devices when they are activated to ensure the required security patch level is installed
12. For iOS devices, in the **iOS app integrity check** section, you can optionally select an attestation method. The choices are:
    - Perform periodic app integrity checks: BlackBerry UEM sends challenges to devices check the integrity of iOSwork apps.
    - Perform app integrity check on BlackBerry Dynamics app activation: BlackBerry UEM sends challenges to devices when they are activated to check the integrity of iOSwork apps
13. Click **Add**.

After you finish: If necessary, rank profiles.

Activation step-by-step for users

If necessary, you can provide users with step-by-step instructions to activate devices.

The steps for individual users may differ slightly from those documented here depending on the user's device model and OS version.

Activating Android devices

The information that users must enter and the steps to activate an Android device are different depending on the activation type that is assigned to them. The activation email templates contain the information that users need. You can update the text in the email templates if necessary. For more information, see Email templates.

For QR Code activations, see Activate a device using a QR Code.

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

Send these activation instructions to users activating devices with the Work and personal - user privacy (Android Enterprise) activation type. The activation steps are the same whether you are using managed Google Play accounts or you are connected to a Google domain.

Before you begin:

- You need the following information:
  - BlackBerry UEM activation password
  - Your work email and password
- You might need the following information:
  - BlackBerry UEM server address
  - Google account password

1. On the device, install the BlackBerry UEM Client. You can download the UEM Client from Google Play.
2. On the device, tap **UEM Client**.
3. Read the license agreement. Tap **I Agree**.
4. Tap **Allow** to allow UEM Client to make and manage phone calls.
5. Type your work email address. Tap **Next**.
6. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
7. Type your activation password. Tap **Activate My Device**.
8. Wait while the profiles and settings are pushed to your device.
9. Tap **Accept & continue** to create a work profile on the device.
10. If necessary, type your Google password. Tap **Next**.
11. If prompted, you can set up a device password and select notification options.
12. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.

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. If users are activating Work and personal - user

privacy devices, send them instructions to 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: Make sure you have the following information that was sent by your administrator in one or more email messages:

- BlackBerry UEM activation password
- Your work email and password
- BlackBerry UEM server address (you might not need this)

1. If you do not see the device setup Welcome screen, reset your device to the factory default setting.
2. During the device setup, in the **Add your account** screen, enter your work email address and password
3. If you are prompted, encrypt the device.
4. On the device, tap **Install** to install the BlackBerry UEM Client.
5. Read the license agreement. Tap **I Agree**.
6. Tap **Allow** to allow UEM Client to make and manage phone calls.
7. Type your work email address. Tap **Next**.
8. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
9. Type your activation password. Tap **Activate My Device**.
10. Wait while the profiles and settings are pushed to your device.
11. On the **Set up your device** screen, tap **Accept & Continue** and wait while the work profile is set up.
12. On the **Unlock selection** screen, choose an unlock method.
13. On the **Secure start-up** screen tap **Yes** to require a password when the device starts.
14. Type a device password, type it again to confirm it. Tap **OK**.
15. Select one of the options for how you want your notifications to show. Tap **Done**.
16. If prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.

Activate an Android Enterprise device using a managed Google Play account

These steps apply to devices that are assigned the Work space only (Android Enterprise) or Work and personal - full control (Android Enterprise) activation type. If users are activating Work and personal - user privacy devices, send them instructions to 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: Make sure you have the following information that was sent by your administrator in one or more email messages:

- Activation username
- BlackBerry UEM activation password

1. If you do not see the device setup Welcome screen, reset your device to the factory default setting.
2. During the device setup, in the **Add your account** screen, type afw#blackberry.
3. On the device, tap **Install** to install the BlackBerry UEM Client.
4. Read the license agreement. Tap **I Agree**.
5. Tap **Allow** to allow UEM Client to make and manage phone calls.
6. Type your work email address. Tap **Next**.

7. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
8. Type your activation password. Tap **Activate My Device**.
9. Wait while the profiles and settings are pushed to your device.
10. On the **Set up your device** screen, tap **Accept & Continue** and wait while the work profile is set up.
11. On the **Unlock selection** screen, choose an unlock method.
12. On the **Secure start-up** screen tap **Yes** to require a password when the device starts.
13. Type a device password, type it again to confirm it. Tap **OK**.
14. Select one of the options for how you want your notifications to show. Tap **Done**.
15. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.

Activate an Android Enterprise device without a Google Play account

These steps apply to devices that do not have access to Google Play. The devices may be assigned the Work space only (Android Enterprise), Work and personal - full control (Android Enterprise), or Work and personal - user privacy (Android Enterprise) activation type.

A secondary device that has the BlackBerry UEM Enroll app installed is required. The same device can be used to help activate an unlimited number of devices with UEM.

Send the following activation instructions to the device user.

Before you begin:

- Make sure you have the following information that was sent by your administrator in one or more email messages:
  - Activation username
  - BlackBerry UEM activation password
- You must have a secondary device that has the BlackBerry UEM Enroll app installed. To download and install the app on a secondary device, visit support.blackberry.com/community to read article 42607.

1. On the device that you want to activate, if you do not see the device setup Welcome screen, reset your device to the factory default setting.
2. On the secondary device, open the BlackBerry UEM Enroll app. Make sure that NFC is enabled on the device.
3. Tap **Activate device**.
4. Tap the backs of both devices together.
5. On the device that you want to activate, follow the instructions on the screen to download and install the BlackBerry UEM Client.
6. Read the license agreement. Tap **I Agree**.
7. Tap **Allow** to allow UEM Client to make and manage phone calls.
8. Type your work email address. Tap **Next**.
9. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
10. Type your activation password. Tap **Activate My Device**.
11. Wait while the profiles and settings are pushed to your device.
12. On the **Set up your device** screen, tap **Accept & Continue** and wait while the work profile is set up.
13. On the **Unlock selection** screen, choose an unlock method.
14. On the **Secure start-up** screen tap **Yes** to require a password when the device starts.
15. Type a device password, type it again to confirm it. Tap **OK**.

16. Select one of the options for how you want your notifications to show. Tap **Done**.
17. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.
18. If necessary, open the email app that your organization wants you to use (for example, BlackBerry Hub) and follow the instructions to set up email on your phone.

Activate an Android device with the MDM controls activation type

Note: These steps apply only to devices assigned the MDM controls activation type. This activation type is deprecated for devices with Android 10. Attempts to activate Android 10 and later devices with the MDM controls activation type will fail. For more information, visit https://support.blackberry.com/community to read article 48386.

Send the following activation instructions to the device user.

1. On the device, install the BlackBerry UEM Client. You can download the BlackBerry UEM Client from Google Play.
2. On the device, tap **UEM Client**.
3. Read the license agreement. Tap **I Agree**.
4. Type your work email address. Tap **Next**.
5. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
6. Type your activation password. Tap **Activate My Device**.
7. Tap **Next**.
8. Tap **Activate**.

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

- On the device, open BlackBerry UEM Client. Tap **About**. In the **Activated Device** section, 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 iOS devices

The information that users must enter and the steps to activate an iOS device may be different depending on the iOS version and whether the activation type includes MDM controls. The activation email templates contain the information that users need. You can update the text in the email templates if necessary. For more information, see Email templates.

For QR Code activations, see Activate a device using a QR Code.

Activate an iOS version 12.2 or later device with the MDM controls activation type

These steps apply to devices with iOS version 12.2 or later that are enrolled using MDM controls or using User Privacy with MDM options enabled.

During MDM enrollment on iOS version 12.2 or later, users must leave the BlackBerry UEM Client app to manually install the MDM profile. These steps are not required for earlier versions of iOS.

Send the following activation instructions to the device user.

1. On the device, install the BlackBerry UEM Client app. You can download the BlackBerry UEM Client app from the App Store.
2. On the device, tap **UEM Client**.
3. Read the license agreement and tap **I Agree**.
4. Do one of the following:
   - Use a QR Code to activate your device. Scan the QR Code that you received in the activation email or that you generated in BlackBerry UEM Self-Service.
   - Manually activate your device.
     - Type your work email address and tap **Go**.
     - If necessary, type the server address and tap **Go**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
     - Type your activation password and tap **Activate My Device**.
5. When prompted to install a certificate, tap **OK**.
6. When prompted to download the configuration profile, tap **Allow**.
7. After the download is complete, open **Settings**.
8. Tap **General** and navigate to **Profiles**.
9. To install the profile, tap **UEM Profile**.
10. After the installation is complete, return to the BlackBerry UEM Client app to complete the enrollment.

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

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

Activate an iOS device

For QR Code activations, see Activate a device using a QR Code.

To activate devices using an activation password, send the following instructions to the device user.

1. On the device, install the BlackBerry UEM Client app. You can download the BlackBerry UEM Client app from the App Store.
2. On the device, tap **UEM Client**.
3. Read the license agreement and tap **I Agree**.
4. Type your work email address and tap **Go**.
5. If necessary, type the server address and tap **Go**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
6. Type your activation password and tap **Activate My Device**.
7. Tap **OK** to install the required certificate.
8. Follow the instructions on the screen to complete the activation.
9. If you are prompted to enter the password for your email account or the passcode for your device, follow the instructions on the screen.

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

- On the device, open the BlackBerry UEM Client app and tap **About**. In the Activated Device and Compliance Status sections, verify that the device information and the activation time stamp are present.

- In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Activate a macOS device

Send the following activation instructions to the device user.

Before you begin: You need the following BlackBerry UEM Self-Service login information:

- Web address for BlackBerry UEM Self-Service
- Username and password
- Domain name

1. Using the device that you want to activate, and the login information that you received from your administrator, log in to BlackBerry UEM Self-Service.
2. If there are already devices displayed, click **Activate a device**.
3. In the Device drop-down menu, click **macOS**.
4. Watch the activation tutorial.
5. Click **Submit**.
6. Follow the instructions to install the required profiles and to complete the activation of the device. When the activation completes, you can see your device displayed in BlackBerry UEM Self-Service.

Activate an Apple TV device

Send the following activation instructions to the device user.

Before you begin:

- You need the web address and your login credentials for BlackBerry UEM Self-Service.
- You need a macOS computer with Apple Configurator 2 installed.
- You need a USB-C or Micro-USB cable (depending on the version of Apple TV).
- Verify that the Apple TV device is in supervised mode.
- Disconnect the HDMI cable and power cord from the Apple TV device.

1. Connect the Apple TV device to your macOS computer using a USB-C or Micro-USB cable.
2. For third and fourth generation versions of Apple TV, connect the power cord.
3. On your macOS computer, log in to BlackBerry UEM Self-Service.
4. Depending on whether you are activating your first device, or you already have an activated device, click  or click  > **Activate a device**.
5. In the Device drop-down menu, click **Apple TV**.
6. Click **Submit**.
7. Click **Download profile**.
8. Click **Close**.
9. Open Apple Configurator 2.
10. Select Apple TV and click **Add > Profiles**.
11. Select the configuration file that you downloaded in Step 7 and click **Add**.
12. When the activation completes, you can see your device displayed in BlackBerry UEM Self-Service.

Activate a Windows 10 tablet or computer

Note: If you want to manage Windows 10 devices using MDM, the devices cannot be managed by Microsoft System Center Configuration Manager.

Send the following activation instructions to the device user.

1. In the browser on your device, type or paste the certificate server address. You can find the certificate server address in the activation email you received. If you did not receive a link to the certificate, contact your administrator for assistance.
2. Click **Save**.
3. In the certificate download notification, tap **Open**.
4. Click **Open**.
5. Click **Install Certificate**.
6. Select the **Current User** option. Click **Next**.
7. Select the **Place all certificates in the following store** option. Click **Browse**.
8. Select **Trusted Root Certification Authorities**. Click **OK**.
9. Click **Next**.
10. Click **Finish**.
11. Click **OK**.
12. Click **OK**.
13. Click the **Start** button.
14. Perform one of the following tasks:

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**.

15. In the **Email address** field, type your email address. Tap **Continue**.
16. 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.
17. 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 BlackBerry UEM Self-Service.
18. Tap **Done**.
19. The activation process is complete.

After you finish:

- To verify that the activation process completed successfully, you can perform the following actions:
  - On the device, click Settings > Accounts > Access work or school (or Work access) to confirm that your device is connected to BlackBerry UEM. Click the briefcase icon > Info to check the sync status information.
  - 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.

- 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.

Activate a Windows 10 Mobile device

Send the following activation instructions to the device user.

1. In the browser on your device, type or paste the certificate server address. You can find the certificate server address in the activation email you received. If you did not receive a link to the certificate, contact your administrator for assistance.
2. Tap the certificate.
3. Tap **install**.
4. Tap **ok**.
5. Tap the **Windows** button to return to the Start menu.
6. Swipe left to open the apps menu.
7. Perform one of the following tasks:

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**.

8. In the **Email address** field, type your work email address and tap **Enter**.
9. 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.
10. In the **Activation password** field, type your activation password and tap **Continue**. You can find your activation password in an email that you received from your administrator, or you can set your own activation password in BlackBerry UEM Self-Service.
11. Tap **Finished**.
12. The activation process is complete.

After you finish:

- To verify that the activation process completed successfully, you can perform the following actions:
  - On the device, click Settings > Accounts > Access work or school (or Work access) to confirm that your device is connected to BlackBerry UEM. Click the briefcase icon > Info to check the sync status information.
  - 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.
- 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.

Activate a BlackBerry 10 device

Send the following activation instructions to the device user.

1. On the device, navigate to **Settings**.
2. Tap **Accounts**.
3. If you have existing accounts on this device, tap **Add Account**. Otherwise, continue to Step 4.
4. Tap **Email, Calendar and Contacts**.
5. Type your work email address and tap **Next**.
6. In the **Password** field, type the activation password you received. Tap **Next**.
7. If you receive a warning that your device could not look up connection information, complete the following steps:
   a) Tap **Advanced**.
   b) Tap **Work Account**.
   c) In the **Server Address** field, type the server address. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
   d) Tap **Done**.
8. 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, navigate to the BlackBerry Hub and confirm that the email address is present. Navigate to the Calendar and confirm that the appointments 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 a BlackBerry OS device

Send the following activation instructions to the device user.

1. On the device, navigate to **Setup**.
2. Click **Email Accounts**.
3. Click **Enterprise Account**.
4. In the **Email** field, type your work email address.
5. In the **Password** field, type the activation password you received.
6. Click **Activate**.
7. Click **OK**.

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

- On the device, navigate to the Setup app and click **Email Accounts**. Confirm that the email address is present.

- In BlackBerry Web Desktop Manager, 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 a device using a QR Code

QR Code activation is supported on iOS and Android devices.

To activate devices using a QR Code, send the following instructions to the device user.

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

1. On the device, install the BlackBerry UEM Client app. For iOS devices, download the app from the App Store. For Android devices, download the app from Google Play.
2. On the device, tap **UEM Client**.
3. Read the license agreement and tap **I Agree**.
4. Scan the QR Code that you received in the activation email or that you generated in BlackBerry UEM Self-Service.
5. If you are prompted to enter the password for your email account or the passcode for your device, follow the instructions on the screen.

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

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

Activate multiple devices using zero-touch enrollment for Android Enterprise devices

Zero-touch enrollment allows you to deploy a large number of Android Enterprise devices at one time.

Your organization purchases these devices from an authorized enterprise reseller, who sets up a zero-touch enrollment account and adds the devices to the account to provision them for device management. When users set up these devices for the first time, the devices will automatically download the BlackBerry UEM Client and start the activation process with BlackBerry UEM. The user must complete the activation process to use the device.

For more information about zero-touch enrollment and how to configure it, see the Android Enterprise Help and https://support.google.com/work/android/answer/7514005.

To use zero-touch enrollment in BlackBerry UEM, devices must be running Android 8.0 or later and have been enabled for zero-touch enrollment.

1. Purchase supported devices from an approved enterprise reseller. The reseller sets up a zero-touch enrollment account for your organization.
2. In the zero-touch platform, the reseller adds the devices that you purchased.
3. In the BlackBerry UEM management console, on the menu bar, click **Settings > External integration**.
4. Click **Android enterprise**.
5. At the bottom of the screen, click **Learn more**.
6. Copy the string generated by this BlackBerry UEM instance for use when configuring devices in the zero-touch enrollment portal.

   You can either leave the username field blank or edit it to include a username so that only that username can be used to log in to the device that uses the configuration.
7. In the zero-touch platform, create configurations and assign them to the devices that you purchased.
8. In BlackBerry 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 fully managed device with work profile)" or "Work space only (Android Enterprise fully managed device) " activation type enabled.
9. Distribute the devices to users.

Activate multiple devices using KNOX Mobile Enrollment

Samsung KNOX Mobile Enrollment allows you to activate large numbers of devices in BlackBerry UEM at one time. For more information, visit https://www.samsungknox.com/en/products/knox-mobile-enrollment.

Before you begin: You need to purchase devices from one of the following:

- An approved reseller
- A reseller that is willing to share the device IMEIs directly with Samsung

1. On the menu bar, click **Settings > External integration**.
2. Click **KNOX Mobile Enrollment**.
3. Complete the steps on the screen.

After you finish: After you have completed the activation, click **Download** to download the configuration.json file. In the file, compare the entry in the CFPrint section with the entry that you added when you configured KNOX Mobile Enrollment. If the entries are different, copy the entire text from the .json file into the Custom JSON Data field on the KNOX Mobile Enrollment page.

Restricting unsupervised iOS devices

There are two ways to restrict unsupervised iOS devices in BlackBerry UEM:

- For devices that are enrolled in DEP, you can assign an enrollment configuration to devices that has the "Enable supervised mode" setting selected. When devices are activated, they are automatically activated in supervised mode. For more information, see Assign an enrollment configuration to iOS devices.
- You can assign an activation profile that has the "Do not allow unsupervised devices to activate" setting selected to user accounts. This setting is supported for the "MDM controls" and "User privacy" (with SIM-based licensing enabled) activation types. BlackBerry UEM prevents unsupervised devices from activating and automatically removes devices if they become unsupervised, whether the devices are activated with the BlackBerry UEM Client or using DEP. For more information, see Create an activation profile.

Activating iOS devices that are enrolled in DEP

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

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

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

Note: For certain features to work, you must assign the BlackBerry UEM Client app to the users. Users must start the BlackBerry UEM Client after they activate the device. For information about when you need to assign the BlackBerry UEM Client app to users, visit support.blackberry.com/community to read article 39313.

Steps to activate devices that are enrolled in DEP

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

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

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

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

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

Before you begin: Configure BlackBerry UEM to use DEP. For more information, see the Configuration content.

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

After you finish: Assign an enrollment configuration to iOS devices.

Assign an enrollment configuration to iOS devices

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

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

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

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

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

1. On the menu bar, click **Users > Apple DEP devices**.
2. Select the check boxes beside the devices that you want to assign an enrollment configuration to. You must select devices that are registered to the same DEP account.
3. Click .
4. In the **Enrollment configuration** drop-down list, select the enrollment configuration that you want to assign.

5. Click **Assign**.

After you finish:

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

Add an enrollment configuration

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

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

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

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

- Siri - if selected, Siri is disabled on devices
- Diagnostics - if selected, diagnostic information is not automatically sent from the device during setup
- Biometric - if selected, users cannot set up Touch ID
- Payment - if selected, users cannot set up Apple pay
- Zoom - if selected, users cannot set up Zoom
- Home button setup - if selected, users cannot adjust the Home button's click

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

After you finish: If you did not select "Automatically assign new devices to this configuration", see Assign an enrollment configuration to iOS devices.

Remove an enrollment configuration that is assigned to iOS devices

If you assigned an enrollment configuration to devices and the configuration is not yet applied to the devices, you can remove the enrollment configuration from the devices.

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

After you finish: Assign an enrollment configuration to iOS devices.

Delete an enrollment configuration

If you delete an enrollment configuration that is assigned to devices before the configuration is applied to the devices, BlackBerry UEM removes the enrollment configuration assigned to the device records.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Apple Device Enrollment Program**.
3. Click the name of a DEP account.
4. In the **DEP enrollment configurations** section, click ✕.
5. Click **Delete**.

After you finish: If BlackBerry UEM removes the enrollment configuration from devices, assign an enrollment configuration to the devices.

Change the settings for an enrollment configuration

If you assigned an enrollment configuration to devices and the configuration is not applied to the devices, BlackBerry UEM updates the enrollment configuration assigned to the devices when you save the changes to the configuration.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Apple Device Enrollment Program**.
3. Click the name of a DEP account.

4. In the **DEP enrollment configurations** section, click the name of the configuration you want to change.
5. Change the settings.
6. Click **Save**.

View the settings for an enrollment configuration that is assigned to a device

If an enrollment configuration is assigned to an iOS device and the configuration is pending, you can view the settings for the enrollment configuration.

1. On the menu bar, click **Users > Apple DEP devices**.
2. In the **Enrollment configuration** column, click the name of an enrollment configuration.

View user details for an activated device

After a device is successfully activated, you can view details associated with the user, such as the groups that the user is assigned to.

1. On the menu bar, click **Users > Apple DEP devices**.
2. In the **Display name** column, click the name of a user.

Activating iOS devices using Apple Configurator 2

You can use Apple Configurator 2 to prepare iOS devices for activation in BlackBerry UEM. Users can activate the prepared devices without using the BlackBerry UEM Client app. They need only their username and activation password.

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

Note: For certain features to work, you must assign the BlackBerry UEM Client app to the users. Users must start the BlackBerry UEM Client after they activate the device. For information about when you need to assign the BlackBerry UEM Client app to users, visit support.blackberry.com/community to read article 39313.

Steps to activate devices using Apple Configurator 2

Step	Action
1	Optionally, add the BlackBerry UEM Client app 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	Set an activation password and send an activation email message.
6	Distribute the devices to users and have them complete the setup. To enforce a compliance profile, users must install and open the BlackBerry UEM Client app after the setup is complete.

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 BlackBerry UEM server URL using the format: *<http or https>://<servername>:<port>*, where the default port number is 8885. For more information about port settings, see BlackBerry UEM listening ports in the Planning content.
5. Click **Next**.

6. Close the **Server** window.

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** checkbox. 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.

Activating BlackBerry 10 devices using the BlackBerry Wired Activation Tool

The BlackBerry Wired Activation Tool allows you to activate multiple BlackBerry 10 devices at the same time using USB connections instead of wireless connections. Your organization may want to use this method for different reasons:

- To make it quick and easy to activate multiple devices at once
- To keep the activation process in the hands of administrators
- To activate devices and configure their security features, such as content encryption requirements and VPN profiles, before giving them to users or connecting them to your organization's network

You can't assign profiles and policies using the BlackBerry Wired Activation Tool. You must assign any profiles and policies to your users in the BlackBerry UEM management console before assigning and activating devices using the BlackBerry Wired Activation Tool. However, you don't need to set any activation passwords to assign and activate devices using the BlackBerry Wired Activation Tool.

To activate devices using the BlackBerry Wired Activation Tool, the devices must be running BlackBerry 10 OS version 10.3 or later.

To obtain the BlackBerry Wired Activation Tool contact your Customer Support representative.

Install the BlackBerry Wired Activation Tool

Complete the following steps to download and install the BlackBerry Wired Activation Tool

1. Browse to the server software download page in *my*Account.
2. Click **Download UEM tools**
3. In the drop-down list, click BlackBerry Wired Activation Tool.
4. Click **Next**.
5. Click **Download**.
6. Select the Yes or No option and click **Download**.
7. Save the install file to your computer.
8. On your computer, browse to the location where you saved the install file.
9. Follow the instructions on the screen to complete the installation.

Configure the BlackBerry Wired Activation Tool and log in to a BlackBerry UEM instance

Before you can activate devices with the BlackBerry Wired Activation Tool, you must create a configuration for each BlackBerry UEM instance you need to access. After you create a configuration, you must also use an administrator account to allow the BlackBerry Wired Activation Tool to access BlackBerry Web Services.

1. In the BlackBerry Wired Activation Tool installation folder, double-click the **BWAT.exe** file.
2. In the **Add a BES12 server screen**, in the **Name** field, type a name to identify the configuration you're creating. For example, if you have two BlackBerry UEM instances, you might create a configuration for each one and name them Server 1 and Server 2.

3. In the **BlackBerry Web Services URL** field, type the address for the BlackBerry Web Services component. The default address is https://<*BlackBerry UEM web address*>:18084.

   You can change the port by modifying the `tomcat.bws.port` setting in the BlackBerry UEM database.
4. In the **BCP Endpoint URL** field, type the address to use for device activations. This is also known as the Activation URL or Server name. The default address is: http://*server.name*:8882/*SRP_ID*/mdm.

   You can find the address by making sure the %ActivationURL% variable is in the Activation email template and clicking **View activation email** from any User summary screen.

   If necessary, you can also look up the host address and port in the BlackBerry UEM database. In the `def_cfg_setting_dfn` table, find the `id_setting_definition` values for `bdmi.enroll.bcp.host` and `bdmi.enroll.bcp.port`. Then use the `id_setting_definition` values to look up the values of those settings in the `obj_global_cfg_setting`.
5. Click **Submit**.
6. In the **Log in** screen, select a BlackBerry UEM configuration from the drop-down list.
7. In the **Username** field, type the username of a BlackBerry UEM user account with administrator permissions.
8. In the **Password** field, type the password for the account.
9. In the **Directory** drop-down list, select an authentication method.
10. If required, in the **Domain** field, type the Microsoft Active Directory domain.
11. Click **Log in**.

Activate BlackBerry 10 devices using the BlackBerry Wired Activation Tool

Before you begin:

- Configure the BlackBerry Wired Activation Tool and log in to a BlackBerry UEM instance.
- Turn on all connected devices and make sure that all devices have either completed the initial setup process, or that they haven't started it. You can't activate devices if the initial setup process is in progress.

1. Connect one or more BlackBerry 10 devices to your computer using USB cables.
2. Check the **Status** column for each device. Perform one of the following actions:
   - If the Status column displays **Requires password**, click **Requires password** to enter the password for the device
   - If the Status column displays **Unsupported device**, upgrade the device software to BlackBerry 10 OS version 10.3 or later
   - If the Status column displays **Ready**, assign the device to a user
3. In the **Search** field, search for a user account that you want to assign a device to.
4. In the list of search results, click the user account.
5. In the main section of the screen, click a user account name and drag the name to a device to assign the device to that user. Repeat this step to assign devices to multiple users.
6. Select the checkbox next to the user and device pairs that you want to activate.
7. Click **Activate devices**.

The BlackBerry Wired Activation Tool activates all the devices you selected. Check the Status column for the progress and results for each device. If an activation doesn't complete, click the message in the Status column for more information about errors.

Tips for troubleshooting device activation

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

- Make sure that BlackBerry UEM supports the device type. For more information about supported device types, see the Compatibility matrix.
- Make sure that there are licenses available for the device type the user activates and the activation type that is assigned to the user. For more information, see the Licensing content.
- Check network connectivity on the device.
  - Verify that the mobile or Wi-Fi network is active and has sufficient coverage.
  - If the user must manually configure a VPN or work Wi-Fi profile to access content behind your organization's firewall, make sure that the user's profiles are configured correctly on the device.
  - If on work Wi-Fi, make sure that the device network path is available. For more information on configuring network firewalls to work with BlackBerry UEM, visit support.blackberry.com/community to read article 36470.
- Make sure that the activation profile assigned to the supports the device type being activated.
- If you have defined compliance rules for devices with a jailbroken or rooted OS, restricted OS versions, or restricted device models, verify that the device is compliant.
- If the device is trying to connect with BlackBerry UEM or the BlackBerry Infrastructure through your organization's firewall, verify that the proper firewall ports are open. For more information about required ports, see the Planning content.
- Gather device logs:
  - For more information on retrieving BlackBerry 10 device log files, visit support.blackberry.com/community to read article 26038.

    Note: BlackBerry 10 device log files are encrypted. To use BlackBerry 10 device log files for troubleshooting purposes, you must have an open ticket with BlackBerry Technical Support Services. Only support agents can decrypt the log files.
  - For more information on retrieving iOS device log files, visit support.blackberry.com/community to read article 36986.
  - For more information on retrieving Android device log files, visit support.blackberry.com/community to read article 32516.

KNOX Workspace and Android Enterprise devices

When you troubleshoot activation of Samsung devices that use Samsung KNOX Workspace, check the following:

- Make sure the device supports KNOX Workspace. See the information from Samsung.
- Make sure that the Warranty Bit has not been triggered. See the information from Samsung.
- Make sure that the KNOX container version is supported. KNOX Workspace requires KNOX Container 2.0 or later. For more information about supported Samsung KNOX versions, see the list from Samsung.

When you troubleshoot activation of Android Enterprise devices, check the following:

- Make sure the device supports Android Enterprise. For more information, visit https://support.google.com/work/android/answer/6174145 to read article 6174145.
- Make sure that there is an available license and the activation type is set to Work and personal - user privacy .
- To use the Work and personal - user privacy activation type, devices must be running Android OS version 5.1 or later.

- Make sure that the user account in BlackBerry UEM has the same email address as the one in the Google domain. If the email addresses do not match, the device will show the following error: Unable to activate device - Unsupported activation type. Look for the following in the core log file:
  - ```
    ERROR AfW: Could not find user in Google domain. Aborting user creation and
     activation.
    ```
  - ```
    ERROR job marked for quarantine due to: Unable to activate device -
     Unsupported activation type
    ```

Device activation can't be completed because the server is out of licenses. For assistance, contact your administrator.

Description

This error is displayed on the device during activation when licenses are not available or the licenses have expired.

Possible solution

In BlackBerry UEM, perform the following actions:

- Verify that licenses are available to support activation.
- If necessary, activate licenses or purchase additional licenses.

For more information, see "Managing licenses for devices".

Please check your username and password and try again

Description

This error is displayed on a device during activation when a user has entered an incorrect username, password, or both.

Possible solution

Enter the correct username and password.

Profile failed to install. The certificate "AutoMDMCert.pfx" could not be imported.

Description

This error is displayed on an iOS device during activation when a profile already exists on the device.

Possible solution

Go to **Settings > General > Profiles** on the device and verify that a profile already exists. Remove the profile and reactivate. If the issue persists, you might have to reset the device because data might be cached.

Error 3007: Server is not available

Description

This error can appear on the device during activation because of the following:

- The certificate that BlackBerry UEM uses to sign the MDM profile that it sends to iOS devices is not trusted by the device. The user is asked to trust this certificate when they activate the device.
- If you configure a transparent proxy such as Blue Coat and it monitors port 443 for non-standard traffic, the BlackBerry UEM Client cannot make the required HTTP CONNECT and HTTP OPTIONS calls to BlackBerry UEM.

Possible solutions

Possible solutions include:

- Install the root certificate for the CA that issued the certificate that BlackBerry UEM uses to sign the MDM profile to the iOS device. For more information about this certificate, see the Configuration content.
- Verify that your proxy configuration is not blocking the BlackBerry UEM Client from making HTTP CONNECT and HTTP OPTIONS calls to BlackBerry UEM. For more information, visit support.blackberry.com/community to read article 38644.

Unable to contact server, please check connectivity or server address

Description

This error can appear on the device during activation because of the following:

- The username was entered incorrectly on the device.
- The customer address for device activation was entered incorrectly on the device.

  Note: This is only required when registration with the BlackBerry Infrastructure has been disabled.
- No activation password has been set, or the password has expired.

Possible solutions

Possible solutions include:

- Verify the username and password.
- Verify the customer address for device activation.
- Set a new activation password using BlackBerry UEM Self-Service.

iOS or macOS device activations fail with an invalid APNs certificate

Possible cause

If you are unable to activate iOS or macOS devices, the APNs certificate may not be registered correctly.

Possible solution

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 BlackBerry 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.

Users are not receiving the activation email

Description

Users are not receiving their activation email, even though all of the settings in BlackBerry UEM are correct.

Possible solution

If users are using a third-party mail server, email messages from BlackBerry UEM can be marked as spam and end up in the spam email folder or the junk mail folder.

Make sure that users have checked their spam email folder or junk mail folder for the activation email.

User details screen is showing more Windows devices activated with UEM than expected

Description

When a user installs BlackBerry Access and BlackBerry Work for Windows on a computer, BlackBerry Access and BlackBerry Work for Windows appear as a "Windows device" on the User details screen in the BlackBerry UEM management console. 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