



BlackBerry UEM

Managing iOS devices

Administration

12.16

Contents

- Managing iOS and iPadOS devices..... 4**
 - Managing other Apple devices.....4
- What you can control on iOS devices.....5**
- Steps to manage iOS devices..... 7**
- Controlling devices with an IT policy..... 8**
 - Setting iOS and password requirements.....8
- Controlling devices with profiles..... 10**
 - Profiles reference - iOS devices..... 11
- Managing apps on devices.....14**
 - App behavior on iOS devices with MDM controls activations..... 14
 - App behavior on iOS devices with User privacy activations..... 18
- Activating iOS devices..... 21**
 - Activation types: iOS devices..... 21
 - Creating activation profiles..... 23
 - Create an activation profile..... 23
 - Activate an iOS or iPadOS device with the MDM controls activation type..... 24
 - Activate an iOS or iPadOS device with Apple User Enrollment..... 25
- Managing and monitoring activated devices..... 27**
 - Send a command to a device..... 27
 - Commands for iOS devices.....28
- Legal notice..... 31**

Managing iOS and iPadOS devices

BlackBerry UEM provides precise management of how iOS and iPadOS devices connect to your network, what device capabilities are enabled, and what apps are available. Whether devices are owned by your organization or your users, you can provide mobile access to your organization's information while protecting it from anyone who should not have access.

Apple introduced iPadOS as a distinct operating system from starting with iPadOS version 13. Due to the extensive similarities between iOS and iPadOS, almost all BlackBerry UEM features and documentation that apply to iOS also apply to iPadOS.

This guide describes the options you have to manage iOS and iPadOS devices and helps you find the details you need to take advantage of all available features.

Managing other Apple devices

You can also activate and manage macOS and Apple TV devices in BlackBerry UEM. Apple TV is a digital media player that can receive data and stream it to a television over an HDMI cable.

BlackBerry UEM supports Apple TV versions that are second generation or later. For more information on supported macOS versions, [see the Compatibility Matrixes](#). To manage Apple TV devices, follow the instructions and use the profile settings for iOS devices. The following BlackBerry UEM features are supported for Apple TV:

- Device activation using BlackBerry UEM Self-Service
- MDM controls activation type
- Wi-Fi and certificate profiles
- App lock mode profiles
- Device commands

To prevent users from activating Apple TV devices, set the device model restriction in the activation profile to not allow any Apple TV devices. For more information on activating macOS and Apple TV devices, [see the Device activation content](#).

What you can control on iOS devices

BlackBerry UEM provides all of the tools you need to control the features that iOS and iPadOS devices allow you to manage. It also includes features that allow you to give device users secure access to work resources without fully managing the device.

Control level	Description
Unmanaged and partially managed devices (devices that are activated on BlackBerry UEM but not fully managed)	<p>You can activate a device on BlackBerry UEM to provide secure access to work resources without fully managing the device. This option is often used for BYOD devices.</p> <p>These activations can allow users to access your network over VPN using BlackBerry 2FA, share files securely using BlackBerry Workspaces, and install BlackBerry Dynamics apps such as BlackBerry Work and BlackBerry Access to access work email and your work intranet.</p>
Partially managed devices with a work profile	<p>You can activate a device on BlackBerry UEM to provide secure access to work resources within a work profile. This option is often used for BYOD devices.</p> <p>With this activation type, a separate work space is created on the device for work apps and the native Notes, iCloud Drive, Mail (attachments and full email bodies), Calendar (attachments), and iCloud Keychain apps.</p>
Managed devices (devices that are managed by BlackBerry UEM)	<p>You can activate a device to be fully managed by BlackBerry UEM. This option is often used for corporate-owned devices.</p> <p>This option lets you manage work data using commands and IT policy rules. You can manage work apps on the device, including BlackBerry Dynamics apps.</p> <p>BlackBerry UEM supports managing supervised iOS devices. Some IT policy rules are supported only on supervised devices</p>

User privacy activations can provide limited device management capabilities and allow users to access work data using BlackBerry Dynamics apps, such as BlackBerry Work and BlackBerry Access. You can choose to allow some of the following device management features:

- Access to SIM card and device hardware information: Allow BlackBerry UEM access to SIM card and device hardware information to enable SIM-based licensing.
- App management: Allow administrators to install or remove work apps and display a list of installed work apps in the user details screen.
- IT policy management: Allow a limited set of IT policy rules to be applied to the device (password policies, allow screenshots, allow documents from managed sources in unmanaged destinations, and allow documents from unmanaged sources in managed destinations).
- Email profile management: Allow email profiles to be applied to the device.
- Wi-Fi profile management: Allow Wi-Fi profiles to be applied to the device.
- VPN profile management: Allow VPN profiles to be applied to the device.

User privacy - User enrollment activations keep user data private and separate from work data. With this activation type, a separate work space is installed on the device for work apps and some native apps. This activation type enables app management, IT policy management, email profiles, Wi-Fi profiles, and per-app VPN. Administrators can manage work data (for example, wipe work data) without affecting personal data.

This activation type is supported on unsupervised devices that run iOS or iPadOS 13.1 and later.

MDM controls activations provide full support for managing iOS devices, including the following features:

- Enforce password requirements
- Control device capabilities using IT policies (for example, disable the camera or Bluetooth)
- Enforce compliance rules
- Wi-Fi and VPN connection profiles (with proxy)
- Synchronize email, contacts, and calendar with devices
- Send CA and client certificates to devices for authentication and S/MIME
- Manage required and allowed public and internal apps, including BlackBerry Dynamics apps.
- Full support for Apple DEP and VPP
- Locate and protect lost or stolen devices

Note: Some features and BlackBerry Dynamics apps are not available with all license levels. For more information about available licenses, see the [Licensing content](#).

Steps to manage iOS devices

Step	Action
1	Install and configure BlackBerry UEM according to the on-premises Installation instructions or the UEM Cloud Configuration instructions . To manage iOS and iPadOS devices you must obtain an APNs certificate from Apple .
2	If your organization uses the Apple Device Enrollment Program, configure BlackBerry UEM to use DEP .
3	Configure IT policies for devices. Assign IT policies to user groups or individual users.
4	Configure profiles for devices. Assign profiles to to user groups or individual users.
5	If your organization has an Apple VPP account, add it to BlackBerry UEM .
6	Specify the apps that devices can or must install .
7	Activate devices .
8	Manage and monitor devices .

Controlling devices with an IT policy

BlackBerry UEM sends an IT policy to each device. You can use a default IT policy or create your own IT policies. You can create as many IT policies as you require for different situations and different users, but only one IT policy is active on a device at any time.

The IT policy rules for iOS and iPadOS are based on the capabilities of the device and the device configuration options provided by Apple. As Apple releases new OS updates with new features and configuration options, new IT policy rules are added to UEM at the next possible opportunity.

You can download the searchable and sortable [IT Policy rule spreadsheet](#). The spreadsheet documents all available rules in UEM, including the minimum device OS that supports the rule.

Device behavior you control with an IT policy includes the following options:

- Device [password requirements](#)
- Allowing device features such as the camera, Bluetooth, and Touch ID
- Allowing App Store and iTunes Store purchases, and allowable content ratings for purchases
- Allowing system apps, such as Safari, Siri, and FaceTime
- Allowing use of iCloud

For more information on sending IT policies to devices, [see the Administration content](#).

Setting iOS and password requirements

You can choose whether iOS and iPadOS devices must have a password. If you require a password, you can set the requirements for the password.

Note: iOS and iPadOS devices and some of the device password rules use the term "passcode." Both "password" and "passcode" have the same meaning.

Rule	Description
Password required for device	Specify whether the user must set a device password.
Allow simple value	Specify whether the password can contain repeated or sequential characters, such as DEFG or 3333.
Require alphanumeric value	Specify whether the password must contain both letters and numbers.
Minimum passcode length	Specify the minimum length of the password. If you enter a value that is less than the minimum required by the device, the device minimum is used.
Minimum number of complex characters	Specify the minimum number of non-alphanumeric characters that the password must contain.
Maximum passcode age	Specify the maximum number of days that the password can be used.

Rule	Description
Maximum auto-lock	Specify the maximum value that a user can set for the auto-lock time, which is the number of minutes of user inactivity that must elapse before a device locks. If set to "None," all supported values are available on the device. If the selected value is outside of the range supported by the device, the device will use the closest value it supports.
Passcode history	Specify the number of previous passwords that a device checks to prevent a user from reusing a recent password.
Maximum grace period for device lock	Specify the maximum value that a user can set for the grace period for device lock, which is the amount of time that a device can be locked before a password is required to unlock it. If set to "None," all values are available on the device. If set to "Immediately," the password is required immediately after the device locks.
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before the device is wiped.
Allow password changes (supervised only)	Specify if a user can add, change, or remove the password.

For more information about the IT policy password rules, [download the Policy Reference Spreadsheet](#).

Controlling devices with profiles

BlackBerry UEM includes several profiles that you can use to control various aspects of iOS and iPadOS device functionality. The most commonly used include the following profiles:

Profile name	Description	Configure
Activation	Specifies the device activation settings for users, such as the activation type, method, and the number and types of devices a user can activate.	Create an activation profile
Wi-Fi	Specifies settings for devices to connect to your work Wi-Fi network.	Create a Wi-Fi profile
VPN	Specifies settings for devices to connect to a work VPN.	Create a VPN profile
Proxy	Specifies how devices use a proxy server to access web services on the Internet or a work network	Create a proxy profile
Email	Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data. If you install and configure BlackBerry Work on devices, you don't need to set up an email profile.	Create an email profile
BlackBerry Dynamics	Allows devices to access BlackBerry Dynamics apps, such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect.	Create a BlackBerry Dynamics profile
BlackBerry Dynamics connectivity	Defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when they use BlackBerry Dynamics apps.	Create a BlackBerry Dynamics connectivity profile
Compliance	Defines the device conditions that are not acceptable in your organization and sets enforcement actions.	Create a compliance profile
Enterprise connectivity	Specifies whether devices can use BlackBerry Secure Connect Plus.	Enable BlackBerry Secure Connect Plus
CA certificate	Specifies a CA certificate that devices can use to establish trust with a work network or server.	Create a CA certificate profile
User credential	Specifies how devices obtain client certificates that are used to authenticate with a work network or server.	Create a user credential profile

Profile name	Description	Configure
SCEP	Specifies the SCEP server that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a SCEP profile

For more information about sending profiles to devices, [see the Administration content](#).

Profiles reference - iOS devices

The following table lists all BlackBerry UEM profiles supported on iOS and iPadOS devices:

Profile name	Description	Configure
Policy		
Activation	Specifies the device activation settings for users, such as the activation type and the number and types of devices.	Create an activation profile
BlackBerry Dynamics	Allows devices to access BlackBerry Dynamics apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect.	Create a BlackBerry Dynamics profile
App lock mode	Specify a single app to run on devices. Supervised devices only.	Create an app lock mode profile
Enterprise Management Agent	Specifies when devices connect to BlackBerry UEM for app or configuration updates when a push notification is not available.	Create an Enterprise Management Agent profile
Compliance		
Compliance	Defines the device conditions that are not acceptable in your organization and sets enforcement actions.	Create a compliance profile
Compliance (BlackBerry Dynamics)	This is a read-only profile that displays the compliance settings that were imported from Good Control into an on-premises BlackBerry UEM.	Managing BlackBerry Dynamics compliance profiles
Email, calendar, and contacts		
Email	Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.	Create an email profile

Profile name	Description	Configure
IMAP/POP3 email	Specifies how devices connect to an IMAP or POP3 mail server, and how to synchronize email messages.	Create an IMAP/POP3 email profile
Gatekeeping	Specifies the Microsoft Exchange servers to use for automatic gatekeeping.	Create a gatekeeping profile
CalDAV	Specifies the server settings that devices can use to synchronize calendar information.	Create a CalDAV profile
CardDAV	Specifies the server settings that devices can use to synchronize contact information.	Create a CardDAV profile
Networks and connections		
Wi-Fi	Specifies how devices connect to a work Wi-Fi network.	Create a Wi-Fi profile
VPN	Specifies how devices connect to a work VPN.	Create a VPN profile
Proxy	Specifies how devices use a proxy server to access web services on the Internet or a work network.	Create a proxy profile
Enterprise connectivity	Specifies whether devices can use BlackBerry Secure Connect Plus.	Enable BlackBerry Secure Connect Plus
BlackBerry Dynamics connectivity	Defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps.	Create a BlackBerry Dynamics connectivity profile
BlackBerry 2FA	Enables two-factor authentication for users and specifies the configuration of the preauthentication and self-rescue features.	Create a BlackBerry 2FA profile
Network usage	Allows you to control whether work apps can use the mobile network or data roaming.	Create a network usage profile
Web content filter	Limits the websites that a user can view on supervised devices. Supervised devices only.	Create a web content filter profile
Single sign-on extension	Allows devices to authenticate using single sign-on.	Create a single sign-on extension profile
Managed domains	Configures devices to notify users about sending email outside of trusted domains and restricts the apps that can view documents downloaded from internal domains.	Create a managed domains profile

Profile name	Description	Configure
AirPrint	Allows you to add printers to users' AirPrint printer lists.	Create an AirPrint profile
AirPlay	Allows you to add devices to users' AirPlay device lists.	Create an AirPlay profile
Protection		
Microsoft Intune app protection	Allows you to manage apps protected by Microsoft Intune.	Create a Microsoft Intune app protection profile
Location service	Allows you to request the location of devices and view the approximate locations on a map.	Create a location service profile
Do not disturb	Allows you to block BlackBerry Work for iOS notifications during off-work days and hours that you define.	Create a Do not disturb profile
Custom		
Device	Allows you to configure the information that displays on devices.	Create a device profile
Custom payload	Specifies custom configuration information using payload code for devices.	Create a custom payload profile
Per-app notification	Allows you to configure the notification settings for system apps and apps that you manage using BlackBerry UEM. Supervised devices only.	Create a per-app notification profile
Certificates		
CA certificate	Specifies a CA certificate that devices can use to establish trust with a work network or server.	Create a CA certificate profile
Shared certificate	Specifies a client certificate that devices can use to authenticate users with a work network or server.	Create a shared certificate profile
User credential	Specifies the CA connection that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a user credential profile
SCEP	Specifies the SCEP server that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a SCEP profile

Managing apps on devices

You can create a library of apps that you want to manage and monitor on devices. BlackBerry UEM provides the following options for managing apps on iOS and iPadOS devices:

- [Assign public apps](#) from the App Store as optional or required on devices.
- [Upload custom apps](#) to UEM and deploy them as optional or required apps.
- [Preconfigure app settings](#), such as connection settings, when allowed by the app.
- [Block users from accessing specific apps or configure a list of allowed apps and block all other apps.](#)
- [Link Apple VPP accounts](#) to UEM so that you can distribute purchased licenses for apps associated with the VPP accounts.
- [Configure public, ISV, and custom BlackBerry Dynamics apps](#) to allow users to access work resources.
- [Connect UEM to Microsoft Intune](#), so that you can set Intune app protection policies from within the UEM management console to deploy and manage Office 365 apps.
- [View the list of personal apps installed on devices.](#)
- [Allow users to rate and review apps](#) for other users in your environment.
- [Configure notification settings](#) for system apps and apps that you manage using UEM.
- [Specify the icon and label for the Work Apps icon](#) on devices.

App behavior on iOS devices with MDM controls activations

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have if you have assigned the "Feature - BlackBerryApp Store" entitlement to the user. For more information, see [Add the work app catalog to the BlackBerry Dynamics Launcher](#).

For iOS and iPadOS devices activated with MDM controls, the following behavior occurs:

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with a required disposition	<p>On supervised devices, apps are installed automatically. If the app is already installed, the app becomes managed by UEM.</p> <p>On non-supervised devices, user is prompted to install apps. If apps are already installed, user is prompted to allow UEM to manage the apps.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p> <p>You can use a compliance profile to define the actions that occur if required apps are not installed.</p>	<p>iTunes notifies users of available updates.</p> <p>Apps are removed from the "New/Updated" list when the user updates the app. (can take up to one hour)</p> <p>For devices that don't have access to iTunes, users aren't notified but can download the update from the app catalog if the device is assigned an Apple VPP license.</p>	<p>Apps are automatically removed without notification.</p> <p>Apps no longer appear in the app catalog.</p>	Apps are removed automatically.

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with an optional disposition	<p>If apps are already installed on supervised devices, the app becomes managed by UEM. On non-supervised devices, user is prompted to allow UEM to manage the apps.</p> <p>User is notified of a change to the app catalog.</p> <p>Apps are removed from the "New/Updated" list only when the user views the details (whether or not the app is installed).</p> <p>Users can choose whether to install the apps.</p>	<p>iTunes notifies users of available updates.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (whether or not the app is updated).</p>	<p>Apps are automatically removed without notification.</p> <p>Apps no longer appear in the app catalog.</p>	Apps are removed automatically.

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Internal apps with a required disposition	<p>On supervised devices, apps are installed automatically. If the app is already installed, the app becomes managed by UEM.</p> <p>On non-supervised devices, user is prompted to install apps. If apps are already installed, user is prompted to allow UEM to manage the apps. If the user cancels the installation, they can install apps from the app catalog.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p> <p>You can use a compliance profile to define the actions that occur if required apps are not installed.</p>	Apps are removed from the "New/Updated" list when the user updates the app.	<p>Apps are automatically removed without notification.</p> <p>Apps no longer appear in the app catalog.</p>	Apps are removed automatically.

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Internal apps with an optional disposition	<p>If apps are already installed on supervised devices, the app becomes managed by UEM. On non-supervised devices, user is prompted to allow UEM to manage the apps.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p>	Apps are removed from the "New/Updated" list when the user updates the app.	<p>Apps are automatically removed from devices activated with MDM controls without notification.</p> <p>Apps are not removed from devices activated with User privacy.</p> <p>Apps no longer appear in the app catalog.</p>	Apps are removed automatically.

App behavior on iOS devices with User privacy activations

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have if you have assigned the "Feature - BlackBerryApp Store" entitlement to the user. For more information, see [Add the work app catalog to the BlackBerry Dynamics Launcher](#).

When you activate iOS and iPadOS devices with User privacy, you can choose whether to allow app management. If you allow app management, app behavior for User privacy activations is the same as for [MDM controls activations](#). If you don't allow app management for devices activated with User privacy, the following behavior occurs:

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with a required disposition	<p>The user isn't prompted to install apps. User must go to the app catalog to install the required apps.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p>	<p>iTunes notifies users of available updates.</p> <p>Apps are removed from the "New/Updated" list when the user updates the app. (can take up to one hour)</p> <p>For devices that don't have access to iTunes, users aren't notified but can download the update from the app catalog.</p>	<p>Apps remain on the device.</p> <p>Apps no longer appear in the app catalog.</p>	Apps remain on the device.
Public apps with an optional disposition	<p>If app is already installed, nothing happens.</p> <p>User is notified of a change to the app catalog.</p> <p>Apps are removed from the "New/Updated" list only when the user views the details (whether or not the app is installed).</p> <p>Users can choose whether to install the apps.</p>	<p>iTunes notifies users of available updates.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (whether or not the app is updated).</p>	<p>Apps remain on the device.</p> <p>Apps no longer appear in the app catalog.</p>	Apps remain on the device.

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Internal apps with a required disposition	<p>If apps are already installed, user is prompted to allow UEM to manage the apps.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p>	Apps are removed from the "New/Updated" list when the user updates the app.	<p>Apps remain on the device.</p> <p>Apps no longer appear in the app catalog.</p>	Apps remain on the device.
Internal apps with an optional disposition	<p>If apps are already installed, nothing happens.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p>	Apps are removed from the "New/Updated" list when the user updates the app.	<p>Apps remain on the device.</p> <p>Apps no longer appear in the app catalog.</p>	Apps remain on the device.

Activating iOS devices

When you or a user activates an iOS or iPadOS device with BlackBerry UEM, the device is associated with BlackBerry UEM so that you can manage devices and users can access work data on their devices.

You can activate devices with BlackBerry UEM with or without using Apple Configurator 2 to prepare devices for activation. For more information about using Apple Configurator 2, see [Activating iOS devices using Apple Configurator 2](#) in the Administration content

You can also enroll devices in the Apple 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. For more information, see [Activating iOS devices that are enrolled in DEP](#) in the Administration content.

If devices are not enrolled in DEP, you can still prevent unsupervised devices from being activated using settings in the activation profile.

Activation types: iOS devices

Activation type	Description
MDM controls	<p>This activation type provides basic device management using device controls made available by iOS and iPadOS. A separate work space is not installed on the device and there is no added security for work data.</p> <p>You can control the device using commands and IT policies. During activation, users must install a mobile device management profile on the device.</p> <p>To specify whether BlackBerry UEM can limit activation by device ID, select Allow only approved device IDs.</p>

Activation type	Description
User privacy	<p>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.</p> <p>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).</p> <p>This activation type is not supported for Apple TV devices.</p> <p>When you allow User privacy activations, you select the profiles that you want manage on the device based on the needs of your organization. You can choose any of the following:</p> <ul style="list-style-type: none"> • 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.
User privacy - User enrollment	<p>You can use the User privacy - User enrollment activation type for iOS and iPadOS devices to make sure that user data is kept private and separated from work data. With this activation type, a separate work space is installed on the device for work apps and the native Notes, iCloud Drive, Mail (attachments and full email bodies), Calendar (attachments), and iCloud Keychain apps.</p> <p>This activation type enables app management, IT policy management, email profiles, Wi-Fi profiles, and per-app VPN. Administrators can manage work data (for example, wipe work data) without affecting personal data.</p> <p>This activation type is supported on unsupervised iPhone and iPad devices that run iOS and iPadOS 13.1 and later.</p>

Activation type	Description
Device registration for BlackBerry 2FA only	<p>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.</p> <p>When a device is activated, you can view limited device information in the management console, and you can deactivate the device using a command.</p> <p>This activation type is supported only for Microsoft Active Directory users.</p> <p>This activation type is not supported for Apple TV devices.</p> <p>For more information, see the BlackBerry 2FA content.</p>

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.

Create an activation profile

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.
 - Select **Not specified** if some users activate personal devices and some users activate work devices.
 - Select **Work** if most users activate work devices.
 - Select **Personal** if most users activate their personal devices.
7. Optionally, select an organization notice in the **Assign organization notice** drop-down list. If you assign an organization notice, users activating iOS, iPadOS, macOS, or Windows 10 devices must accept the notice to complete the activation process.
8. In the **Device types that users can activate** section, select the device OS types that users can activate. 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:
 - a) Click the tab for the device type.

b) In the **Device model restrictions** drop-down list, select one of the following options:

- **No restrictions:** Users can activate any device model.
- **Allow selected device models:** Users can activate only the device models that you specify. Use this option to limit the allowed devices to only some models.
- **Do not allow selected device models:** Users can't activate the device models that you specify. Use this option to block activation of some device models or devices from specific manufacturers.

If you restrict the device models users can activate, click **Edit** to select the devices you want to allow or restrict and click **Save**.

c) In the **Minimum allowed version** drop-down list, select the minimum allowed OS version.

Many older OS versions are no longer supported by BlackBerry UEM. You only need to select a minimum version if you don't want to support the earliest version currently supported by BlackBerry UEM. For more information on supported versions, [see the Compatibility Matrix](#).

d) Select the supported activation types.

10. For iOS and iPadOS devices, perform the following actions:

- a) If you selected the "User privacy" activation type and you want to enable SIM-based licensing, select **Allow access to SIM card and device hardware information to enable SIM-based licensing**.
- b) If you selected the "User privacy" activation type and you want to manage specific features, select the appropriate check boxes. For more information on each option, see [Activation types: iOS devices](#).
- c) If you selected the "MDM controls" or "User privacy" (with SIM-based licensing) activation types and you only want to activate supervised devices, select **Do not allow unsupervised devices to activate**.
- d) In the **iOS app integrity check** section, optionally select one of the following attestation methods:
 - **Perform app integrity check on BlackBerry Dynamics app activation:** Use this method to send challenges to devices when they are activated to check the integrity of iOS work apps.
 - **Perform periodic app integrity checks:** Use this method to send challenges to devices to check the integrity of iOS work apps.

To perform iOS app integrity checking, you must enable BlackBerry Protect in your BlackBerry UEM domain. For more information, see the [BlackBerry Protect Mobile](#) content.

11. Click **Add**.

After you finish: If necessary, rank profiles.


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

These steps apply to iOS and iPadOS devices that are activated using MDM controls or User privacy with MDM options enabled.

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

Send the following activation instructions to the device user, or send them a link to the following workflow: [Activating your iOS device](#).

1. On the device, install the BlackBerry UEM Client. You can download the BlackBerry UEM Client from the App Store.
2. On the device, tap **UEM Client** and accept the License Agreement.
3. Do one of the following:

Task	Steps
Use a QR Code to activate the device	<ol style="list-style-type: none"> Tap . Tap Allow to allow the BlackBerry UEM Client to take pictures and record video. Scan the QR Code in the activation email message that you received.
Manually activate the device	<ol style="list-style-type: none"> Type your work email address and activation password. If necessary, type the server address. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service. Tap Next.

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

After you finish: To verify that the activation process completed successfully, 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 or iPadOS device with Apple User Enrollment

Apple User Enrollment is supported on devices running iPad and iPadOS 13.1 or later.

To start enrollment, users use the camera app on the device to scan a QR Code provided in the Apple User Enrollment activation email to manually download and install the MDM profile to the device. To activate their device, users log in to their managed Apple ID account that matches the email address of the BlackBerry UEM user account. You should assign the UEM Client using a VPP license to users if you want to allow them to easily activate other BlackBerry Dynamics apps, import certificates, use BlackBerry 2FA features, use BlackBerry Protect, and check their compliance status. The UEM Client setup starts when the user accepts the license agreement.

Send the following activation instructions to the device user.

Before you begin:

- Verify that you received an activation email that has the QR Code for Apple User Enrollment. If you didn't receive the email, contact an administrator.
- If your device is already activated with BlackBerry UEM, you must deactivate your device.
- Uninstall the BlackBerry UEM Client.
- You must have a managed Apple ID account that is managed through your organization.

- Your device must not be a supervised device. If your device is supervised, it is noted in the Settings app near your Apple ID.
1. Open the activation email that contains the QR Code for Apple User Enrollment. If the QR Code already expired, you can request a new activation code from BlackBerry UEM Self-Service or contact your administrator.
 2. Open the Camera app on your device and scan the QR code in the activation email. When you are prompted, tap the notification to open the URL in Safari.
 3. When you are prompted to download the UEM configuration profile, tap **Allow**.
 4. After the download is complete, tap **Close**.
 5. Go to **Settings > General > Profile**.
 6. Tap **UEM profile**.
 7. On the User Enrollment screen, tap **Enroll my iPhone** or **Enroll my iPad**.
 8. Type your passcode.
 9. Log in to Apple ID using your managed Apple ID credentials.
 10. If your administrator assigned the BlackBerry UEM Client app to you, tap **Install** when prompted or open Work Apps.
 11. To set up the BlackBerry UEM Client app, open it and accept the license agreement. Follow the instructions on the screen to complete the activation process.

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

- On the device, open the 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.

Managing and monitoring activated devices

After iOS and iPadOS devices are activated and managed by an IT policy and profiles, you have several features available to control users' devices.

You have the following options:

Option	Description
Check for available software updates and update the device	<p>You can view available OS updates for all managed devices. You can force supervised devices to install an available update.</p> <p>For more information, see the Administration content.</p>
Turn on location settings and enable Lost Mode	<p>You can turn on location settings to track the location of devices. You can also enable Lost Mode to find a lost device.</p> <p>For more information, see the Administration content.</p>
Enable Activation Lock	<p>The Activation Lock feature on devices requires users to confirm the Apple ID and password to disable Find My iPhone, delete data from the device, or reactivate and use the device.</p> <p>To manage the Activation Lock feature in BlackBerry UEM:</p> <ul style="list-style-type: none">• The device must be supervised.• The device must have an iCloud account configured.• The device must have Find My iPhone or Find My iPad enabled. <p>BlackBerry UEM stores a bypass code that you can use to clear the lock so that data on the device can be deleted and it can be reactivated without the user's Apple ID and password.</p> <p>For more information, see the Administration content.</p>
Retrieve device logs	<p>You can retrieve logs from devices for monitoring and troubleshooting purposes.</p> <p>For more information, see the Administration content.</p>
Deactivate a device	<p>When you or a user deactivates a device, the connection between the device and the user account in BlackBerry UEM is removed. You can't manage the device and the device is no longer displayed in the management console. The user can't access work data on the device.</p> <p>You can deactivate a device using the "Delete all device data" or "Delete only work data" command.</p> <p>Users can deactivate a device by selecting Deactivate My Device on the About screen in the BlackBerry UEM Client app.</p>

Send a command to a device

Before you begin:

If you want to set an expiry period for commands that delete data from devices in BlackBerry UEM, see [Set an expiry time for commands](#).

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Click the device tab.
5. In the **Manage device** window, select the command that you want to send to the device.

Commands for iOS devices

These commands also apply to iPadOS devices.

Command	Description	Activation types
View device report	This command displays detailed information about a device. You can export and save the device report on your computer. For more information, see View and save a device report .	MDM controls User privacy
View device actions	This command displays any actions that are in progress on a device. For more information, see Viewing device actions .	MDM controls User privacy
Delete all device data	<p>This command deletes all user information and app data that the device stores and returns the device to factory default settings.</p> <p>If the device is unable to connect to BlackBerry UEM when you send this command, you can either cancel the command or remove the device from the console. If the device connects to BlackBerry UEM after you remove it, only the work data is deleted from the device.</p> <p>To send this command to multiple devices, see Send a bulk command.</p>	MDM controls
Delete only work data	<p>This command deletes work data, including the IT policy, profiles, apps, and certificates that are on the device.</p> <p>If the device is unable to connect to BlackBerry UEM when you send this command, you can either cancel the command or remove the device from the console. If the device connects to BlackBerry UEM after you remove it, the work data is deleted from the device.</p> <p>To send this command to multiple devices, see Send a bulk command.</p>	MDM controls User privacy

Command	Description	Activation types
Lock device	<p>This command locks a device. The user must type the existing device password to unlock the device. If a device is temporarily lost, you might use this command.</p> <p>When you send this command, the device locks only if there is an existing device password. Otherwise, no action is taken on the device.</p> <p>This command is not supported for Apple TV devices.</p>	MDM controls
Unlock and clear password	<p>This command unlocks a device and deletes the existing password. The user is prompted to create a device password. You can use this command if the user forgets the device password.</p> <p>This command is not supported for Apple TV devices.</p>	MDM controls
Turn on Lost Mode	<p>This command locks the device and lets you set a phone number and message to display on the device. For example, you can display contact information for when the device is found.</p> <p>After you send this command, you can view the location of the device from BlackBerry UEM.</p> <p>This command is supported only for supervised devices.</p> <p>This command is not supported for Apple TV devices.</p>	MDM controls
Deactivate BlackBerry 2FA	<p>This command deactivates devices that are activated with the "BlackBerry 2FA" activation type. The device is removed from BlackBerry UEM and the user can't use the BlackBerry 2FA feature.</p> <p>This command is not supported for Apple TV devices.</p>	MDM controls
Update OS	<p>This command forces devices to install an available OS update.</p> <p>For more information, see Update the OS on supervised iOS devices.</p> <p>To send this command to multiple devices, see Send a bulk command.</p> <p>This command is supported only for supervised devices.</p> <p>This command is not supported for Apple TV devices.</p>	MDM controls
Restart device	<p>This command forces devices to restart.</p> <p>This command is supported only for supervised devices.</p> <p>This command is not supported for Apple TV devices.</p>	MDM controls

Command	Description	Activation types
Turn off device	<p>This command forces devices to turn off.</p> <p>This command is supported only for supervised devices.</p> <p>This command is not supported for Apple TV devices.</p>	MDM controls
Wipe apps	<p>This command wipes data from all Microsoft Intune-managed apps on the device. The apps are not removed from the device.</p> <p>For more information, see Wipe apps managed by Microsoft Intune.</p>	MDM controls
Update device information	<p>This command sends and receives updated device information. For example, you can send newly updated IT policy rules or profiles to a device, and receive updated information about a device such as OS version or battery level.</p> <p>To send this command to multiple devices, see Send a bulk command.</p>	MDM controls User privacy
Update time zone	This command sets the device time according to the region that you select.	MDM controls
Remove device	<p>This command removes the device from BlackBerry UEM but does not remove data from the device. The device may continue to receive email and other work data.</p> <p>This command is intended for devices that have been irretrievably lost or damaged and are not expected to contact the server again. If a device that has been removed attempts to contact BlackBerry UEM, the user receives a notification and the device won't be able to communicate with BlackBerry UEM unless it is reactivated.</p> <p>To send this command to multiple devices, see Send a bulk command.</p>	MDM controls User privacy
Refresh eSIM cellular plans	For devices that have an eSIM-based cellular plan, this command queries updated plan details for the device from the device carrier URL.	MDM controls

Legal notice

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

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

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

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

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

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

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

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

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

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

Published in Canada