BlackBerry UEM

Managing iOS devices

Administration

12.11

Contents

Managing iOS devices

BlackBerry UEM provides precise management of how iOS 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.

This guide describes the options you have to manage iOS 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 iOSdevices. The following BlackBerry UEM features are supported for Apple TV:

- Device activation using BlackBerry UEM Self-Service
- MDM controls activation type
- Wi-Fiand 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 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)	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. 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.
Managed devices (devices that are managed by BlackBerry UEM)	You can activate a device to be fully manged by BlackBerry UEM. This option is often used for corporate-owned devices. 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. BlackBerry UEM supports managing supervised iOS devices. Some IT policy rules are supported only on supervised devices

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.

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

Licenses consumed by iOS devices

When you or a user activates an iOS device with BlackBerry UEM, you associate the device with BlackBerry UEM so that you can manage devices and users can access work data on their devices. Most iOS activation types require a minimum of a Silver BlackBerry UEM license or a BlackBerry Enterprise Mobility Suite - Management Edition license, but other licenses may be required depending on the features that you want to enable for users.

Feature	Minimum Required license
MDM controls or User privacy activation	One of the following: • Silver • BlackBerry Enterprise Mobility Suite - Management Edition
BlackBerry Secure Gateway	One of the following: • Gold • BlackBerry Enterprise Mobility Suite - Enterprise Edition For more information about the BlackBerry Secure Gateway, see the BlackBerry UEM Administration content or the BlackBerry UEM Cloud Administration content.
BlackBerry Secure Connect Plus	One of the following: • Gold • BlackBerry Enterprise Mobility Suite - Collaboration Edition For more information about BlackBerry Secure Connect Plus, see the BlackBerry UEM Administration content or the BlackBerry UEM Cloud Administration content.
BlackBerry Access app	BlackBerry Enterprise Mobility Suite - Management Edition
BlackBerry Work and BlackBerry Tasks apps	BlackBerry Enterprise Mobility Suite - Enterprise Edition
All other BlackBerry and ISV BlackBerry Dynamics apps	BlackBerry Enterprise Mobility Suite - Collaboration Edition
Device registration for BlackBerry 2FA only	One of the following: • BlackBerry 2FA • BlackBerry Enterprise Mobility Suite - Application Edition

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 Installation instructions. To manage iOS 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	Verify that you have the required licenses to activate iOS devices with the features that you want to enable.
4	Configure IT policies for devices. Assign IT policies to user groups or individual users.
5	Configure profiles for devices. Assign profiles to to user groups or individual users.
6	If your organization has an Apple VPP account, add it to BlackBerry UEM.
7	Specify the apps that devices can or must install.
8	Activate devices.
9	Manage and monitor devices.

Controlling iOS 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 are based on the 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 password requirements

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

Note: iOS 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 iOS 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 rules password rules, download the Policy Reference Spreadsheet.

Controlling iOS devices with profiles

BlackBerry UEM includes several profiles that you can use to control various aspects of 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

Profile name	Description	Configure
User credential	Specifies how devices obtain client certificates that are 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 certficate 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 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 iOS 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. BlackBerry UEM includes a Default compliance profile.	Create a compliance profile
Compliance (BlackBerry Dynamics)	This is a read-only profile that displays the compliance settings that were imported from Good Control.	Managing BlackBerry Dynamics compliance profiles
Email, calendar, and contacts		

Profile name	Description	Configure
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
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 how devices can connect to your organization's resources using enterprise connectivity. For iOS devices, the enterprise connectivity profile specifies whether devices can use BlackBerry Secure Connect Plus.	Create an enterprise connectivity profile
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 on iOS devices can use the mobile network or data roaming.	Create a network usage profile

Profile name	Description	Configure
Web content filter	Limits the websites that a user can view on supervised iOS devices. Supervised iOS devices only.	Create a web content filter profile
Single sign-on	Specifies how devices authenticate with secure domains automatically after users type their username and password for the first time.	Create a single sign-on profile
Managed domains	Configures iOS 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
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 iOS 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

Profile name	Description	Configure
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 certficate that is used to authenticate with a work network or server.	Create a SCEP profile

Managing apps on iOS 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 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

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have added it to the BlackBerry Dynamics Launcher.

For iOS devices activated with MDM controls and 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	If apps are already installed, user is prompted to allow UEM to manage the apps. On supervised devices, apps are installed automatically. On non-supervised devices activated with MDM controls, user is prompted to install apps. On devices activated with User privacy, user is not prompted to install apps. User must go to the app catalog to install the required apps. 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. You can use a compliance profile to define the actions that occur if required apps are not installed.	iTunes notifies users of available updates. Apps are removed from the "New/Updated" list when the user updates the app. (can take up to one hour) For devices that do not have access to iTunes, users are not notified but can download the update from the app catalog.	Apps are automatically removed from devices activated with MDM controls without notification. Apps are not removed from devices activated with User privacy. Apps no longer appear in the app catalog.	For devices activated with MDM controls, apps are removed automatically. For devices activated with User privacy, users are prompted to remove the apps.

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	If app is already installed, nothing happens. User is notified of a change to the app catalog. Apps are removed from the "New/Updated" list only when the user views the details (whether or not the app is installed). Users can choose whether to install the apps.	iTunes notifies users of available updates. Apps are removed from the "New/Updated" list when the user views the details (whether or not the app is updated).	Apps are automatically removed from devices activated with MDM controls without notification. Apps are not removed from devices activated with User privacy. Apps no longer appear in the app catalog.	For devices activated with MDM controls, apps are removed automatically. For devices activated with User privacy, users are prompted to remove the apps.

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	If apps are already installed, user is prompted to allow UEM to manage the apps. On supervised devices, apps are installed automatically. On non-supervised devices, users are prompted to install apps. If the user cancels the installation, they can install apps from the app catalog. 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. You can use a compliance profile to define the actions that occur if required apps are not installed.	Apps are removed from the "New/ Updated" list when the user updates the app.	Apps are automatically removed from devices activated with MDM controls without notification. Apps are not removed from devices activated with User privacy. Apps no longer appear in the app catalog.	For devices activated with MDM controls, apps are removed automatically. For devices activated with User privacy, users are prompted to remove the apps.

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	If apps are already installed, nothing happens. 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.	Apps are removed from the "New/Updated" list when the user updates the app.	Apps are automatically removed from devices activated with MDM controls without notification. Apps are not removed from devices activated with User privacy. Apps no longer appear in the app catalog.	For devices activated with MDM controls, apps are removed automatically. For devices activated with User privacy, users are prompted to remove the apps.

Activating iOS devices

When you or a user activates an iOS device with BlackBerry UEM, you associate the device 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 iOS 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	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.

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 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 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.

Managing and monitoring activated iOS devices

After 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	You can view available OS updates for all managed devices. You can force the following devices to install an available update: • Supervised devices running iOS 10.3 and later • Supervised DEP devices For more information, see the Administration content.
Turn on location settings and enable Lost Mode	You can turn on location settings to track the location of iOS devices. You can also enable Lost Mode to find a lost device. For more information, see the Administration content.
Enable Activation Lock	The Activation Lock feature on iOS 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. To manage the Activation Lock feature in BlackBerry UEM: • 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. 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. For more information, see the Administration content.
Retrieve device logs	You can retrieve logs from devices for monitoring and troubleshooting purposes. For more information, see the Administration content.
Deactivate a device	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. You can deactivate a device using the "Delete all device data" or "Delete only work data" command. Users can deactivate an iOS device by selecting Deactivate My Device on the About screen in the BlackBerry UEM Client app.

Commands for iOS devices

Command	Description	Activation types
Delete all device data	This command deletes all user information and app data that the device stores and returns the device to factory default settings. 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. To send this command to multiple devices, see Send a bulk command.	MDM controls
Delete only work data	This command deletes work data, including the IT policy, profiles, apps, and certificates that are on the device. 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. To send this command to multiple devices, see Send a bulk command.	MDM controls User privacy
Lock device	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. When you send this command, the device locks only if there is an existing device password. Otherwise, no action is taken on the device. This command is not supported for Apple TV devices.	MDM controls
Unlock and clear password	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. This command is not supported for Apple TV devices.	MDM controls

Command	Description	Activation types
Turn on Lost Mode	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. After you send this command, you can view the location of the device from BlackBerry UEM. This command is supported for supervised iOS devices. This command is not supported for Apple TV devices.	MDM controls
Deactivate BlackBe 2FA	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. This command is not supported for Apple TV devices.	MDM controls
Update OS	This command forces devices to install an available OS update. Supported on the following devices: • supervised devices running iOS 10.3 and later • supervised DEP devices For more information, see Update the OS on supervised iOSdevices. To send this command to multiple devices, see Send a bulk command. This command is not supported for Apple TV devices.	MDM controls
Restart device	This command forces devices to restart. Supported on supervised iOS devices that are running 10.3 and later. This command is not supported for Apple TV devices.	MDM controls
Turn off device	This command forces devices to turn off. Supported on supervised iOS devices that are running 10.3 and later. This command is not supported for Apple TV devices.	MDM controls
Wipe apps	This command wipes data from all Microsoft Intune-managed apps on the device. The apps are not removed from the device. For more information, see Wipe apps managed by Microsoft Intune	MDM controls

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
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada