BlackBerry UEM

Managing device features

Administration

12.17

Contents

Managing device features and behavior

You have several options for controlling device behavior. You can use profiles and IT policies to turn on or limit the use of many features. You can also send commands to devices to initiate various actions.

You can specify settings for different device types in the same IT policy or profile and then assign the IT policy or profile to user accounts, user groups, or device groups.

Managing devices with IT policies

You can use IT policies to manage the security and behavior of devices in your organization. An IT policy is a set of rules that control features and functionality on devices. You can configure rules for all device types in the same IT policy. The device OS determines the list of features that can be controlled using IT policies and the device activation type determines which rules in an IT policy apply to a specific device. Devices ignore rules in an IT policy that to not apply to them.

BlackBerry UEM includes a Default IT policy with preconfigured rules for each device type. If no IT policy is assigned to a user account, a user group that a user belongs to, or a device group that a user's devices belong to, BlackBerry UEM sends the Default IT policy to a user's devices. BlackBerry UEM automatically sends an IT policy to a device when a user activates it, when you update an assigned IT policy, or when a different IT policy is assigned to a user account or device.

BlackBerry UEM on-premises synchronizes daily with the BlackBerry Infrastructure over port 3101 to determine whether any updated IT policy information is available. In If updated IT policy information is available, BlackBerry UEM retrieves it and, by default, stores the updates in the BlackBerry UEM database. Administrators with the "View IT policies" and "Create and edit IT policies" permissions are notified about the update when they log in. If your organization's security policy does not allow automatic updates, you can turn off the automatic updates and import updates into BlackBerry UEM manually. for more information, see Importing IT policy and device metadata updates.

Updated IT policy information is applied automatically in UEM Cloud instances.

For more information about the IT policy rules for each device type, download the Policy Reference Spreadsheet.

Restricting or allowing device capabilities

When you configure IT policy rules, you can restrict or allow device capabilities. The IT policy rules available for each device type are determined by the device OS and version and by the device activation type. For example, depending on the device and activation type, you can use IT policy rules to:

- Enforce password requirements for the device or the work space on a device
- Prevent users from using device features, such as the camera
- Control connections that use Bluetooth wireless technology
- Control the availability of certain apps
- Require encryption and other security features

Depending on the device activation type, you can use IT policy rules to control the entire device, only the work space on a device, or both.

For Android 8.0 and later devices, you can create a device support message that displays on the device for some features when they are disabled by IT policy rules.

For more information about the IT policy rules for each device type, download the Policy Reference Spreadsheet.

Setting device password requirements

You use IT policy rules to set the password requirements for devices. You can set requirements for password length and complexity, password expiration, and the result of incorrect password attempts. The following topics explain the password rules that apply to the various device and activation types.

For more information about the IT policy rules, download the Policy Reference Spreadsheet.

Setting iOS 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.
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.

Setting macOS password requirements

You can choose whether password rules for macOS devices apply to the device or the user and whether a password is required. If you require a password, you can set the requirements for the password.

Rule	Description
IT policy rules target	This rule specifies whether the IT policy rules for the password apply only to the assigned user's account or to the entire device.
Password required for device	Specify whether the user must set a device password.
Allow simple password	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 password length	Specify the minimum length of the password.
Minimum number of complex characters	Specify the minimum number of non-alphanumeric characters that the password must contain.
Maximum password age	Specify the maximum number of days that the password can be used before it expires and the user must set a new password.
Maximum auto-lock	Specify the maximum number of minutes of user inactivity that must elapse before a device locks. If set to "None," the user can select any value.
Password history	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a 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.
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before a device is wiped.

For more information about the IT policy password rules, download the Policy Reference Spreadsheet.

Setting Android password requirements

There are four groups of IT policy rules for Android passwords. The group of rules that you use depends on the device activation type and whether you are setting requirements for the device password or the work space password.

After you set password rules in the IT policy, use a compliance profile to enforce the password requirements.

Activation type	Supported password rules
Work and personal - user privacy (Android Enterprise) and Work and personal - full control (Android Enterprise)	Use the global password rules to set device password requirements. Use the work profile password rules to set the password requirements for the work profile. Knox password rules are ignored by the device.

Activation type	Supported password rules
Work space only (Android Enterprise)	Use the global password rules to set password requirements for the device. Because the device only has a work space, the password is also the work space password. All other password rules are ignored by the device.
MDM controls	Use the global password rules to set device password requirements. All other password rules are ignored by the device. **Note:** The MDM controls activation type is deprecated for devices with Android 10. For more information, visit https://support.blackberry.com/community to read article 48386.
MDM controls (Samsung Knox)	Use the Knox MDM password rules to set device password requirements. All other password rules are ignored by the device.
Work and personal - user privacy (Samsung Knox)	You have no control over the device password. Use the Knox Premium - Workspace password rules to set password requirements for the work space. All other password rules are ignored by the device. **Note:** The Samsung Knox activation types will be deprecated in a future release. Devices that support Knox Platform for Enterprise can be activated using the Android Enterprise activation types. For more information, visit https://support.blackberry.com/community to read article 54614.
Work and personal - full control (Samsung Knox)	Use the Knox MDM password rules to set device password requirements. Use the Knox Premium - Workspace password rules to set password requirements for the work space. All other password rules are ignored by the device.
Work space only (Samsung Knox)	Use the Knox Premium - Workspace password rules to set password requirements for the work space. All other password rules are ignored by the device.

Android: Global password rules

The global password rules set the device password requirements for devices with the following activation types:

- Work and personal - user privacy (Android Enterprise)
- Work and personal - full control (Android Enterprise)
- Work space only (Android Enterprise)
- MDM controls (without Samsung Knox)

Note: The MDM controls activation type is deprecated for devices with Android 10. For more information, visit https://support.blackberry.com/community to read article 48386.

Rule	Description
Password complexity (Global (all Android devices))	Specify the minimum complexity level for the device password. You can choose one of the following options: • Low - allows patterns and PINs with repeating or sequential values. • Medium - requires PINs with no repeating or sequential values and a minimum length of four or a password with a minimum length of four. • High - requires PINs with no repeating or sequential values and minimum length of eight or a password with a minimum length of six. **Note:** If you set the password complexity to High, and you then set the password complexity to Medium in the Work profile (all Android devices) section of the IT policy, the global setting takes precedence over the Work profile setting and users will be forced to set a password with high complexity.
Password requirements	Specify the minimum requirements for the password. You can choose one of the following options: • Unspecified - no password required • Something - the user must set a password but there are no requirements for length or quality • Numeric - the password must include at least one number • Alphabetic - the password must include at least one letter • Alphanumeric - the password must include at least one letter and one number • Complex - allows you to set specific requirements for different character types
Password complexity (Work profile (all Android devices))	Specify the minimum complexity level for the device password. You can choose one of the following options: • Low - allows patterns and PINs with repeating or sequential values. • Medium - requires PINs with no repeating or sequential values and a minimum length of four or a password with a minimum length of four. • High - requires PINs with no repeating or sequential values and minimum length of eight or a password with a minimum length of six. **Note:** If you the password complexity to Medium or low, and you have already set the password complexity to High in the Global (all Android devices) section of the IT policy, the global setting takes precedence over the Work profile setting and users will be forced to set a password with high complexity.
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before a device is wiped or deactivated. Devices with the "MDM controls" activation type are wiped. Devices with the "Work and personal - user privacy " and the "Work and personal - user privacy (Premium)" activation types are deactivated and the work profile removed.
Maximum inactivity time lock	Specify the maximum number of minutes of user inactivity that must elapse before the device or work space locks. On Android devices with a work profile, the work space also locks. Users can set a shorter time period on the device. This rule is ignored if no password is required.

Rule	Description
Password expiration timeout	Specify the maximum amount of time that the password can be used. After the specified amount of time elapses, the user must set a new password. If set to 0, the password does not expire.
Password history restriction	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a recent numeric, alphabetic, alphanumeric, or complex password. If set to 0, the device does not check previous passwords.
Minimum password length	Specify the minimum number of characters for a numeric, alphabetic, alphanumeric, or complex password.
Minimum uppercase letters required in password	Specify the minimum number of uppercase letters that a complex password must contain.
Minimum lowercase letters required in password	Specify the minimum number of lowercase letters that a complex password must contain.
Minimum letters required in password	Specify the minimum number of letters that a complex password must contain.
Minimum non-letters in password	Specify the minimum number of non-letter characters (numbers or symbols) that a complex password must contain.
Minimum numerical digits required in password	Specify the minimum number of numerals that a complex password must contain.
Minimum symbols required in password	Specify the minimum number of non-alphanumeric characters that a complex password must contain.

For more information about the IT policy password rules, download the Policy Reference Spreadsheet.

Android: Work profile password rules

The work profile password rules set the work space password requirements for devices with the following activation types:

- Work and personal - user privacy (Android Enterprise)
- Work and personal - full control (Android Enterprise)

Rule	Description
Password requirements	Specify the minimum requirements for the work space password. You can choose one of the following options: • Something - the user must set a password but there are no requirements for length or quality • Numeric - the password must include at least one number • Alphabetic - the password must include at least one letter • Alphanumeric - the password must include at least one letter and one number • Complex - allows you to set specific requirements for different character types • Numeric Complex - the password must contain numeric characters with no repeating sequence (4444) or ordered sequence (1234, 4321, 2468). • Biometric Weak - the password allows for low-security biometric recognition technology For BlackBerry devices powered by Android, you can force the work space and device passwords to be different using the BlackBerry devices "Force the device and work space passwords to be different" rule.
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect work space password before the device is deactivated and the work profile is removed.
Maximum inactivity time lock	Specify the maximum number of minutes of user inactivity that must elapse before the device and work space lock. If you set both this rule and the Android global "Maximum inactivity time lock" rule, the device and work space lock when either timer expires. Users can set a shorter time period on the device.
Password expiration timeout	Specify the maximum amount of time that the work space password can be used. After the specified amount of time elapses, the user must set a new work space password. If set to 0, the password does not expire.
Password history restriction	Specify the maximum number of previous work space passwords that a device checks to prevent a user from reusing a recent numeric, alphabetic, alphanumeric, or complex password. If set to 0, the device does not check previous passwords.
Minimum password length	Specify the minimum number of characters for a numeric, alphabetic, alphanumeric, or complex work space password.
Minimum uppercase letters required in password	Specify the minimum number of uppercase letters that a complex work space password must contain.
Minimum lowercase letters required in password	Specify the minimum number of lowercase letters that a complex work space password must contain.
Minimum letters required in password	Specify the minimum number of letters that a complex work space password must contain.
Minimum non-letters in password	Specify the minimum number of non-letter characters (numbers or symbols) that a complex work space password must contain.

Rule	Description
Minimum numerical digits required in password	Specify the minimum number of numerals that a complex work space password must contain.
Minimum symbols required in password	Specify the minimum number of non-alphanumeric characters that a complex work space password must contain.
Force the device and work profile passwords to be different	Specify whether users must set different passwords for the device and the work profile. When the passwords are the same, unlocking the device unlocks the work profile.

For more information about the IT policy password rules, download the Policy Reference Spreadsheet.

Android: Knox MDM password rules

The Knox MDM password rules set the device password requirements for devices with the following activation types:

- Work and personal - full control (Samsung Knox)
- MDM controls (Knox MDM)

Devices with these activation types must have a device password.

If you are activating devices with Android Enterprise activation types to use Knox Platform for Enterprise, use the Android Global password rules. The Samsung Knox activation types and Knox MDM IT policy rules will be deprecated in a future release. For more information, visit https://support.blackberry.com/community to read article 54614.

Note: The MDM controls activation type is deprecated for devices with Android 10. For more information, visit https://support.blackberry.com/community to read article 48386.

Rule	Description
Password requirements	Specify the minimum requirements for the password. You can choose one of the following options: • Numeric - the password must include at least one number • Alphabetic - the password must include at least one letter • Alphanumeric - the password must include at least one letter and one number • Complex - allows you to set specific requirements for different character types
Minimum password length	Specify the minimum length of the password. The password must be at least 4 characters.
Minimum lowercase letters required in password	Specify the minimum number of lowercase letters that a complex password must contain.
Minimum uppercase letters required in password	Specify the minimum number of uppercase letters that a complex password must contain.

Rule	Description
Minimum complex characters required in password	Specify the minimum number of complex characters (for example, numbers or symbols) that a complex password must contain. If you set this value to 1, then at least one number is required. If you set a value greater than 1, then at least one number and one symbol are required.
Maximum character sequence length	Specify the maximum length of an alphabetic sequence that is allowed in an alphabetic, alphanumeric, or complex password. For example, if the alphabetic sequence length is set to 5, the alphabetic sequence "abcde" is allowed but the sequence "abcdef" is not allowed. If set to 0, there are no alphabetic sequence restrictions.
Maximum inactivity time lock	Specify the maximum period of user inactivity before the device locks (key guard lock). If the device is managed by multiple EMM solutions, the device uses the lowest value as the inactivity period. If the device uses a password, the user must provide the password to unlock the device. If set to 0, the device doesn't have an inactivity timeout.
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before a device is wiped.
Password history restriction	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a recent password. If set to 0, the device does not check previous passwords.
Password expiration timeout	Specify the maximum amount of time that the device password can be used. After the specified amount of time elapses, the password expires and a user must set a new password. If set to 0, the password does not expire.
Allow password visibility	Specify whether the device password can be visible when the user is typing it. If this rule is not selected, users and third-party apps cannot change the visibility setting.
Allow fingerprint authentication	Specify whether the user can use fingerprint authentication for the device.

For more information about the IT policy password rules, download the Policy Reference Spreadsheet.

Android: Knox Premium - Workspace password rules

The Knox Premium - Workspace password rules set the work space password requirements for devices with the following activation types:

- Work and personal - user privacy (Samsung Knox)
- Work and personal - full control (Samsung Knox)
- Work space only (Samsung Knox)

Devices with these activation types must have a work space password.

If you are activating devices with Android Enterprise activation types to use Knox Platform for Enterprise, use the Android Work profile password rules. The Samsung Knox activation types and Knox Premium IT policy rules will be deprecated in a future release. For more information, visit https://support.blackberry.com/community to read article 54614.

Rule	Description
Password requirements	Specify the minimum requirements for the password. You can choose one of the following options: • Numeric - the password must include at least one number • Numeric Complex - the password must include at least one number, with no repeating (4444) or ordered (1234, 4321, 2468) sequences • Alphabetic - the password must include at least one letter • Alphanumeric - the password must include at least one letter and one number • Complex - allows you to set specific requirements for different character types
Minimum lowercase letters required in password	Specify the minimum number of lowercase letters that a complex password must contain.
Minimum uppercase letters required in password	Specify the minimum number of uppercase letters that a complex password must contain.
Minimum complex characters required in password	Specify the minimum number of complex characters (for example, numbers or symbols) that a complex password must contain. At least three complex characters are required, including at least one number and one symbol.
Maximum character sequence length	Specify the maximum length of an alphabetic sequence that is allowed in an alphabetic, alphanumeric, or complex password. For example, if the alphabetic sequence length is set to 5, the alphabetic sequence "abcde" is allowed but the sequence "abcdef" is not allowed. If set to 0, there are no alphabetic sequence restrictions.
Minimum password length	Specify the minimum length of the password. If you enter a value that is less than the minimum required by Knox Workspace, the Knox Workspace minimum is used.
Maximum inactivity time lock	Specify the maximum period of user inactivity in the work space before the work space locks. If set to 0, the work space doesn’t have an inactivity timeout.
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before the work space is wiped. If set to 0, there are no restrictions on the number of times a user can enter an incorrect password.
Password history restriction	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a recent password. If set to 0, the device does not check previous passwords.
Password expiration timeout	Specify the maximum number of days that the password can be used. After the specified number of days elapses, the password expires and a user must set a new password. If set to 0, the password does not expire.
Minimum number of changed characters for new passwords	Specify the minimum number of changed characters that a new password must include compared to the previous password. If set to 0, no restrictions are applied.

Rule	Description
Allow keyguard customizations	Specify whether a device can use keyguard customizations, such as trust agents. If this rule is not selected, keyguard customizations are turned off.
Allow keyguard trust agents	Specify whether a user can keep the work space unlocked for 2 hours after the maximum inactivity timeout value. If you do not set an inactivity timeout value, the user can perform this action by default.
Allow password visibility	Specify whether the device password can be visible when the user is typing it. If this rule is not selected, users and third-party apps cannot change the visibility setting.
Enforce two-factor authentication	Specify whether a user must use two-factor authentication to access the work space. For example, you can use this rule if you want the user to authenticate using a fingerprint and a password.
Allow fingerprint authentication	Specify whether the user can use fingerprint authentication to access the work space.

For more information about the IT policy password rules, download the Policy Reference Spreadsheet.

Setting Windows 10 password requirements

You can choose whether Windows 10 devices must have a password. If you require a password, you can set the requirements for the password.

Rule	Description
Password required for device	Specify whether the user must set a device password.
Allow simple password	Specify whether the password can contain repeated or sequential characters, such as DEFG or 3333.
Minimum password length	Specify the minimum length of the password. The password must be at least 4 characters.
Password complexity	Specify the complexity of the password. You can choose the following options: • Alphanumeric - the password must contain letters and numbers • Numeric - the password must contain only numbers
Minimum number of character types	Specify the minimum number of character types that an alphanumeric password must contain. Select from the following options: **1.** numbers required **2.** numbers and lowercase letters required **3.** numbers, lowercase letters, and uppercase letters required **4.** numbers, lowercase letters, uppercase letters, and special characters required Password character requirements for Windows 10 computers and tablets are determined by the user account type, not this setting.

Rule	Description
Password expiration	Specify the maximum number of days that the password can be used. If set to 0, the password does not expire.
Password history	Specify the number of previous passwords that a device checks to prevent a user from reusing a recent password. If set to 0, the device does not check previous passwords.
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before the device is wiped. If set to 0, the device is not wiped regardless of how many times the user enters an incorrect password. This rule does not apply to devices that allow multiple user accounts, including Windows 10 computers and tablets.
Maximum inactivity time lock	Specify the period of user inactivity that must elapse before the device locks. If set to 0, the device does not lock automatically.
Allow idle return without password	Specify whether a user must type the password when the idle grace period ends. If this rule is selected, the user can set the password grace period timer on the device. This rule does not apply to Windows 10 computers and tablets.

For more information about the IT policy password rules, download the Policy Reference Spreadsheet.

Creating and managing IT policies

You can use the Default IT policy or create custom IT policies (for example, to specify IT policy rules for different user groups or device groups in your organization). If you plan to use the Default IT policy, you should review it and, if necessary, update it to make sure that the rules meet your organization's security standards.

Create an IT policy

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click +.
4. Type a name and description for the IT policy.
5. Click the tab for each device type in your organization and configure the appropriate values for the IT policy rules.
   Hold the mouse over the name of a rule to display help tips.
6. Click **Add**.

After you finish: Rank IT policies

Copy an IT policy

You can copy existing IT policies to quickly create custom IT policies for different groups in your organization.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click the name of the IT policy that you want to copy.

4. Click  .
5. Type a name and description for the new IT policy.
6. Make changes on the appropriate tab for each device type.
7. Click **Add**.

After you finish: Rank IT policies

Rank IT policies

Ranking is used to determine which IT policy BlackBerry UEM sends to a device in the following scenarios:

- A user is a member of multiple user groups that have different IT policies.
- A device is a member of multiple device groups that have different IT policies.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click  .
4. Use the arrows to move IT policies up or down the ranking.
5. Click **Save**.

View an IT policy

You can view the following information about an IT policy:

- IT policy rules specific to each device type
- List and number of user accounts that the IT policy is assigned to (directly and indirectly)
- List and number of user groups that the IT policy is assigned to (directly)

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click the name of the IT policy that you want to view.

Change an IT policy

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click the name of the IT policy that you want to change.
4. Click  .
5. Make changes on the appropriate tab for each device type.
6. Click **Save**.

After you finish: If necessary, change the IT policy ranking.

Remove an IT policy from user accounts or user groups

If an IT policy is assigned directly to user accounts or user groups, you can remove it from users or groups. If an IT policy is assigned indirectly by user group, you can remove the IT policy from the group or remove user accounts from the group. When you remove an IT policy from user groups, the IT policy is removed from every user that belongs to the selected groups.

Note: The Default IT policy can only be removed from a user account if you assigned it directly to the user.

1. On the menu bar, click **Policies and Profiles**.

2. Click **Policy > IT policies**.
3. Click the name of the IT policy that you want to remove from user accounts or user groups.
4. Perform one of the following tasks:

Task	Steps
Remove an IT policy from user accounts	a. Click the **Assigned to users** tab. b. If necessary, search for user accounts. c. Select the user accounts that you want to remove the IT policy from. d. Click  .
Remove an IT policy from user groups	a. Click the **Assigned to groups** tab. b. If necessary, search for user groups. c. Select the user groups that you want to remove the IT policy from. d. Click  .

Delete an IT policy

You cannot delete the Default IT policy. When you delete a custom IT policy, BlackBerry UEM removes the IT policy from the users and devices that it is assigned to.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Select the check boxes for the IT policies you want to delete.
4. Click  .
5. Click **Delete**.

Export IT policies

You can export IT policies to an .xml file for auditing purposes.

Note:

Profiles that are associated with IT policies are not exported.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Select the check boxes for the IT policies you want to export.
4. Click  .
5. Click **Next**.
6. Click **Export**.

How BlackBerry UEM chooses which IT policy to assign

BlackBerry UEM sends only one IT policy to a device and uses predefined rules to determine which IT policy to assign to a user and the devices that the user activates.

Assigned to	Rules
User account (view Summary tab)	**1.** An IT policy assigned directly to a user account takes precedence over an IT policy assigned indirectly by user group. **2.** If a user is a member of multiple user groups that have different IT policies, BlackBerry UEM assigns the IT policy with the highest ranking. **3.** The Default IT policy is assigned if no IT policy is assigned to a user account directly or through user group membership.
Device (view device tab)	By default, a device inherits the IT policy that BlackBerry UEM assigns to the user who activates the device. If a device belongs to a device group, the following rules apply: **1.** An IT policy assigned to a device group takes precedence over the IT policy that BlackBerry UEM assigns to a user account. **2.** If a device is a member of multiple device groups that have different IT policies, BlackBerry UEM assigns the IT policy with the highest ranking.

BlackBerry UEM might have to resolve conflicting IT policies when you perform any of the following actions:

- Assign an IT policy to a user account, user group, or device group
- Remove an IT policy from a user account, user group, or device group
- Change the IT policy ranking
- Delete an IT policy
- Change user group membership (user accounts and nested groups)
- Change device attributes
- Change device group membership
- Delete a user group or device group

Importing IT policy and device metadata updates

BlackBerry regularly sends IT policy and device metadata updates to BlackBerry UEM installations to provide information about updates from device and OS vendors.

For example, after device vendor releases a new device model, BlackBerry may send updated device metadata to BlackBerry UEM installations so that activation and compliance profiles include the new device model and it can be allowed or restricted by the profile. After Apple, Google, or Microsoft release OS updates, a new IT policy pack may be sent to BlackBerry UEM UEM installations to allow you to control the new features in the OS update.

By default, BlackBerry UEM installs these updates automatically. If your organization's security policy does not allow automatic updates, you can turn off the automatic updates and import updates into BlackBerry UEM manually.

You can also set up event notifications to inform administrators when IT policy and device metadata updates have been installed.

Import IT policy and device metadata updates manually

BlackBerry sends notifications when new updates are available. Update files are cumulative. If you miss an update, the next update installs all previously updated IT policy rules or device metadata.

Before you begin: Download the metadata or IT policy pack according to the instructions in the update notification email.

1. On the menu bar, click **Settings**.
2. Click **Infrastructure > Import configuration data**.
3. Perform one or both of the following actions:
   - To turn off automatic updates for IT policy packs, clear the **Automatically update IT policy pack data** check box.
   - To turn off automatic updates for device metadata, clear the **Automatically update device metadata** check box.
4. Click the appropriate **Browse** button to find the data file that you want to import and after you locate the file, click **Open**.

Creating device support messages

For Android devices, you can create a support message that displays on the device when a feature is disabled by an IT policy. The message displays in the settings screen for the feature that is disabled. If you don't create a support message, the device displays the default message for the OS.

You can also specify an administrator support message that displays on the Device administrators settings screen. For example, you may want to display a disclaimer that your organization can monitor and manage apps and data in the work profile.

If your organization has users who work in more than one language, you can add support messages in additional languages and specify the default language that displays on devices that don’t use one of the available languages.

Create device support messages

Device support messages are supported by Android 8.0 and later devices.

1. On the menu bar, click **Settings > General settings**.
2. Click **Custom device support messages**.
3. On the **Custom device support messages** tab, click **Add**.
4. Select the language that you want the notification to appear in.
5. In the **Disabled feature notice** field, type the notice that you want to display on the device when a feature is disabled. The message can be up to 200 characters.
6. Optionally, in the **Administrator support message** field, type a notice that displays on the Device administrators settings screen.
7. If you want to create a message in more than one language, click **Add an additional language** and repeat steps 4 to 6 for each language.
8. If you added messages in more than one language, select **Default language** beside the language that you want to appear on devices that don’t use one of the available languages. For example, if English and French are the available languages, and English is the default language, the English message appears on devices that use German.
9. Click **Save**.

Enforcing compliance rules for devices

You can use compliance profiles to encourage users to follow your organization's standards for the use of devices. A compliance profile defines the device conditions that are not acceptable in your organization. For example, you can choose to disallow devices that are jailbroken, rooted, or have an integrity alert due to unauthorized access to the operating system.

A compliance profile specifies the following information:

- Conditions that would make a device non-compliant
- Email messages and device notifications that users receive if they violate the compliance conditions
- Actions that are taken if users do not correct the issue, including limiting a user's access to the organization's resources, deleting work data from the device, or deleting all data from the device

For Samsung Knox devices, you can add a list of restricted apps to a compliance profile. However, BlackBerry UEM does not enforce the compliance rules. Instead, the restricted app list is sent to devices and the device enforces compliance. Any restricted apps cannot be installed, or if they are already installed, they are disabled. When you remove an app from the restricted list, the app is re-enabled if it is already installed.

BlackBerry UEM includes a Default compliance profile. The Default compliance profile does not enforce any compliance conditions. To enforce compliance rules, you can change the settings of the Default compliance profile or you can create and assign custom compliance profiles. Any user accounts that are not assigned a custom compliance profile are assigned the Default compliance profile.

Create a compliance profile

Before you begin:

- If you define rules to restrict or allow specific apps, add those apps to the restricted apps list. For more information, see Add an app to the restricted app list. Note that this does not apply to built-in apps for supervised iOS devices. To restrict built-in apps you must create a compliance profile and add the apps to the restricted app list in the profile. For more information, see iOS: Compliance profile settings.
- If you want to send an email notification to users when their devices are not compliant, edit the default compliance email, or create a new email template. For more information, see Create a template for compliance email notifications.

Note: If you define rules for a jailbroken or rooted OS, restricted OS versions, or restricted device models, users will be unable to complete new activations for devices that are not compliant, regardless of the enforcement action that you set.

1. On the menu bar, click **Policies and profiles**.
2. Click **Compliance > Compliance**.
3. Click +.
4. Type a name and description for the compliance profile.
5. If you want to send a notification message to users when their devices become non-compliant, perform any of the following actions:
   - In the **Email sent when violation is detected** drop-down list, select an email template. To see the default compliance email, click Settings > General settings > Email templates.
   - In the **Enforcement interval** drop-down list, select how often BlackBerry UEM checks for compliance.
   - Expand **Device notification sent out when violation is detected**. Edit the message if necessary.

   You can use variables to populate notifications with user, device, and compliance information. For more information, see Variables.

6. Click the tab for each device type in your organization and configure the appropriate values for each profile setting. For details about each profile setting, see Compliance profile settings.
7. Click **Add**.

After you finish: If necessary, rank profiles.

Compliance profile settings

Compliance profiles are supported on the following device types:

- iOS
- macOS
- Android
- Windows

Common: Compliance profile settings

iOS, iPadOS, and Android devices

For each compliance rule that you select on the device tabs, choose the action that you want BlackBerry UEM to perform if a user's device is not compliant.

Common: Compliance profile setting	Description
Prompt behavior	This setting specifies whether BlackBerry UEM prompts the user to correct a compliance issue and gives the user time to fix the issue before taking action, or whether BlackBerry UEM takes immediate action. Possible values: • Prompt for compliance • Immediate enforcement action
Prompt method	This setting specifies how BlackBerry UEM prompts the user to correct a compliance issue. Possible values • Device notification • Email and device notification BlackBerry Dynamics apps don't send email notifications to users. BlackBerry Dynamics apps provide only device notifications, regardless of this setting. For compliance rules that apply to the device, the default value is "Email and device notification." For compliance rules that apply only to BlackBerry Dynamics apps, the default value is "Device notification." This setting is valid only if "Prompt behavior" is set to "Prompt for compliance."

Common: Compliance profile setting	Description
Prompt count	This setting specifies the number of times the user is prompted to correct a compliance issue. The default value is "3." This setting is valid only if "Prompt behavior" is set to "Prompt for compliance."
Prompt interval	This setting specifies the amount of time between prompts, in minutes, hours, or days. The default value is "4 hours." This setting is valid only if "Prompt behavior" is set to "Prompt for compliance."
Enforcement action for device	This setting specifies the action that BlackBerry UEM takes on devices that are not compliant. Possible values: • Monitor and log: BlackBerry UEM identifies the compliance violation but takes no enforcement action on the device. • Untrust: On iOS, iPadOS, macOS, Android, and Windows devices, this option prevents the user from accessing work resources and applications from the device. Data and apps are not deleted from the device. **Note:** On iOS and iPadOS devices, the work email account is removed from the native email app. Users must restore the email account settings to the app after the device returns to compliance. • Delete only work data • Delete all data • Remove from server: On iOS, iPadOS, Android, and Windows devices, a device can be deactivated from BlackBerry UEM if it violates the "Out of contact" rule. The default value is "Monitor and log." This setting is not valid for devices activated with User privacy. On devices activated with "Work and personal - user privacy," you cannot delete all data on a user's device. If you select, "Delete all data" BlackBerry UEM performs the same action as "Delete only work data." For Samsung Knox Workspace devices that have only a work space, if you select "Delete only work data," "Delete all data," or "Remove from server," all data will be deleted from the device. For supervised iOS and iPadOS devices, enforcement actions for the "Restricted app is installed" rule are not applicable. Users are automatically prevented from installing restricted apps.

Common: Compliance profile setting	Description
Enforcement action for BlackBerry Dynamics apps	This setting defines what happens with BlackBerry Dynamics apps when a device is not in compliance. Possible values: • Do not allow BlackBerry Dynamics apps to run • Delete BlackBerry Dynamics app data • Monitor and log: BlackBerry UEM identifies the compliance violation but takes no enforcement action The default value is "Monitor and log."

Windows 10 and macOS devices

For each compliance rule that you select on the device tabs, choose the action that you want BlackBerry UEM to perform if a user's device is not compliant.

Common: Compliance profile setting	Description
Enforcement action	This setting specifies the action that BlackBerry UEM takes on devices that are not compliant. Possible values: • Prompt for compliance • Untrust: On Windows devices, this option prevents the user from accessing work resources and applications from the device. Data and apps are not deleted from the device. **Note:** Untrust is not supported for BlackBerry Dynamics apps. • Delete only work data • Delete all data • Remove from server: On Windows devices, a device can be deactivated from BlackBerry UEM if it violates the "Out of contact" rule. • None: Identifies a compliance violation but takes no action. The default value is "Prompt for compliance."
Prompt method	The possible values are: • Email notification • Device notification • Both The default value is "Both." This setting is valid only if the "Enforcement action" is set to "Prompt for compliance." Device notifications are not supported on Windows 10 devices.

Common: Compliance profile setting	Description
Prompt count	This setting specifies the number of times the user is prompted to correct the breach. The default value is "3." This setting is valid only if the "Enforcement action" is set to "Prompt for compliance."
Prompt interval	This setting specifies the amount of time between prompts, in minutes, hours, or days. The default value is "4 hours." This setting is valid only if the "Enforcement action" is set to "Prompt for compliance."
Prompt interval expired action	This setting defines what happens when the user has received the total number of prompts as defined in Prompt count, and the does not correct the breach. Possible values: • None • Untrust: On Windows devices, this option prevents the user from accessing work resources and applications from the device. Data and applications are not deleted from the device. **Note:** Untrust is not supported for BlackBerry Dynamics apps. Use an alternate enforcement action. • Delete only work data • Delete all data The default value is "Untrust." This setting is valid only if the "Enforcement action" is set to "Prompt for compliance".
Enforcement action for BlackBerry Dynamics apps	This setting defines what happens with BlackBerry Dynamics apps when a device is not in compliance. Possible values: • Delete BlackBerry Dynamics app data • Do not allow BlackBerry Dynamics apps to run The default value is "Delete BlackBerry Dynamics app data."

iOS: Compliance profile settings

See Common: Compliance profile settings for descriptions of the possible actions if you select a compliance rule.

These settings also apply to iPadOS devices.

iOS: Compliance profile setting	Description
Jailbroken OS	This setting creates a compliance rule to ensure that devices are not jailbroken. A device is jailbroken when a user or attacker bypasses various restrictions on a device to modify the OS. If you select this setting, users will also be unable to complete new activations for jailbroken devices, regardless of the enforcement action that you set.
Non-assigned app is installed	This setting creates a compliance rule to ensure that devices do not have apps installed that were not assigned to the user. When you select this setting and a non-assigned app is installed on a device, a warning message and a link is displayed on the Managed Devices tab. When you click the link, a list of apps that are putting the device out of compliance is displayed. This setting is not valid for devices activated with the User privacy activation type.
Required app is not installed	This setting creates a compliance rule to ensure that devices have required apps installed. When you select this setting and a required app is not installed on a device, a warning message and a link is displayed on the Managed Devices tab. When you click the link, a list of applications that are putting the device out of compliance is displayed.
Restricted OS version is installed	This setting creates a compliance rule to ensure that devices do not have a restricted OS version installed. You can select the restricted OS versions. If you select this setting, users will be unable to complete new activations for devices that are not compliant, regardless of the enforcement action that you set.
Restricted device model detected	This setting creates a compliance rule to restrict device models. You can choose one of these options: • Allow selected device models • Do not allow selected device models You can select the devices models that are allowed or restricted. If you select this setting, users will be unable to complete new activations for devices that are not compliant, regardless of the enforcement action that you set.
Device is out of contact	This setting creates a compliance rule to ensure that devices are not out of contact with BlackBerry UEM for more than a specified amount of time.
Last contact time	This setting specifies the number days a device can be out of contact with BlackBerry UEM. This setting is valid only if the "Device out of contact" setting is selected.

iOS: Compliance profile setting	Description
BlackBerry Dynamics library version verification	This setting creates a compliance rule that allows you to select the BlackBerry Dynamics library versions that cannot be activated. You can select the blocked library versions.
BlackBerry Dynamics connectivity verification	This setting creates a compliance rule to monitor whether BlackBerry Dynamics apps are out of contact with BlackBerry UEM for more than a specified amount of time. The enforcement action is applied to BlackBerry Dynamics apps. The "Base connectivity interval on authentication delegate apps" setting specifies that the connectivity verification is based on when an authentication delegate app connects to BlackBerry UEM. This setting applies only if an authentication delegate is specified in a BlackBerry Dynamics profile. The "Last contact time" setting specifies the number days a device can be out of contact with BlackBerry UEM before the device is out of compliance. BlackBerry Dynamics apps don’t prompt users for compliance for this rule. If you set the “Prompt behavior” setting to “Prompt for compliance,” the user is not prompted. If the device is able to contact UEM, the device returns to compliance when the user opens the BlackBerry Dynamics app.
BlackBerry Dynamics app screen capture detected	This setting creates a compliance rule that reacts to screen captures of BlackBerry Dynamics apps on devices. The "Maximum number of screen captures within period" setting specifies the number of allowed screen captures within the time that you specify in the "Period length" field. The "Enforcement action for BlackBerry Dynamics apps" setting specifies the action that occurs if the user exceeds the allowed number of screen captures.

iOS: Compliance profile setting	Description
Restricted app is installed	This setting creates a compliance rule for BlackBerry UEM to periodically check for restricted apps. To restrict apps, complete any of the following tasks: • Select an app from the restricted app list. For more information, see Add an app to the restricted app list. Do one of the following: • To select apps using the app name, click the Select apps from the app list option. • To select apps using the app package ID, click the Specify the app package ID option. You should not use the package ID to add public apps. Add public apps to the restricted app list and then use the Select apps from the app list option to select the apps instead. • Select a built-in app (supervised devices only) To remove an app from the list, click ✕. When you select this setting and a restricted app is installed on a device, a warning message and a link is displayed on the Managed Devices tab. When you click the link, a list of applications that are putting the device out of compliance is displayed. For supervised devices, enforcement actions for this rule are not applicable. Users are automatically prevented from installing restricted apps. If restricted apps (either built-in or installed by the user) are already installed, those apps are automatically removed from the device.
Show only allowed apps on device	This setting creates a compliance rule that specifies a list of apps that are allowed to be installed on users' devices. All other apps are not allowed. To allow specific apps, complete one of the following tasks: • Select an app from the restricted app list. For more information, see Add an app to the restricted app list. • Select a built-in app Some apps are included in the allowed list by default. To remove an app from the list, click ✕. This setting is valid only for supervised devices.

macOS: Compliance profile settings

See Common: Compliance profile settings for descriptions of the possible actions if you select a compliance rule.

macOS: Compliance profile setting	Description
Restricted OS version is installed	This setting creates a compliance rule to ensure that devices do not have a restricted OS version installed. You can select the restricted OS versions. If you select this setting, users will be unable to complete new activations for devices that are not compliant, regardless of the enforcement action that you set.
Restricted device model detected	This setting creates a compliance rule to restrict device models. You can choose one of these options: • Allow selected device models • Do not allow selected device models You can select the the devices models that are allowed or restricted. If you select this setting, users will be unable to complete new activations for devices that are not compliant, regardless of the enforcement action that you set.
BlackBerry Dynamics library version verification	This setting creates a compliance rule that allows you to select the BlackBerry Dynamics library versions that cannot be activated. You can select the blocked library versions.
BlackBerry Dynamics connectivity verification	This setting creates a compliance rule to monitor whether BlackBerry Dynamics apps are out of contact with BlackBerry UEM for more than a specified amount of time. The enforcement action is applied to BlackBerry Dynamics apps. The "Base connectivity interval on authentication delegate apps" setting specifies that the connectivity verification is based on when an authentication delegate app connects to BlackBerry UEM. This setting applies only if an authentication delegate is specified in a BlackBerry Dynamics profile. The "Last contact time" setting specifies the number days a device can be out of contact with BlackBerry UEM before the device is out of compliance.

Android: Compliance profile settings

See Common: Compliance profile settings for descriptions of the possible actions if you select a compliance rule.

Android: Compliance setting	Description
Rooted OS or failed Knox attestation	This setting creates a compliance rule that specifies the actions that occur if a user or attacker gains access to the root level of an Android device. A device is rooted when a user or attacker gains access to the root level of the Android OS. This rule applies to the rooted state of the device the UEM Client, the BlackBerry Dynamics SDK or Knox Attestation detects it. If you select this setting, users will be unable to complete new activations for rooted devices, regardless of the enforcement action that you set. If you set a compliance rule for "Rooted OS or failed Knox attestation," selecting "Enable anti-debugging for BlackBerry Dynamics apps" stops BlackBerry Dynamics apps if the BlackBerry Dynamics Runtime detects an active debugging tool.
SafetyNet attestation failure	This setting creates a compliance rule that specifies the actions that occur if devices do not pass SafetyNet attestation. When you use SafetyNet attestation, BlackBerry UEM sends challenges to test the authenticity and integrity of Android devices and apps in your organization's environment. For these settings to take affect, you must enable the SafetyNet attestation feature in the management console under Settings > Attestation > SafetyNet attestation frequency. For more information about configuring SafetyNet attestation, see Configure attestation for Android devices and BlackBerry Dynamics apps using SafetyNet .
Non-assigned app is installed	This setting creates a compliance rule to ensure that devices do not have apps installed that were not assigned to the user. When you select this setting and a non-assigned app is installed on an Android device, a warning message and a link is displayed on the Managed Devices tab. When you click the link, a list of applications that are putting the device out of compliance is displayed. For Android Enterprise and Samsung Knox devices, users can't install non-assigned apps in the work space. The enforcement actions do not apply. This setting is not valid for devices activated with User privacy.
Required app is not installed	This setting creates a compliance rule to ensure that devices have required apps installed. When you select this setting and a required app is not installed on an Android device, a warning message and a link is displayed on the Managed Devices tab. When you click the link, a list of applications that are putting the device out of compliance is displayed. For Android Enterprise devices the enforcement actions do not apply. For Samsung Knox devices, required internal apps are automatically installed. The enforcement actions apply only to required public apps.

Android: Compliance setting	Description
Restricted OS version is installed	This setting creates a compliance rule to ensure that devices do not have a restricted OS version installed. You can select the restricted OS versions. If you select this setting, users will be unable to complete new activations for devices that are not compliant, regardless of the enforcement action that you set.
Restricted device model detected	This setting creates a compliance rule to restrict device models. You can choose one of these options: • Allow selected device models • Do not allow selected device models You can specify the devices models that are allowed or restricted. If you select this setting, users will be unable to complete new activations for devices that are not compliant, regardless of the enforcement action that you set.
Device out of contact	This setting creates a compliance rule to monitor whether devices are out of contact with BlackBerry UEM for more than a specified amount of time. The "Last contact time" setting specifies the number days a device can be out of contact with BlackBerry UEM before the device is out of compliance.
Required security patch level is not installed.	This setting creates a compliance rule to ensure that devices have required security patches installed. You can specify the device models that must have security patches installed and a security patch date. Devices running a security patch equal to or later than the specified security patch date are considered compliant. After an upgrade, if you have previously created a compliance profile with the "Required security patch level is not installed" setting enabled, the enforcement action is set to "Monitor and log". This setting is valid for devices and for BlackBerry Dynamics apps developed with BlackBerry Dynamics SDK 6.0 and later.
BlackBerry Dynamics library version verification	This setting creates a compliance rule that allows you to select the BlackBerry Dynamics library versions that cannot be activated. You can select the blocked library versions.

Android: Compliance setting	Description
BlackBerry Dynamics connectivity verification	This setting creates a compliance rule to monitor whether BlackBerry Dynamics apps are out of contact with BlackBerry UEM for more than a specified amount of time. The enforcement action is applied to BlackBerry Dynamics apps. The "Base connectivity interval on authentication delegate apps" setting specifies that the connectivity verification is based on when an authentication delegate app connects to BlackBerry UEM. This setting applies only if an authentication delegate is specified in a BlackBerry Dynamics profile. The "Last contact time" setting specifies the number days a device can be out of contact with BlackBerry UEM before the device is out of compliance. BlackBerry Dynamics apps don't prompt users for compliance for this rule. If you set the "Prompt behavior" setting to "Prompt for compliance," the user is not prompted. If the device is able to contact UEM, the device returns to compliance when the user opens the BlackBerry Dynamics app.
Restricted app is installed	This setting creates a compliance rule to ensure that devices do not have restricted apps installed. To restrict apps, see Add an app to the restricted app list. For Android Enterprise devices, users can't install restricted apps in the work space. The enforcement actions do not apply. For Samsung Knox devices, restricted apps in the work space are automatically disabled. The enforcement actions do not apply. For Android Enterprise and Samsung Knox devices with Work and personal - full control activations, select "Enforce compliance actions in the personal space" to apply the rule to apps in both the work profile and the personal profile. This option is supported only on Android 10 and earlier devices. This setting is not valid for devices activated with User privacy. When you select this setting and a restricted app is installed on an Android device, a warning message and a link is displayed on the Managed Devices tab. When you click the link, a list of applications that are putting the device out of compliance displays. **Note:** If you have activated a device using the Android Enterprise - Full Control activation type, and you use this option to disable apps on the personal side of the device, when the device is upgraded from Android 10 to Android 11 those apps become permanently disabled unless you re-activate the device. For more information, visit support.blackberry.com/community to read article 76852.
Password does not meet complexity requirements	This setting creates a compliance rule to ensure that the user has set device or work space passwords that meet the complexity requirements defined in the IT policy assigned to them.

Windows: Compliance profile settings

See Common: Compliance profile settings for descriptions of the possible actions if you select a compliance rule.

Windows: Compliance profile setting	Description
Required app is not installed	This setting creates a compliance rule to ensure that devices have required apps installed. Internal app dispositions can't be monitored.
Restricted OS version is installed	This setting creates a compliance rule to ensure that devices do not have a restricted OS version installed as specified in this setting. You can select the restricted OS versions.
Restricted device model detected	This setting creates a compliance rule to restrict device models as specified in this setting. Possible values: • Allow selected device models • Do not allow selected device models You can select the device models that are allowed or restricted.
Device out of contact	This setting creates a compliance rule to ensure that devices are not out of contact with BlackBerry UEM for more than a specified amount of time.
BlackBerry Dynamics library version verification	This setting creates a compliance rule that allows you to select the BlackBerry Dynamics library versions that cannot be activated. You can select the blocked library versions.
BlackBerry Dynamics connectivity verification	This setting creates a compliance rule to ensure that BlackBerry Dynamics apps are not out of contact with BlackBerry UEM for more than a specified amount of time. The enforcement action is applied to BlackBerry Dynamics apps.
Antivirus signature	This setting creates a compliance rule to ensure that devices have an antivirus signature enabled.
Antivirus status	This setting creates a compliance rule to ensure that devices have antivirus software enabled. You can select the vendors that are allowed.
Firewall status	This setting creates a compliance rule to ensure that devices have a firewall enabled.
Encryption status	This setting creates a compliance rule to ensure that devices require encryption.
Windows update status	This setting creates a compliance rule to ensure that devices allow BlackBerry UEM to install Windows OS updates or notify users of required updates.
Restricted app is installed	This setting creates a compliance rule to ensure that devices do not have restricted apps installed. To restrict apps, see Add an app to the restricted app list.
Grace period expired	This setting creates a compliance rule to specify actions that occur if the attestation grace period has expired.

Windows: Compliance profile setting	Description
Attestation Identity Key not present	This setting creates a compliance rule to specify actions that occur if an AIK is not present on the device.
Data Execution Prevention Policy is disabled	This setting creates a compliance rule to specify actions that occur if the DEP policy is disabled on the device.
BitLocker is disabled	This setting creates a compliance rule to specify actions that occur if BitLocker is disabled on the device.
Secure Boot is disabled	This setting creates a compliance rule to specify actions that occur if Secure Boot is disabled on the device.
Code integrity is disabled	This setting creates a compliance rule to specify actions that occur if the Code Integrity feature is disabled on the device.
Device is in safe mode	This setting creates a compliance rule to specify actions that occur if the device is in safe mode.
Device is in Windows preinstallation environment	This setting creates a compliance rule to specify actions that occur if the device is in the Windows preinstallation environment.
Early launch antimalware driver is not loaded	This setting creates a compliance rule to specify actions that occur if the early launch antimalware driver is not loaded.
Virtual Secure Mode is disabled	This setting creates a compliance rule to specify actions that occur if Virtual Secure Mode is disabled.
Boot debugging is enabled	This setting creates a compliance rule to specify actions that occur if boot debugging is enabled.
OS kernel debugging is enabled	This setting creates a compliance rule to specify actions that occur if OS kernel debugging is enabled.
Test signing is enabled	This setting creates a compliance rule to specify actions that occur if test signing is enabled.
Boot manager revision list is not the expected version	This setting creates a compliance rule to specify actions that occur if the boot manager revision list is not the expected version.
Code Integrity revision list is not the expected version	This setting creates a compliance rule to specify actions that occur if the code integrity revision list is not the expected version.
Code Integrity policy hash is present and is not an allowed value	This setting creates a compliance rule to specify actions that occur if the code integrity policy hash is present and is not an allowed value.

Windows: Compliance profile setting	Description
Custom Secure Boot configuration policy hash is present and is not an allowed value	This setting creates a compliance rule to specify actions that occur if the Custom Secure Boot configuration policy hash is present and is not an allowed value.
PCR value is not an allowed value	This setting creates a compliance rule to specify actions that occur if the PCR value is not an allowed value.

Managing BlackBerry Dynamics compliance profiles

BlackBerry Dynamics compliance profiles are imported from Good Control when you synchronize Good Control with BlackBerry UEM. You cannot edit BlackBerry Dynamics compliance profiles, but they can be used as a reference when you are creating new compliance profiles in BlackBerry UEM. Users that were assigned to a compliance profile in Good Control remain assigned to the same profile after they are synchronized with BlackBerry UEM. When a user is assigned to a BlackBerry Dynamics compliance profile, the BlackBerry Dynamics compliance profile takes precedence over any BlackBerry Dynamics rules in the BlackBerry UEM compliance profiles that a user may also be assigned to.

Setting	Description
Jailbroken OS	This setting specifies the actions that occur if a user or attacker bypasses various restrictions on a device to modify the OS, installs unapproved apps, or obtains elevated permissions and the actions that occur for BlackBerry Dynamics apps if a jailbroken OS is used.
OS version verification	This setting specifies the versions of the OS that are allowed and restricted and the actions that occur for BlackBerry Dynamics apps if a restricted OS is installed on a device.
Hardware model verification	This setting specifies the hardware models that are allowed and restricted and the actions that occur for BlackBerry Dynamics apps if a restricted hardware model is being used.
BlackBerry Dynamics library version verification	This setting specifies the BlackBerry Dynamics libraries that can be used and the actions that occur for BlackBerry Dynamics apps if a device is using a disallowed version of the library.
Connectivity verification	This setting specifies whether a device must connect to BlackBerry UEM within a specified number of days and the actions that occur for BlackBerry Dynamics apps if a device does not connect to BlackBerry UEM. The "Base connectivity interval on auth delegate app" subsetting specifies whether the app that is set as the authentication delegate manages the connectivity interval. If you use the authentication delegate to manage the connectivity interval, less frequently used apps will not be blocked or wiped if they do not connect to BlackBerry UEM.

Sending commands to users and devices

You can send various commands to manage user accounts and devices. The list of commands that are available depends on the device type and activation type. You can send commands to a specific user or device, or you can send commands to multiple users and devices using bulk commands.

For example, you can use commands in the following circumstances:

- If a device is temporarily misplaced, you can send a command to lock the device or delete work data from the device.
- If you want to redistribute a device to another user in your organization, or if a device is lost or stolen, you can send a command to delete all data from the device.
- When an employee leaves your organization, you can send a command to the user's personal device to delete only the work data.
- If a user forgets the work space password, you can send a command to reset the work space password.
- For users with supervised DEP devices, you can send a command to trigger an OS upgrade.

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.

Send a bulk command

You can send a command to multiple user accounts or devices at the same time by selecting the users or devices from the user list and sending a bulk command.

Before you begin: If you want to set an expiry period for commands that delete data from devices, see Set an expiry time for commands.

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

Icon	Description
	Locate devices You can select a maximum of 100 devices at a time. For more information, see Locate a device.
	Send email For more information, see Send an email to users.
	Send activation email For more information, see Send an activation email to multiple users.
	Add to user groups You can select a maximum of 200 devices at a time. For more information, see Add users to user groups.
	Export For more information, see Export the user list to a .csv file.
	Remove devices To use this bulk command, you must be a Security Administrator. You can select a maximum of 200 devices at a time. For more information, see Commands reference.
	Update device information. For more information, see Commands reference.
	Delete all device data To use this command, you must be a Security Administrator. You can select a maximum of 200 devices at a time. This bulk command is not supported for macOS devices. For more information, see Commands reference.
	Delete only work data To use this command, you must be a Security Administrator. You can select a maximum of 200 devices at a time. For more information, see Commands reference.
	Edit device ownership You can select a maximum of 100 devices at a time. For more information, see Change the device ownership label.

Icon	Description
	Update OS You can force supervised iOS devices to install an available OS update. To use this command, you must be a Security Administrator. You can select a maximum of 200 devices at a time. For more information, see Update the OS on supervised iOS devices.
	Change console passwords You can send a BlackBerry UEM Self-Service password to multiple users at one time. For more information, see Send a BlackBerry UEM Self-Service password to multiple users.

Set an expiry time for commands

When you send the "Delete all device data" or "Delete only work data" command to a device, the device must connect to BlackBerry UEM for the command to complete. If the device is unable to connect to BlackBerry UEM, the command remains in pending status and the device is not removed from BlackBerry UEM unless you manually remove it. Alternatively, you can configure BlackBerry UEM to automatically remove devices when the commands do not complete after a specified amount of time.

1. On the menu bar, click **Settings > General settings > Delete command expiry**.
2. For one or both of **Delete all device data** and **Delete only work data** , select **Automatically remove the device if the command has not completed**.
3. In the **Command expiration** field, type the number of days after which the command expires and the device is automatically removed from BlackBerry UEM.
4. Click **Save**.

Commands reference

The commands you can send to devices depends on the device type and activation type. Some commands can be sent to multiple devices at the same time.

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

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
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 only for supervised devices. This command is not supported for Apple TV devices.	MDM controls

Command	Description	Activation types
Deactivate BlackBerry 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. For more information, see Update the OS on supervised iOS devices. To send this command to multiple devices, see Send a bulk command. This command is supported only for supervised devices. This command is not supported for Apple TV devices.	MDM controls
Restart device	This command forces devices to restart. This command is supported only for supervised devices. This command is not supported for Apple TV devices.	MDM controls
Turn off device	This command forces devices to turn off. This command is supported only for supervised devices. 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
Update device information	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. To send this command to multiple devices, see Send a bulk command.	MDM controls User privacy
Update time zone	This command sets the device time according to the region that you select.	MDM controls

Command	Description	Activation types
Remove device	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. 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. To send this command to multiple devices, see Send a bulk command.	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

Commands for macOS devices

Command	Description
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.
View device actions	This command displays any actions that are in progress on a device. For more information, see Viewing device actions.
Lock desktop	This command allows you to set a PIN and lock the device.
Delete only work data	This command deletes work data, including the IT policy, profiles, apps, and certificates that are on the device, and optionally, deletes the device from BlackBerry UEM. To send this command to multiple devices, see Send a bulk command.
Delete all device data	This command deletes all user information and app data from the device. It returns the device to factory defaults, locks the device with a PIN that you set, and optionally, deletes the device from BlackBerry UEM.
Update desktop data	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. To send this command to multiple devices, see Send a bulk command.
Remove device	This command removes the device from BlackBerry UEM. The device may continue to receive email and other work data. To send this command to multiple devices, see Send a bulk command.

Commands for Android 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.	All (except BlackBerry 2FA)
View device actions	This command displays any actions that are in progress on a device. For more information, see Viewing device actions.	All (except BlackBerry 2FA)
Lock device	This command locks the 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.	MDM controls Work and personal - full control (Android Enterprise) Work and personal - user privacy (Android Enterprise) Work space only (Android Enterprise)
Delete all device data	This command deletes all user information and app data that the device stores, including information in the work space 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, including the work space, if applicable. To send this command to multiple devices, see Send a bulk command.	MDM controls Work and personal - full control (Android Enterprise) Work and personal - full control (Samsung Knox) Work space only - (Samsung Knox)

Command	Description	Activation types
Delete only work data	This command deletes work data, including the IT policy, profiles, apps, and certificates that are on the device and deactivates the device. If the device has a work space, the work space information and the work space are deleted from the device but all personal apps and data remain on the device. For more information, see Deactivating devices. When you use this command on Android Enterprise devices, you can type a reason that appears in the notification on the user's device to explain why the work profile was deleted. For Work and personal - full control (Android Enterprise) activations, this command is supported only by devices running Android 11 and later. 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, including the work space, if applicable. To send this command to multiple devices, see Send a bulk command.	MDM controls Work and personal - user privacy (Android Enterprise) Work and personal - full control (Android Enterprise) Work and personal - user privacy (Samsung Knox) Work and personal - full control (Samsung Knox) Work space only - (Samsung Knox)
Unlock device and clear password	This command unlocks the device and prompts the user to create a new device password. If the user skips the "Create device password" screen, the previous password is retained. You can use this command if a user forgets the device password. **Note:** This command is not supported by devices with Samsung Knox SDK 3.2.1 and later.	MDM controls (Samsung devices only) Work and personal - full control (Samsung Knox) Work and personal - user privacy (Samsung Knox)
Specify device password and lock	This command lets you create a device password and then lock the device. You must create a password that complies with existing password rules. To unlock the device, the user must type the new password. **Note:** For the Work and personal - user privacy activation types, only BlackBerry devices powered by Android 8.x and later support this command. **Note:** For the Work and personal - full control (Android Enterprise) activation type, only devices that use a version of the Android OS earlier than Android 11 support this command.	Work and personal - full control (Samsung Knox) Work space only (Android Enterprise) Work and personal - full control (Android Enterprise) Work and personal - user privacy (Android Enterprise)

Command	Description	Activation types
Reset work space password	This command deletes the current work space password from the device. When the user opens the work space, the device prompts the user to set a new work space password.	Work and personal - full control (Samsung Knox) Work and personal - user privacy - (Samsung Knox) Work space only - (Samsung Knox)
Specify work space password and lock	You can specify a work profile password and lock the device. When the user opens a work app, they must type the password that you specified.	Work and personal - user privacy (Android Enterprise) Work and personal - full control (Android Enterprise)
Disable/enable work space	This command disables or enables access to the work space apps on the device.	Work and personal - full control (Samsung Knox) Work and personal - user privacy - (Samsung Knox) Work space only - (Samsung Knox)
Deactivate BlackBerry 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.	BlackBerry 2FA
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	All (except BlackBerry 2FA)
Update device information	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. To send this command to multiple devices, see Send a bulk command.	All (except BlackBerry 2FA)
Request bug report	This command sends a request to the device for the client logs. The device user must accept or decline the request.	Work space only (Android Enterprise) Work and personal - full control (Android Enterprise)

Command	Description	Activation types
Restart device	This command sends a request to the device to restart. A message displays to the user that the device will restart in one minute. The device user has the option to snooze the restart for 10 minutes.	Work space only (Android Enterprise)
Remove device	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. 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. To send this command to multiple devices, see Send a bulk command.	All (except BlackBerry 2FA)

Commands for Windows devices

Command	Description
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.
View device actions	This command displays any actions that are in progress on a device. For more information, see Viewing device actions.
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 supported only on devices running Windows 10 Mobile.
Generate device password and lock	This command generates a device password and locks the device. The generated password is sent to the user by email. You can use the preselected email address, or specify an email address. The generated password complies with any existing password rules. This command is supported only on devices running Windows 10 Mobile.

Command	Description
Delete only work data	This command deletes work data, including the IT policy, profiles, apps, and certificates that are on the device, and optionally, deletes the device from BlackBerry UEM. The user account is not deleted when you send this command. After you send this command, you are given the option of deleting the device from BlackBerry UEM. If the device is unable to connect to BlackBerry UEM, you can remove the device from BlackBerry UEM. If the device connects to BlackBerry UEM after you removed it, only the work data is deleted from the device, including the work space, if applicable. To send this command to multiple devices, see Send a bulk command.
Delete all device data	This command deletes all user information and app data that the device stores. It returns the device to factory defaults and optionally, deletes the device from BlackBerry UEM. After you send this command, you are given the option of deleting the device from BlackBerry UEM. If the device is unable to connect to BlackBerry UEM, you can remove the device from BlackBerry UEM. If the device connects to BlackBerry UEM after you removed it, only the work data is deleted from the device, including the work space, if applicable. To send this command to multiple devices, see Send a bulk command.
Restart desktop/device	This command forces devices to restart.
Update device information	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. The command also sends a request to the device to create a health certificate validation request. The device sends the request to the Microsoft Health Attestation Service to check for compliance. This feature is only supported in an on-premises environment. To send this command to multiple devices, see Send a bulk command.
Remove device	This command removes the device from BlackBerry UEM. The device may continue to receive email and other work data. To send this command to multiple devices, see Send a bulk command.

Deactivating devices

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 only work data" or "Delete all device data" command. BlackBerry UEM may also deactivate a device if it violates the compliance profile and the specified enforcement action is to deactivate the device. Users can deactivate their devices using the following methods:

- For iOS and Android devices, users can select Deactivate My Device on the About screen in the BlackBerry UEM Client app.
- For Windows 10 devices, users can select Settings > Accounts > Work access > Delete.

For devices that use Knox MDM, when the device is deactivated, internal apps are uninstalled, and the uninstall option becomes available for any public apps that were installed from the app list as required.

For Android Enterprise devices that only have a work profile, if you deactivate a device you have the option to delete all data from the SD card and remove factory reset protection.

For Android Enterprise devices with Work and personal - user privacy and Work and personal - full control activations, if you use the "Delete only work data" command you can type a reason that appears in the notification on the user's device to explain why the work profile was deleted. If the device is deactivated for violating compliance rules, the notification specifies the reason the device was out of compliance.

For Android Enterprise devices with Work and personal - full control activations, only the "Delete all device data" command is supported by devices running Android 10 and earlier. The "Delete only work data" command is supported by devices running Android 11 and later. The "Delete only work data" command removes all work data and apps but allows the user to keep personal data and apps and continue using the unmanaged device.

For Samsung Knox Workspace devices that have been activated using the Work and personal - full control or Work space only activation types, deactivating the device deletes all data from the device or from the work space only. You can specify which data is wiped using the "Data wipe on deactivation" IT policy rule.

Controlling the software updates that are installed on devices

You can control the device software releases that are installed on Android Enterprise and Samsung Knox devices. For Android Enterprise devices, you can also set an update period for apps that are running in the foreground.

For Android Enterprise devices with Work space only and Work and personal - full control activations, you can specify whether the user can choose when to install available software updates or whether software updates are automatically installed. You can specify different rules depending on the device model and currently installed OS version. For all Android Enterprise devices, you can also set an update period for apps that are running in the foreground because, by default, when an app is running in the foreground, Google Play can't update it. You can also control how Google Play applies the changes to the device, for example, specifying whether the user can allow the change or whether the change occurs only when the device is connected to a Wi-Fi network.

For Android Enterprise devices with Work space only and Work and personal - full control activations, for any devices that you have specified an OS update rule other than the default rule, you can also suspend updates during dates when updates should not occur. For example, you may want to suspend updates during holiday periods. If you want to suspend updates for all devices, you must first create an OS update rule for all devices. For example you could create an OS update rule for all devices running Android 7.0 and later to apply updates automatically at certain hours.

On Samsung Knox devices, you can use Enterprise Firmware Over the Air (E-FOTA) to control when firmware updates from Samsung are installed.

Note: Samsung E-FOTA will reach end of service on July 31, 20022. For more information see the information from Samsung. For information about migrating to Samsung E-FOTA One, visit support.blackberry.com to read article 69901.

Samsung Knox devices that are activated as Work space only (Samsung Knox), Work and personal - full control (Samsung Knox), Work space only (Android Enterprise fully managed device), and Work and personal - full control (Android Enterprise fully managed device with work profile) support software restrictions using E-FOTA.

E-FOTA is not supported for Work and personal - user privacy (Samsung Knox) or Work and personal - user privacy (Android Enterprise with work profile) activation types.

Controlling firmware versions ensures that users' devices are using firmware versions that their apps support and comply with your organization's policies. You can use a device SR requirements profile to create firmware rules for the Samsung Knox devices that are activated on UEM. You can schedule when firmware updates are installed and specify when forced updates must be installed. For more information about E-FOTA, visit https://seap.samsung.com/sdk/enterprise-fota.

Note: Depending on the wireless service provider that a device uses, E-FOTA updates may not be available. Some wireless service providers (for example, AT&T and Verizon) use their own systems to manage wireless updates.

On devices with MDM controls activations, you can't control when and how users update their device OS but you can use compliance profiles to restrict a device OS version. For all devices, to enforce a particular action if a restricted software release version is installed on a device, you must create a compliance profile and assign the compliance profile to users, user groups, or device groups. The compliance profile specifies the actions that occur if the user does not remove the restricted software release from the device.

You can't control the software releases installed on iOS devices, but you can can force supervised iOS devices to install an available update. For more information, see Update the OS on supervised iOS devices.

Create a device SR requirements profile for Android Enterprise devices

OS update rules apply only to Work space only and Work and personal - full control devices. App update rules apply to all Android Enterprise devices. For more information on setting rules for Samsung Knox devices that use E-FOTA, see Create a device SR requirements profile for Samsung Knox devices.

Note: Samsung E-FOTA will reach end of service on July 31, 20022. For more information see the information from Samsung. For information about migrating to Samsung E-FOTA One, visit support.blackberry.com to read article 69901.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Compliance > Device SR requirements**
3. Click +.
4. Type a name and description for the profile.
5. Click the **Android** tab.
6. For Work space only and Work and personal - full control devices, perform the following steps to set rules for OS updates:
   a) In the **OS update rule** table, click +.
   b) In the **Device model** drop-down list, select a device model.
   c) In the **OS version** drop-down list, select the installed OS version.
   d) In the **Update rule** drop-down list, select one of the following options:
      - Select **Default** to allow the user to choose when to install updates.
      - Select **Update automatically** to install updates without prompting the user.
      - Select **Update automatically between** to install updates between the times you specify without prompting the user. The user can choose to install updates outside of this window.
      - Select **Postpone up to 30 days** to block installation of updates for 30 days. After 30 days, the user can choose when to install an update. Depending on the device manufacturer and wireless service provider, security updates might not be postponed.
   e) When you are done, click **Add**.
   f) Repeat step 6 for each rule that you want to add.

   Rules set for Samsung Knox devices that use E-FOTA take precedence over these rules.
7. For Work space only and Work and personal - full control devices, if you want to specify time periods when OS updates should not occur, perform the following steps:
   a) In the **Suspend OS updates** table, click +.
   b) In the **Start month** drop-down list, select the month that the suspension period starts.
   c) In the **Start day** drop-down list, select the day that the suspension period starts.
   d) In the **Duration** drop-down list, select the length of the suspension.

      The suspension can't exceed 90 days. If you specify more than one suspension period, there must be at least 60 days between periods.

      These settings don't apply to Samsung Knox devices that use E-FOTA.
8. To specify an update period for apps that are running in the foreground, select **Enable update period for apps that are running in the foreground**, and set the following options:
   - **Start time (local device time)**: Specifies the time when apps will start to update.
   - **Duration**: Specifies the number of hours that you will allow apps to be updated.

9. To specify how Google Play applies the changes to apps running in the foreground, select App auto update policy. Select one of the following options:
   - **User can allow**: The user is prompted to allow the apps to update on the device. Note that this is the default setting if you don't select the App auto update policy option
   - **Always**: The apps will always update. Note that for an app that is always running, such as BlackBerry UEM Client, BlackBerry Work, or BlackBerry Connectivity, if you don't select the **Enable update period for apps that are running in the foreground** option, the app will not update until the user manually updates the app on the device.
   - **Wi-Fi only**: The apps will update only when the device is connected to a Wi-Fi network. Note that for an app that is always running, such as BlackBerry UEM Client, BlackBerry Work, or BlackBerry Connectivity, if you don't select the **Enable update period for apps that are running in the foreground** option, the app will not update until the user manually updates the app on the device.
   - **Disable**: The apps will never update.

     Note:

     This profile affects the Auto-Update Apps setting in Google Play. If you select **Always**, **Wi-Fi only**, or **Disable**, the user cannot select a different option on the device. For example, if you select **Disable** in the profile, the user cannot enable an app to update on the device. However, users can still manually update apps in Google Play.
10. Click **Add**.

After you finish: If necessary, rank profiles.

Create a device SR requirements profile for Samsung Knox devices

Note: Depending on the wireless service provider that a device uses, E-FOTA updates may not be available. Some wireless service providers (for example, T&T and Verizon) use their own systems to manage wireless updates.

Before you begin: Verify that an E-FOTA license has been added to BlackBerry UEM. To use E-FOTA, you must select the Android global "Allow OTA updates" rule in the associated IT policy in the BlackBerry UEM management console.

Note: Samsung E-FOTA will reach end of service on July 31, 20022. For more information see the information from Samsung. For information about migrating to Samsung E-FOTA One, visit support.blackberry.com to read article 69901.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Compliance > Device SR requirements**.
3. Click +.
4. Type a name and description for the profile.
5. In the **Samsung device firmware rule** table, click +.
6. Select **Apply restriction to all Android devices** to allow Android OS updates to be applied to Samsung devices.
7. In the **Device model** field, enter the device model or select one from the drop-down list.
8. In the **Language** drop-down list, select a language.
9. In the **Carrier code** field, enter the CSC code for the wireless service provider for the device.
10. Click **Get firmware version**.
11. Repeat steps 5 to 8 for each firmware rule that you want to add.
12. When you are done, click **Add**.
13. In the **Samsung device firmware rules** table, click **Schedule** beside the firmware version you added.

14. In the **Schedule forced update** dialog box, do the following (**Note**: If you select the Schedule forced update option, the Knox device is no longer restricted to the firmware version and you can manually update it if a later version is available.):
    a) In the **Schedule forced update between** fields, select a date range when the update must be installed. The date range must be between 3 and 7 days. The default value is 7 days.
    b) In the **Schedule forced update during the hours of** drop-down lists, specify when the forced update must be installed and the time zone for the user. The time range must be between 1 and 12 hours.
15. Click **Save**.

After you finish: If necessary, rank profiles.

Add an E-FOTA license

You can use Enterprise Firmware Over the Air (E-FOTA) to control when firmware updates from Samsung are installed on Samsung Knox devices. Controlling firmware versions ensures that users' devices are using firmware versions that their apps support and comply with your organization's policies.

Before you can create a device SR requirements profile to control firmware versions, you must add an E-FOTA license in UEM.

Note: Samsung E-FOTA will reach end of service on July 31, 20022. For more information see the information from Samsung. For information about migrating to Samsung E-FOTA One, visit support.blackberry.com to read article 69901.

1. On the menu bar, click **Licensing** > **Licensing summary**.
2. In the **E-FOTA** section, click **Add license**.
3. In the **Add an E-FOTA license** dialog box, enter the name, client ID, client secret, customer ID, and license key.
4. Click **Save**.

View users who are running a revoked software release

You can view a list of users who are running a revoked software release. A revoked software release is a software release that is no longer accepted by a service provider but might still be installed on a user's device.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Compliance > Device SR requirements**.
3. Click the name of the profile that you want to view.
4. Click the **x users running revoked SR** tab to see the list of users who are running a revoked software release.

Managing OS updates on devices with MDM controls activations

You can't control when software releases are installed on devices with MDM controls activations; however, you can use compliance profiles to help manage devices that users have updated to an OS version that your organization doesn't allow. For example, Android 10 and later devices do not support MDM controls activations. If users with Android 9.x devices upgrade to Android 10, some device management features will no longer work, leaving the device in a compromised state. You can use device groups and compliance profiles to detect Android devices with the MDM controls activation type and set compliance rules to take appropriate action, such as notifying the user, untrusting the device, or unmanaging the device.

Follow these steps to manage OS updates on devices with MDM controls activations.

Step	Action
1	Create a device group that includes devices that conform to the following parameters: • MDM controls activation type • Device OS version that you want to restrict If a user upgrades a device to the specified OS it automatically becomes part of the device group.
2	Create a compliance profile and specify the device OS version as a restricted OS version.
3	In the compliance profile, specify the enforcement action that is appropriate for your organization. For example, you can notify the user that their activation type is not supported by the device OS and recommend reactivating the device with a different activation type, or you can deactivate the device.
4	Assign the compliance profile to the device group.
5	Optionally, create an event notification to inform administrators when a device is out of compliance with the compliance profile.

View available updates for iOS devices

You can see if a software update is available for your users' iOS devices so that you can have them upgrade the software to the latest version.

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. Select the device tab.
5. In the Activated device section, see if an update is available.

Update the OS on supervised iOS devices

You can force iOS devices to install an available OS update. To update the OS on multiple devices, see Send a bulk command.

You can also control the timing of iOS software updates using the "Delay software updates and "Software update delay period" IT policy rules. For more information, download the Policy Reference Spreadsheet.

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 left pane, if a software update is available, click **Update now**.
6. In the drop-down list, select one of the following options:

- **Download and install**: The update is automatically downloaded and installed on the device.
- **Download only**: The update is automatically downloaded on the device and the user is prompted to install it.
- **Install downloaded update**: If the update is already downloaded on a device, it is automatically installed.

7. In the **OS version** list, select the OS version that you want to update the device to
8. Click **Update**.

Configuring communication between devices and BlackBerry UEM

The Enterprise Management Agent profile ensures that devices contact BlackBerry UEM regularly for app or configuration updates. When there is an update for a device, BlackBerry UEM prompts the device to contact BlackBerry UEM to receive the updates. If for any reason the device doesn't receive the prompt, the Enterprise Management Agent profile is used to make sure that the device contacts BlackBerry UEM at intervals that you specify.

In on-premises environments, you can also use the Enterprise Management Agent profile to allow BlackBerry UEM to collect a list of personal apps on users' devices. To turn off the collection of personal apps, you must deselect the "Allow personal app collection" setting. For more information, see Turn off personal apps collection.

You can assign an Enterprise Management Agent profile to users, user groups, and device groups.

Create an Enterprise Management Agent profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > Enterprise Management Agent**.
3. Click +.
4. Type a name and description for the profile.
5. Set the values for each device type as required by your organization.
6. Click **Add**.

After you finish: If necessary, rank profiles.

iOS: Enterprise Management Agent profile settings

Setting	Description
Enterprise Management Agent poll rate	Specify how often, in seconds, the device polls for Enterprise Management Agent server commands. The device polls only when the UEM Client is open on the device. Possible values: • 900 to 86400 The default value is 3600.
Allow personal app collection	This setting specifies whether BlackBerry UEM receives a list of personal apps that are installed on users' devices. This setting is not supported on devices with user privacy activations.

Android: Enterprise Management Agent profile settings

Setting	Description
App changes	Specify how often, in seconds, the device checks for changes in installed apps. Possible values: • 3600 to 86400 seconds The default value is 3600.
Battery level threshold	Specify the percent battery level change (from 5 to 100) required before the device sends information back to BlackBerry UEM. Possible values: • 5 to 100 percent The default value is 20.
RAM free space threshold	Specify the required change in the amount of free memory in megabytes before the device sends information back to BlackBerry UEM. By default, the device does not send this information back to BlackBerry UEM.
Internal storage threshold	Specify the required change in the amount of internal free storage space in megabytes before the device sends information back to BlackBerry UEM. The default value is 250.
Memory card threshold	Specify the required change in the amount of external free space in megabytes before the device sends information back to BlackBerry UEM The default value is 500.
Enterprise Management Agent poll rate	Specify how often, in seconds, the device polls for Enterprise Management Agent server commands. Possible values: • Minimum: 900 The default value is 900.
Allow personal app collection	This setting specifies whether BlackBerry UEM receives a list of personal apps that are installed on users' devices. This setting is not supported on devices with user privacy activations.

Windows: Enterprise Management Agent profile settings

Setting	Description
Poll interval for device configuration updates	Specify, in minutes, how often the device polls for configuration updates when push notification is not available.

Setting	Description
Poll interval for the first set of retries	Specify, in minutes, the waiting time between attempts in the first set of retries if polling for device configuration updates fails.
Number of first retries	Specify the number of attempts in the first set of retries.
Poll interval for the second set of retries	Specify, in minutes, the waiting time between attempts in the second set of retries if polling for device configuration updates fails.
Number of second retries	Specify the number of attempts in the second set of retries.
Poll interval for the remaining scheduled retries	Specify, in minutes, the waiting time between subsequent attempts after the second set of retries if polling for device configuration updates fails.
Number of remaining scheduled retries	Specify the number of subsequent attempts after the second set of retries if polling for device configuration updates fails. If set to “0”, the device continues to poll until a connection is successful or the device is deactivated.
Poll on user login	Specify whether the device starts a management session on any user login.
All users poll on first login	Specify whether the device starts a management session on first user login for all users.
Allow personal app collection	This setting specifies whether BlackBerry UEM receives a list of personal apps that are installed on users' devices.

Displaying organization information on devices

You can configure BlackBerry UEM to display organization information and custom organization notices on devices.

For iOS, macOS, Android, and Windows 10 devices, you can create custom organization notices and have them display during activation. For example, a notice could include the conditions that a user must follow to comply with your organization's security requirements. The user must accept the notice to continue the activation process. You can create multiple notices to cover different requirements and you can create separate versions of each notice to support different languages.

You can create device profiles to display information about your organization on devices. For iOS and Android devices, organization information is displayed in the BlackBerry UEM Client on the device. For Windows 10, the phone number and email address are displayed in the support information on the device. For Samsung Knox devices, you can use the device profile to display the custom organization notice when the user restarts the device.

For Samsung Knox and supervised iOS devices, you can also use the device profile to add a custom wallpaper image to display information for your users. For example, you can create an image that has your support contact information, internal website information, or your organization's logo. On Samsung Knox devices, the wallpaper displays in the work space.

Note: Device profiles are not supported for iOS devices that are activated with a user privacy activation type.

Where organization information is displayed	How to configure the organization information
Display an organization notice on activation for iOS, macOS, Android, and Windows 10 devices	Create an organization notice and assign it to an activation profile.
Display an organization notice on restart for Samsung Knox devices	Create an organization notice and assign it in the Android tab of the device profile. To change the notice that displays on device restart, you must update the device profile.
Display organization information in the BlackBerry UEM Client on iOS and Android devices, or in the support information on Windows 10 devices	Type the information you want to display in the appropriate tab of the device profile.
In a wallpaper image on Samsung Knox or supervised iOS devices	Select an image file in the appropriate tab of the device profile.

Create organization notices

You can create custom organization notices to display during activation of iOS, macOS, Android, and Windows 10 devices.

Samsung Knox devices can also display the organization notice when a user restarts the device.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **General settings**.
3. Click **Organization notices**.

4. Click + at the right side of the screen.
5. In the **Name** field, type a name for the organization notice.
6. Optionally, you can reuse text from an existing organization notice by selecting it in the **Text copied from organization notice** drop-down list.
7. In the **Device language** drop-down list, select the language to use as the default language for the organization notice.
8. In the **Organization notice** field, type the text of the organization notice.
9. Optionally, you can click **Add an additional language** multiple times to post the organization notice in more languages.
10. If you post the organization notice in more than one language, select the **Default language** option below one of the messages to make it the default language.
11. Click **Save**.

After you finish:

- To display the organization notice during activation, assign the organization notice to an activation profile.
- To display the organization notice when a Samsung Knox device restarts, assign the organization notice to a device profile.

Create a device profile

Before you begin: For Samsung Knox devices, create organization notices.

Note: Device profiles are not supported for iOS devices that are activated with a user privacy activation type.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Custom > Device**.
3. Click +.
4. Type a name and description for the profile. Each device profile must have a unique name.
5. Perform one of the following tasks:

Task	Steps
Assign an organization notice to display on Samsung Knox devices during device restart	a. Click **BlackBerry** or **Android**. b. In the **Assign organization notice** drop-down list, select the organization notice that you want to display on devices.
For iOS and Android devices, define the organization information to display in the BlackBerry UEM Client app. For Windows 10, define the phone number and email address to display in the support information on devices.	a. Click **iOS**, **Android**, or **Windows**. b. Type the name, address, phone number, and email address for your organization.

6. If necessary, perform the following tasks:

Task	Steps
Add a wallpaper image to the work space on Samsung Knox devices	**a.** Click **BlackBerry** or **Android**. **b.** In the **Work space wallpaper** section, click **Browse.** **c.** Select the image that you want to use for the wallpaper. **d.** Click **Open**.
Add a wallpaper image to supervised iOS devices	**a.** Click **iOS**. **b.** In the **Device wallpaper** section, select whether the wall paper displays on the **Home screen**, **Lock screen**, or **Both**. **c.** Click **Browse** and select the image that you want to use for the wallpaper. **d.** Click **Open**. **e.** In the **Set wallpaper for** field, select where you want the wallpaper to display.

7. Click **Add**.

After you finish:

- If necessary, rank profiles.

Using location services on devices

You can use a location service profile to request the location of devices and view their approximate locations on a map. You can also allow users to locate their devices using BlackBerry UEM Self-Service. If you enable location history for iOS and Android devices, the devices must report location information periodically and administrators can view the location history.

Location service profiles use the location services on iOS, Android, and Windows 10 Mobile devices. Depending on the device and available services, location services may use information from GPS, cellular, and Wi-Fi networks to determine the location of the device.

Configure location service settings

You can configure the settings for location service profiles, such as the unit of speed that is displayed for a device when you view its location on a map. If you enable location history for iOS and Android devices, BlackBerry UEM stores the location history for 1 month by default.

1. On the menu bar, click **Settings > General settings > Location service**.
2. If you have an on-premises environment, in the **Location history age** field, specify the number of days, weeks, or months that BlackBerry UEM stores the location history for devices.
3. In the **Displayed unit of speed** drop-down list, click **km/h** or **mph**.
4. Click **Save**.

Create a location service profile

You can assign a location service profile to user accounts, user groups, or device groups. Users must accept the profile before the management console or BlackBerry UEM Self-Service can display iOS and Android device locations on a map. Windows 10 Mobile devices automatically accept the profile.

Before you begin: Configure location service settings

1. On the menu bar, click **Policies and profiles**.
2. Click **Protection > Location service**.
3. Click +.
4. Type a name and description for the location service profile.
5. Optionally, clear the check box for any device type that you do not want to configure the profile for.
6. Perform any of the following tasks:

Task	Steps
Enable location history for iOS devices	**a.** On the **iOS** tab, verify that the **Log device location history** check box is selected. **Note:** BlackBerry UEM collects a device's location hourly and, if possible, when there has been a significant change in the device's location (for example, 500 meters or more).

Task	Steps
Enable location history for Android devices	**a.** On the **Android** tab, verify that the **Log device location history** check box is selected. **b.** In the **Device location check distance** field, specify the minimum distance that a device must travel before the device location is updated. **c.** In the **Location update frequency** field, specify how often the device location is updated. **Note:** Both the distance and frequency conditions must be met before the device location is updated.

7. Click **Add**.

After you finish: If necessary, rank profiles.

Locate a device

You can locate iOS, Android, and Windows 10 Mobile devices (for example, if a device is lost or stolen). Users must accept the location service profile before the management console can display iOS and Android device locations on a map. Windows 10 Mobile devices automatically accept the profile. Location history is available for iOS and Android devices if you enabled it in the profile.

Before you begin: Create and assign a location service profile.

1. On the menu bar, click **Users > Managed devices**.
2. Select the check box for each device that you want to locate.
3. Click  .
4. Find the devices on the map using the following icons. If an iOS or Android device does not respond with the latest location information and location history is enabled in the profile, the map displays the last known location of the device.
   - Current location: 
   - Last known location: 

   You can click or hover over an icon to display location information, such as latitude and longitude and when the location was reported (for example, 1 minute ago or 2 hours ago).
5. To view the location history for an iOS or Android device, perform the following actions:
   a) Click **View location history**.
   b) Select a date and time range.
   c) Click **Submit**.

Using Lost Mode for supervised iOS devices

You can enable and manage Lost Mode for supervised iOS devices. When a device is lost, enabling Lost Mode allows you to:

- Lock the device and set the message you want to display (for example, you can display contact information for when the device is found).

- View the current location of the device without using a Location service profile.
- Track all devices that are in Lost Mode from the management console.

Turn on Lost Mode

Lost Mode is supported on supervised iOS devices.

1. On the menu bar, click **Users > Managed devices**.
2. Click on a device that you want to turn on Lost Mode for.
3. In the device tab, click **Turn on Lost Mode**.
4. In the **Contact phone number** and **Message** fields, enter the appropriate information.
5. Optionally, select **Replace slide to unlock text** and enter the text to display.
6. Click **Enable**.

Locate a device in Lost Mode

Before you begin: Turn on Lost Mode

1. On the menu bar, click **Users > Managed devices**.
2. Click on a device that has Lost Mode turned on.
3. In the device tab, click **Get device location**.

Turn off Lost Mode

Before you begin: Turn on Lost Mode

1. On the menu bar, click **Users > Managed devices**.
2. Click on a device that has Lost Mode turned on.
3. In the device tab, click **Turn off Lost Mode**.

Using Activation Lock on iOS devices

The Activation Lock feature on iOS devices allows users to protect their devices if they are lost or stolen. When the feature is enabled, the user must confirm the Apple ID and password to disable Find My iPhone, erase 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.

When a device is activated on BlackBerry UEM, Activation Lock is disabled by default. You can enable it for each device individually, or you can enforce it using the IT policy. When you enable Activation Lock, BlackBerry UEM stores a bypass code that you can use to clear the lock so that the device can be erased and reactivated without the user's Apple ID and password.

Enable Activation Lock

Complete the following steps to enable Activation Lock for each device individually. If Activation Lock is enforced using the IT policy rule, it is already enabled.

Note: When enabling the Activation Lock feature, a short delay may occur between BlackBerry UEM and Apple.

Before you begin:

- 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.

1. On the menu bar, click **Users**.
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, click **Enable Activation Lock**.

After you finish: To view the list of bypass codes for devices, see View the Activation Lock bypass code

Disable Activation Lock

Complete the following steps to disable Activation Lock for each device individually. If Activation Lock is enforced using an IT policy rule, you cannot disable it.

Note: When you enable the Activation Lock feature, a short delay may occur between BlackBerry UEM and Apple.

1. On the menu bar, click **Users**.
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 **Disable Activation Lock**.

View the Activation Lock bypass code

You can view the Activation Lock bypass code and the date that the bypass code was generated.

1. On the menu bar, click **Users > Apple Activation Lock**.
2. Search for a device.
3. In the search results, click the device.
4. If necessary, scroll to the right of the main screen to view the bypass code.

Managing iOS features using custom payload profiles

You can use custom payload profiles to control features on iOS devices that aren't controlled by existing BlackBerry UEM policies or profiles.

Note: If a feature is controlled by an existing BlackBerry UEM policy or profile, a custom payload profile may not work as expected. You should use existing policies or profiles whenever possible.

You can create Apple configuration profiles using the Apple Configurator and add them to BlackBerry UEM custom payload profiles. You can assign custom payload profiles to users, user groups, and device groups.

- Control an existing iOS feature that isn't included in the BlackBerry UEM policies and profiles. For example, with BES10, your CEO's assistant was able to access both her own email account and the CEO's on an iPhone. In BlackBerry UEM, you can assign only one email profile to a device, so the assistant can only access his own email account. To solve this, you can assign an email profile to let the assistant's iPhone access the assistant's email account and a custom payload profile that lets the assistant's iPhone access your CEO's email account.
- Control a new iOS feature that was released after the latest BlackBerry UEM software release. For example, you want to control a new feature that will be available to devices when they upgrade to a recent iOS update, but BlackBerry UEM won't have an IT policy rule for the new feature until the next BlackBerry UEM software release. To solve this, you can create a custom payload profile that controls that feature until the next BlackBerry UEM software release.

Create a custom payload profile

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

1. In the Apple Configurator, create an Apple configuration profile.
2. In the BlackBerry UEM management console, click **Policies and Profiles**.
3. Click **Custom > Custom payload**.
4. Click +.
5. Type a name and description for the profile.
6. In the Apple Configurator, copy the XML code for the Apple configuration profile. When you copy the text, copy only the elements in bold text as shown in the following code sample.

```
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
    "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
    <plist version="1.0">
    <dict>
         <key>PayloadContent</key>
         <array>
               <dict>
                    <key>CalDAVAccountDescription</key>
                    <string>CalDAV Account Description</string>
                    <key>CalDAVHostName</key>
                    <string>caldav.server.example</string>
                    <key>CalDAVPort</key>
                    <integer>8443</integer>
                    <key>CalDAVPrincipalURL</key>
                    <string>Principal URL for the CalDAV account</string>
                    <key>CalDAVUseSSL</key>
                    </true>
                    <key>CalDAVUsername</key>
```

```
                    <string>Username</string>
                    <key>PayloadDescription</key>
                    <string>Configures CalDAV account.</string>
                    <key>PayloadDisplayName</key>
                    <string>CalDAV (CalDAV Account Description)</string>
                    <key>PayloadIdentifier</key>
                    <string>.caldav1</string>
                    <key>PayloadOrganization</key>
                    <string></string>
                    <key>PayloadType</key>
                    <string>com.apple.caldav.account</string>
                    <key>PayloadUUID</key>
                    <string>9ADCF5D6-397C-4E14-848D-FA04643610A3</string>
                    <key>PayloadVersion</key>
                    <integer>1</integer>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string>Profile description.</string>
        <key>PayloadDisplayName</key>
        <string>Profile Name</string>
        <key>PayloadOrganization</key>
        <string></string>
        <key>PayloadRemovalDisallowed</key>
        <false/>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>7A5F8391-5A98-46EA-A3CF-C0D6EDC74632</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
    </plist>
```

7. In the **Custom payload** field, paste the XML code from the Apple Configurator.
8. Click **Add**.

Managing factory reset protection for Android Enterprise devices

You can use the factory reset protection profile to control the factory reset protection feature for your organization's Android Enterprise devices that have been activated using the Work space only and Work and personal - full control activation types.

Factory reset protection requires an Android device user to enter their Google account credentials to unlock a device that has been reset to factory settings. It is enabled by default when a user adds a Google account to the device. This profile allows you to disable factory reset protection or specify a user account that can be used to unlock a device after it has been reset to factory settings.

This profile provides three options:

- You can disable factory reset protection. If you disable factory reset protection, anyone can reset a lost or stolen device to factory settings and begin using the device. This option is useful if a known user has forgotten their Google account credentials or if you need to reset a device owned by your organization that has been returned to you.
- Users can use Google account credentials that are already associated with the device after a factory reset. This is the default behavior. If a device is reset to factory settings, the user must log into the device using Google account credentials that are already on the device. This prevents someone with a lost or stolen device from resetting and using it themselves.
- You can specify Google account credentials that a user can use to log into the device after it has been reset to factory settings.This option allows your organization to control who can log into a device after it is reset to factory settings. BlackBerry recommends that you only use this option if you fully understand the device user experience.

Create a Factory reset protection profile

1. On the menu bar, click **Policies and Profiles > Managed devices > Protection > Factory reset protection**.
2. Type a name and description for the profile.
3. Choose a **Factory reset protection setting**. Select one of the following options:
   - **Disable factory reset protection**: If you disable factory reset protection, users are not prompted to enter a Google user ID after the device is reset to factory settings.
   - **Enable and use previous Google account credentials when the device is reset to factory settings**: This is the default option. If the user resets the device to factory settings using an untrusted method and a Google account existed on the device before it was reset, the account must be verified after the device is reset to factory settings. Note that if your organization uses a managed Google account structure, a Google account will not exist on the device and factory reset protection will not be available on the device.
   - **Enable and specify Google account credentials when the device is reset to factory settings**: Select this option to specify the Google account that must be used to log into the device after an untrusted factory reset. If you select this option, the user's personal Google account credentials can't be used after a factory reset.
4. If you selected **Enable and specify Google account credentials when the device is reset to factory settings**, click **+** > **Add using Google authentication**, and then sign into the Google account that you want to use to log into devices that have been reset.

   You can add up to 20 accounts. You can also specify the account manually. For more information, see Manually obtain a user ID for a Google account.

5. If you selected **Enable and specify Google account credentials when the device is reset to factory settings** and your organization has a G Suite or Google Cloud domain, select **Add a Google account created by BlackBerry UEM** if you want to include the user's work Google account in the list of accounts that can unlock the device after a factory reset.
6. Click **Save**.

Manually obtain a user ID for a Google account

You can use an existing Google account or create one specifically for use with factory reset protection. If you choose to add an account manually rather than using Google authentication, you must obtain the user ID for the account.

1. Go to the Google developers People API site (https://developers.google.com/people/api/rest/v1/people/get).
2. In the **resourceName** field type: people/me
3. In the **personalFields** field type: metadata
4. Click **Execute**.
5. On the **Choose an account** screen, select an account to use to set up the factory reset protection profile.
6. On the **Google APIs Explorer wants to access your Google Account** screen, click **Allow**.
7. On the right-hand side of the People ID page, the 21-digit user ID displays in the "id" field. Note that the ID displays under the green header with the number 200 in it.

How factory reset protection responds to device resets

There are several ways that a device can be reset to the default factory settings. Depending on which way that the device is reset, factory reset protection responds differently. For more information about trusted and untrusted resets, visit support.blackberry.com/community to read KB56972.

- Deactivation of the BlackBerry UEM Client is not considered a trusted reset because the device user is not verified before the device is deactivated. Therefore factory reset protection is triggered when the device resets and the deactivation has completed.
- Sending the "Delete all device data" command from the management console can be either a trusted or untrusted reset. If you select the "Remove factory reset protection" option when you send the command, factory reset protection is not triggered when the device resets.
- Resetting the device from device settings requires the user to authenticate themselves before the reset. This is considered a trusted reset and factory reset protection is not triggered.
- Device bootloader/recovery or debugging tools (ADB) can be used to reset the device to factory settings and are considered untrusted because the user identity is not validated before the factory reset occurs. Therefore factory reset protection is triggered when the device resets.

Considerations for using a specific Managed Google Play account when setting up a factory reset protection profile

If your organization uses a Managed Google Play account, you might want to consider using the "Enable and specify Google account credentials when the device is reset to factory settings" option in the factory reset protection profile because a Google account does not exist on your organization's devices that you use to reset the device and therefore factory reset protection is not available on the device.

If you decide to use the "Enable and specify Google account credentials when the device is reset to factory settings" option, there are several factors for you to consider:

- Ensure that the 21-digit user ID that you enter in the profile is correct. If this number does not match your organization's Google account that you want to use, there is no way to clear factory reset protection on the device after it has been triggered. For more information, see Manually obtain a user ID for a Google account.
- In the IT policy for your organizations's users who you assign the factory reset protection profile to, BlackBerry recommends that you clear the "Allow factory reset" option. Clearing the option disables the factory reset option in the device settings and disables the deactivate button in the BlackBerry UEM Client.This ensures that users do not use the untrusted deactivation option in the UEM Client which always triggers Factory Reset Protection on the device. When this option is enabled, users must contact their organization's BlackBerry UEM administrator to have their device reset.
- Provide information to your organization's users about the factory reset protection experience on the device and the procedure they should use to clear factory reset protection when it is triggered on the device. For more information, see Clear factory reset protection from a device. The BlackBerry UEM administrator must choose if they want to provide the account details to users to clear factory reset protection or if the users will need to have local support personnel unlock the device.

Clear factory reset protection from a device

When factory reset protection is triggered on the device, enterprise activation on BlackBerry UEM will no longer work. You must first clear factory reset protection using the Android out of box experience.

1. If you are using any form of automated activation system (such as zero-touch enrollment or Samsung Knox Mobile Enrollment), you must disable it so that the device can go through the out of box experience.
2. Once the device has connectivity, on the first Android account screen, the user is prompted to enter the Google account credentials that are associated with the device. If you have set up a specific Google account in the factory reset protection profile, the user must enter the email address and the password that is associated with the account.
3. Once the user has entered the Google account email address and password, they will be asked if they want to add this user to the device. The user must select the option to use a new user for the device.
    - On non-Samsung devices that are not using zero-touch enrollment: Users can enter 'afw#blackberry' or the enterprise Google account details to install the BlackBerry UEM Client, and re-activate the device against BlackBerry UEM.
    - On Samsung devices that are not using zero-touch enrollment or Samsung Knox Mobile Enrollment: Complete the out of box experience, and use the device settings to reset the device. When the device restarts, it will be able to re-activate with the enterprise.
    - Devices using zero-touch enrollment or Samsung Knox Mobile Enrollment: If you are using any form of automated activation system (such as zero-touch enrollment or Samsung Knox Mobile Enrollment) you can re-enable it for the device, complete the out of box experience and use the device settings to reset the device. The device should now restart and use the automated activation system you have configured.

Setting up Windows Information Protection for Windows 10 devices

You can set up Windows Information Protection (WIP) for Windows 10 devices when you want to:

- Separate personal and work data on devices and be able to wipe only work data
- Prevent users from sharing work data outside of protected work apps or with people outside of your organization
- Protect data even if it is moved to or shared on other devices, such as a USB key
- Audit user behavior and take appropriate actions to prevent data leaks

When you set up WIP for devices, you specify the apps that you want to protect with WIP. Protected apps are trusted to create and access work files, while unprotected apps can be blocked from accessing work files. You can choose the level of protection for protected apps based on how you want users to behave when they share work data. When WIP is enabled, all data sharing practices are audited. For more information about WIP, visit https://technet.microsoft.com/itpro/windows/keep-secure/protect-enterprise-data-using-wip.

The apps that you specify can be enlightened or unenlightened for enterprise. Enlightened apps can create and access work and personal data. Unenlightened apps can only create and access work data. For more information about enlightened and unenlightened apps, visit https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/enlightened-microsoft-apps-and-wip.

Create a Windows Information Protection profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Protection > Windows Information Protection**.
3. Click +.
4. Type a name and description for the profile.
5. Configure the appropriate values for each profile setting. For details about each profile setting, see Windows 10: Windows Information Protection profile settings.
6. Click **Add**.

Windows 10: Windows Information Protection profile settings

Windows 10: Windows Information Protection profile setting	Description
Windows Information Protection settings	This setting specifies whether Windows Information Protection is enabled and the level of enforcement. When this setting is set to "Off," data is not encrypted and audit logging is turned off. When this setting is set to "Silent," data is encrypted and any attempts to share protected data are logged. When this setting is set to "Override," data is encrypted, the user is prompted when they attempt to share protected data, and any attempts to share protected data are logged. When this setting is set to "Block," data is encrypted, users cannot share protected data, and any attempts to share protected data are logged. Possible values: • Off • Silent • Override • Block The default value is "Off."
Enterprise protected domain names	This setting specifies the work network domain names that your organization uses for its user identities. You can separate multiple domains with pipes (|). The first domain is used as a string to tag files that are protected by apps that use WIP. For example, `example.com|example.net`.
Data recovery certificate file (.der, .cer)	This setting specifies the data recovery certificate file. The file that you specify must be a PEM encoded or DER encoded certificate with a .der or .cer file extension. You use the data recovery certificate file to recover files that were locally protected on a device. For example, if your organization wants to recover data protected by WIP from a device. For information on creating a data recovery certificate, see the Microsoft Windows Information Protection documentation.
Remove the Windows Information Protection settings when a device is removed from BlackBerry UEM	This setting specifies whether to revoke WIP settings when a device is deactivated. When WIP settings are revoked, the user can no longer access protected files.
Show Windows Information Protection overlays on protected files and apps that can create enterprise content	This setting specifies whether an overlay icon is shown on file and app icons to indicate whether a file or app is protected by WIP.

Windows 10: Windows Information Protection profile setting	Description
Work network IP range	This setting specifies the range of IP addresses at work to which an app protected with WIP can share data. Use a dash to denote a range of addresses. Use a comma to separate addresses.
Work network IP ranges are authoritative	This setting specifies if only the work network IP ranges are accepted as part of the work network. When this setting is enabled, no attempts are made to discover other work networks. By default, the option is not selected.
Enterprise internal proxy servers	This setting specifies the internal proxy servers that are used when connecting to work network locations. These proxy servers are only used when connecting to the domain listed in the Enterprise cloud resources setting.
Enterprise cloud resources	This setting specifies the list of enterprise resource domains hosted in the cloud that need to be protected. Data from these resources are considered enterprise data and protected.
Cloud resources domain	This setting specifies the domain name.
Paired proxy	This setting specifies a proxy that is paired with a cloud resource. Traffic to the cloud resource will be routed through the enterprise network via the denoted proxy server (on port 80). A proxy server used for this purpose must also be configured in the Enterprise internal proxy servers field.
Enterprise proxy servers	This setting specifies the list of internet proxy servers.
Enterprise proxy servers are authoritative	This setting specifies whether the client should accept the configured list of proxies and not try to detect other enterprise proxies.
Neutral resources	This setting specifies the domains that can be used for work or personal resources.
Enterprise network domain names	This setting specifies a comma-separated list of domains that comprise the boundaries of the enterprise. Data from one of these domains that is sent to a device will be considered enterprise data and protected. These locations will be considered a safe destination for enterprise data to be shared to. For example, `example.com,example.net`.

Windows 10: Windows Information Protection profile setting	Description

Desktop app payload code	Specify the desktop app keys and values used to configure application launch restrictions on Windows 10 devices. You must use the keys defined by Microsoft for the payload type that you want to configure.
	
	To specify the apps, copy the XML code from the AppLocker policy .xml file and paste it in this field. When you copy the text, copy only the elements as shown in the following code sample:
	
	`<RuleCollection Type="Appx" EnforcementMode="Enabled">`
	`  <FilePublisherRule Id="0c9781aa-bf9f-4352-`
	`b4ba-64c25f36f558"`
	`  Name="WordMobile" Description="`
	` UserOrGroupSid="S-1-1-0" Action="Allow">`
	`  <Conditions>`
	`  <FilePublisherCondition`
	`  PublisherName="CN=Microsoft Corporation, O=Microsoft`
	` Corporation, L=Redmond, S=Washington, C=US"`
	`  ProductName="Microsoft.Office.Word" BinaryName="*">`
	`  <BinaryVersionRange LowSection="*"`
	` HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`</RuleCollection>`
	
	For more information about using AppLocker, see the Microsoft AppLocker documentation.

Windows 10: Windows Information Protection profile setting	Description

Universal Windows Platform app payload code	Specify the Universal Windows Platform app keys and values used to configure WIP on Windows 10 devices. You must use the keys defined by Microsoft for the payload type that you want to configure.
	
	To specify the apps, copy the XML code from the AppLocker policy .xml file and paste it in this field. When you copy the text, copy only the elements as shown in the following code sample:
	
	`<RuleCollection Type="Exe" EnforcementMode="Enabled">`
	`  <FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20"`
	`  Name="(Default Rule)`
	`  All files" Description="" UserOrGroupSid="S-1-1-0"`
	`  Action="Allow">`
	`  <Conditions>`
	`  <FilePathCondition Path="*" />`
	`  </Conditions>`
	`  </FilePathRule>`
	`  <FilePublisherRule Id="ddd0bc90-`
	`dada-4002-9e2f-0fc68e1f6af0" Name="WORDPAD.EXE,`
	`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`  C=US" Description=""`
	`  UserOrGroupSid="S-1-1-0" Action="Deny">`
	`  <Conditions>`
	`  <FilePublisherCondition PublisherName="O=MICROSOFT`
	`  CORPORATION`
	`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`  BinaryName="WORDPAD.EXE">`
	`  <BinaryVersionRange LowSection="*"`
	`  HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`  <FilePublisherRule Id="c8360d06-f651-4883-`
	`abdd-9c3a95a415ff" Name="NOTEPAD.EXE,`
	`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`  C=US" Description=""`
	`  UserOrGroupSid="S-1-1-0" Action="Allow">`
	`  <Conditions>`
	`  <FilePublisherCondition PublisherName="O=MICROSOFT`
	`  CORPORATION,`
	`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`  BinaryName="NOTEPAD.EXE">`
	`  <BinaryVersionRange LowSection="*"`
	`  HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`</RuleCollection>`
	
	For more information about using AppLocker, see the Microsoft AppLocker documentation.

Windows 10: Windows Information Protection profile setting	Description
Associated VPN profile	This setting specifies the VPN profile that a device uses to connect to a VPN when using an app protected by WIP. This setting is valid only if "Use a VPN profile" is selected for the "Secure connection used with WIP."
Collect device audit logs	This setting specifies whether to collect device audit logs.

Allowing BitLocker encryption on Windows 10 devices

BitLocker Drive Encryption is a data protection feature of the operating system that helps mitigate unauthorized data access when a device is lost or stolen. You can allow BitLocker encryption on Windows 10 devices and protection is strengthened if the device also has a Trusted Platform Module (TPM), which gives you the option to require additional authentication at startup (for example, a startup key, PIN, or removable USB drive). In BlackBerry UEM, you can also create a compliance profile to prevent users from disabling BitLocker to enforce its use on devices that require encryption.

You can configure the recovery options to access a BitLocker-protected operating system or data drives. Users can access recovery keys from the Active Directory console, and if enabled, recovery passwords can be backed up to Active Directory Domain Services so that an administrator can recover them using the BitLocker Recovery Password Viewer tool.

Configure the following UEM IT policy rules to support BitLocker encryption on Windows 10 devices:

- BitLocker encryption method for desktop
- Allow storage card encryption prompts on the device
- Allow BitLocker Device Encryption to enable encryption on the device
- Set default encryption methods for each drive type
- Require additional authentication at startup
- Require minimum PIN length for startup
- Pre-boot recovery message and URL
- BitLocker OS drive recovery options
- BitLocker fixed drive recovery options
- Require BitLocker protection for fixed data drives
- Require BitLocker protection for removable data drives
- Allow recovery key location prompt
- Enable encryption for standard users

For more information about the BitLocker IT policy rules, see the Policy Reference Spreadsheet.

Managing attestation for devices

When you turn on attestation, BlackBerry UEM sends challenges to test the authenticity and integrity of devices. You can turn on attestation for the following devices:

- Samsung Knox devices
- Android devices
- Windows 10 devices

Manage attestation for Samsung Knox devices

When you turn on attestation, BlackBerry UEM sends challenges to test the authenticity and integrity of Samsung Knox devices activated with the following activation types:

- Work and personal - full control (Samsung Knox)
- Work space only (Samsung Knox)
- Work and personal - user privacy (Samsung Knox)

1. On the menu bar, click **Settings > General settings > Attestation**.
2. To turn on attestation for Samsung Knox devices, select **Enable periodic attestation challenges for KNOX Workspace devices**.
3. In the **Challenge frequency** section, specify, in days or hours, how often the device must return an attestation response to BlackBerry UEM.
4. In the **Grace period** section, specify a grace period. After the grace period expires with no successful attestation response, a device is considered non-compliant and the device is subject to the conditions specified in the compliance profile that is assigned to the user. Note that if a user's device is out of coverage, turned off, or has a dead battery, it cannot respond to the attestation challenges that BlackBerry UEM sends and BlackBerry UEM will consider the device to be non-compliant. If you have your organization's compliance policy set to wipe the device when it is out of compliance, when the device does not respond before the grace period expires, data on the device will be deleted.
5. Click **Save**.

After you finish: Create a compliance profile that specifies the actions that occur when a device is considered rooted. For instructions, see Enforcing compliance rules for devices

Manage attestation for Android devices and BlackBerry Dynamics apps using SafetyNet

When you use Android SafetyNet attestation, BlackBerry UEM sends challenges to test the authenticity and integrity of Android devices and BlackBerry Dynamics apps in your organization's environment. SafetyNet helps you assess the security and compatibility of the environments in which your organization's apps run. You can use SafetyNet attestation in addition to BlackBerry's existing root and exploitation detection. For more information about SafetyNet, see the information from Google.

BlackBerry UEM performs SafetyNet attestation in the following circumstances:

- After device activation when the BlackBerry UEM Client is installed
- During device activation when the BlackBerry UEM Client is installed
- During BlackBerry Dynamics apps activation
- After app activation for BlackBerry Dynamics apps

- On demand using REST APIs
- At device restart if the BlackBerry UEM Client is activated

Considerations for configuring SafetyNet attestation

- The Google SafetyNet attestation failure option is a compliance profile setting for Android devices and BlackBerry Dynamics apps that allows you to specify the actions that occur if devices or apps do not pass SafetyNet attestation. To set this option, navigate to **Policies and profiles > Compliance > Android** tab.
- If you do not enable the 'Google SafetyNet attestation failure' compliance rule, apps that are already activated will not have compliance actions enforced on them.
- When you enable SafetyNet, attestation during activation is performed; you cannot use a policy to enforce attestation during activation.
- The BlackBerry UEM Client is not required for you to enable SafetyNet attestation.
- The BlackBerry UEM Client does not appear in the list of BlackBerry Dynamics apps that you can configure for SafetyNet attestation. BlackBerry UEM sends attestation challenges to, and receives responses from, the BlackBerry UEM Client.
- BlackBerry UEM sends attestation challenges to each BlackBerry Dynamics app that you configure.
- BlackBerry UEM does not trust old versions of apps. For example, if you want to enable attestation challenges for BlackBerry Work, you must ensure that the version of BlackBerry Work on your organization's devices is the latest version or new activations will fail. Note that until you enable the "Google SafetyNet Attestation failure" option in your organization's compliance profile, even if your existing activated users are using older versions of apps, no adverse action will be taken on apps or devices.
- In addition to activation and periodic attestation, BlackBerry UEM uses new REST APIs that allow you to create custom server workflows. For example, if an app needs to access a specific secure remote item, before granting access, the app server communicates with BlackBerry UEM to enforce SafetyNet attestation on the app or device.
- If a user's device is out of coverage, turned off, or has a dead battery, it cannot respond to the attestation challenges that BlackBerry UEM sends and BlackBerry UEM will consider the device to be non-compliant. If you have your organization's compliance policy set to wipe the device when it is out of compliance, if the device does not respond before the grace period expires, data on the device will be deleted when it connects to a wireless network.
- If you set a time in App grace period field, only apps that do not respond within the time frame that you set will have an action taken on them. For example, if you set the App grace period value to 7 days, and your users use BlackBerry Work every day, but do not use BlackBerry Tasks within the 7 days, only BlackBerry Tasks will have an action taken on it.
- If you add a new app to BlackBerry UEM and it fails attestation during activation, the app is not activated no matter which option you have configured in the 'Google SafetyNet attestation failure' section of your organization's compliance profile. If an app has already been activated, it is subject to the rules that you specified in the compliance profile.
- Your organization's users must have the latest version of Google Play services installed.
- If a device fails attestation, there is no indication of the failure in the OS compromised column on the Managed devices page.
- For information about developing BlackBerry Dynamics apps for Android devices, see the Developer content.

Configure attestation for Android devices and BlackBerry Dynamics apps using SafetyNet

1. On the menu bar, click **Settings > General settings > Attestation**.
2. To turn on attestation for Android devices, select **Enable periodic attestation challenges using SafetyNet**.
3. Select **Enable CTS profile matching** if you want to turn on Google's Compatibility Test Suite. For more information about CTS, see the information from Google.
4. In the **Challenge frequency** section, specify, in days or hours, how often the device must return an attestation response to BlackBerry UEM. Considerations for configuring the challenge frequency:

- While you can configure how often BlackBerry UEM tests the authenticity and integrity of the device, attestation during activation of the app is mandatory.
- If you have deployed the BlackBerry UEM Client, it is added as one of the apps that BlackBerry UEM tests for SafetyNet attestation automatically.
- The BlackBerry UEM Client uses a different communication channel to BlackBerry UEM than other BlackBerry Dynamics apps, which must be running and authorized to connect to BlackBerry UEM to receive policy updates. BlackBerry UEM can proactively communicate with the BlackBerry UEM Client and start the app if it is not running. If you set a challenge frequency of 3 hours, then BlackBerry UEM communicates with the BlackBerry UEM Client every 3 hours and the attestation check is performed. However, BlackBerry Dynamics app commands are stored until the app connects to BlackBerry UEM , and only the latest attestation command is stored. So, if the app is not used for 24 hours, when the user starts it, only one attestation challenge is performed.

5. In the **Grace period** section, specify a grace period. After the grace period expires with no successful attestation response, a device is considered non-compliant and the device is subject to the conditions specified in the compliance profile that is assigned to the user. Also, if a user's device is out of coverage, turned off, or has a dead battery, it cannot respond to the attestation challenges that BlackBerry UEM sends, and BlackBerry UEM will consider the device to be non-compliant. If you have your organization's compliance policy set to wipe the device when it is out of compliance, if the device does not respond before the grace period expires, data on the device will be deleted when it connects to a wireless network.
6. In the **App grace period** section, specify a grace period. After the grace period expires, the BlackBerry Dynamics apps are subject to the conditions specified in the compliance profile that is assigned to the user. The grace period is enforced on a per-app basis. Note that if you have deployed only the BlackBerry UEM Client to the device, then the grace period is ignored. Also, the BlackBerry UEM Client does not appear in the list of BlackBerry Dynamics apps. When you add BlackBerry Dynamics apps to the list of apps that will be subject to attestation challenges, the following rules apply:
   - Only apps in this list are sent attestation challenges.
   - Only apps in this list are evaluated for the app grace period check.
   - Only apps in this list are subject to attestation during app activation.

   Note: Only BlackBerry Dynamics apps that have been developed specifically for SafetyNet will display in the list. For more information, see the Developer content.
7. To add an app that will be subject to attestation challenges, click +.
8. Do one of the following:
   - Click the name of an app that is already on the list.
   - Search for and click on the name of the app.
9. Click **Select**.
10. Click **Save**.

Manage attestation for Windows 10 devices

When you turn on attestation, BlackBerry UEM sends challenges to test the authenticity and integrity of Windows 10 devices. The device communicates with the Microsoft Health Attestation Service to check for compliance based on settings that you set in your organization’s compliance profile.

Note: The Windows 10 attestation settings do not apply to BlackBerry Desktop (BlackBerry Access + BlackBerry Work).

1. On the menu bar, click **Settings > General settings > Attestation**.
2. To turn on attestation for Windows 10 devices, select **Enable periodic attestation challenges for Windows 10 devices**.

3. In the **Challenge frequency** section, specify, in days or hours, how often the device must return an attestation response to BlackBerry UEM.
4. In the **Grace period** section, specify a grace period. After the grace period expires with no successful attestation response, a device is considered non-compliant and the device is subject to the conditions specified in the compliance profile that is assigned to the user. Also to consider, if a user's device is out of coverage, turned off, or has a dead battery, it cannot respond to the attestation challenges that BlackBerry UEM sends and BlackBerry UEM will consider the device to be non-compliant. If you have your organization's compliance policy set to wipe the device when it is out of compliance, when the device does not respond before the grace period expires, data on the device will be deleted.
5. Click **Save**.

You can view any compliance violations on the device details page.

After you finish: Create a compliance profile that specifies the actions that occur when a device is considered rooted. For instructions, see Enforcing compliance rules for devices

Migrate iOS devices to use a hardened channel

Perform these steps to export a list of devices that are not already using a hardened channel. During migration, devices will be reactivated, and users may be impacted, such as with the reinstallation of work apps and profiles. For more information, visit support.blackberry.com to read KB99869.

Note: For devices enrolled with DEP, the DEP enrollment configuration is not migrated and the devices will lose the enrollment configuration settings in the destination environment. Users must factory rest the devices and then reactivate the BlackBerry UEM Client after migration. For more information, visit support.blackberry.com to read KB 100525.

1. In the management console, on the menu bar, click **Settings > Migration > iOS Hardened Channel**.
2. Click **Export**. A list of devices that are not already using a hardened channel is downloaded. Note that devices that are in shared device groups are included in the export for information purposes only. These devices will be skipped during import and users must factory reset the device and then reactivate the BlackBerry UEM Client.
3. Click **Browse** and navigate to the file that contains the devices that you want to migrate. Note that if the list that you downloaded in step 2 contains more than 1000 entries, you must divide the entries in the files that you upload so that they contain 1000 entries at most and upload multiple files.

Migrate a single iOS device to use a hardened channel

You can migrate individual devices to use a hardened channel.

1. Navigate to the device that you want to migrate.
2. In the Manage device section, click **Migrate to iOS hardened channel**.
3. Click **Submit**.

Export a list of macOS devices that need to be reactivated to use a hardened channel

Perform these steps to export a list of devices that are impacted by the security issue communicated in KB99869. Each user that has a device that is listed in the file that you export must reactivate their device in the Self-Service portal.

1. Navigate to **Settings > Migration > macOS Hardened Channel**.
2. Click **Export**. A list of devices that must be reactivated is downloaded.
3. Contact the users who have devices in the list and have them reactivate their devices in the Self-Service Portal. For information about reactivating in the Self-Service portal, see the User Guide.

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada