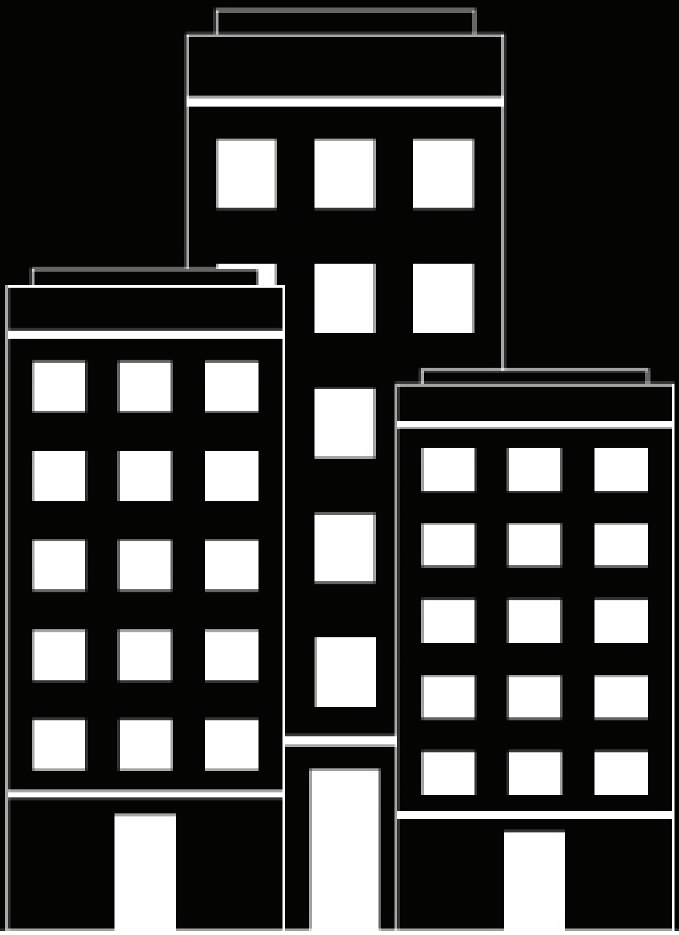

BlackBerry UEM

Managing device configurations

Administration

12.20

Contents

Managing device configurations.. 6

Using profiles to manage device features.. 8
- BlackBerry UEM profiles... 8
- Manage profiles...13

Using variables in profiles, emails, and notifications..................................... 15
- Define custom variables... 15

Using email templates to send messages to users..16
- Edit an email template...16
- Create an activation email template... 16
- Create a template for compliance notifications..17
- Create an event notification email template...17
- Suggested template text...17

Managing devices with IT policies.. 25
- Manage IT policies..25
- Import IT policy and device metadata updates manually.................................26

Create device support messages for disabled features on Android devices.... 28

Enforcing compliance rules for devices.. 29
- Create a compliance profile...29
- Common: Compliance profile settings...30
- iOS and iPadOS: Compliance profile settings..31
- macOS: Compliance profile settings.. 34
- Android: Compliance profile settings... 34
- Windows: Compliance profile settings...37
- Monitor compliance events..39

Sending commands to users and devices.. 41
- Send commands to users and devices..41
- Set an expiry time for commands.. 41
- Commands for iOS and iPadOS devices...42
- Commands for macOS devices... 44
- Commands for Android devices.. 45
- Commands for Windows devices... 48

Controlling how software updates are installed devices................................. 50
Create a device SR requirements profile for Android Enterprise and Android Management devices............ 50
Create a device SR requirements profile for Samsung Knox devices...51
Update the OS on supervised iOS devices...52

Configuring how devices contact BlackBerry UEM for app and configuration updates..53
Create an Enterprise Management Agent profile.. 53
iOS: Enterprise Management Agent profile settings... 53
Android: Enterprise Management Agent profile settings...53
Windows: Enterprise Management Agent profile settings..54

Displaying organization information on devices.. 56
Create organization notices.. 56
Create a device profile..56

Using location services on devices.. 58
Configure location service settings... 58
Create a location service profile...58
Locate a device.. 59
Turn on Lost Mode for supervised iOS devices.. 60

Enable Activation Lock for an iOS device...61

Managing iOS features with custom payload profiles....................................62
Create a custom payload profile.. 62

Managing factory reset protection for Android Enterprise and Android Management devices...64
Create a factory reset protection profile...65
Clear factory reset protection from a device...66

Configuring attestation for devices.. 67
Configuring attestation for Android devices and BlackBerry Dynamics apps..67
Configure attestation for Android devices and BlackBerry Dynamics apps..67
Configure attestation for iOS devices.. 68
Configure attestation for Samsung Knox devices..68
Configure attestation for Windows 10 devices... 69

Set up Windows Information Protection for Windows 10 devices....................70
Windows Information Protection profile settings...70

Move iOS or macOS devices to a hardened channel.......................................74

Legal notice... 75

Managing device configurations

This guide provides instructions for using BlackBerry UEM profiles, IT policies, and other key features to configure work devices to meet your organization's needs and security requirements.

Task	Description
Use profiles to manage device features.	Configure and assign UEM profiles to users and groups to manage a wide variety of device features and capabilities for all device types.
Use variables in profiles, emails, and notifications.	Use variables in profiles, compliance notifications, activation emails, and event notifications to customize configurations and messages for individual users.
Use email templates to send messages to users.	Use email templates to customize and personalize email messages that UEM sends to users for various reasons, including providing instructions for device activation, notifying users about compliance issues, and providing access keys for BlackBerry Dynamics apps.
Manage devices with IT policies.	Use IT policies to control device features and functionality. For example, you can use IT policy rules to enforce password requirements, prevent the use of certain device features (for example, the camera), and control the availability of certain apps.
Create device support messages for disabled features on Android devices.	Display a support message on Android devices when a feature is disabled by an IT policy.
Enforce compliance rules for devices.	Use compliance profiles to encourage users to follow your organization’s device standards. A compliance profile defines the device conditions that are not acceptable in your organization, and specifies enforcement actions for UEM to carry out if the user does not correct compliance issues.
Send commands to users and devices.	You can send various commands to manage user accounts and devices. For example, you can send a command to lock a device or to delete all work data from a device.
Control how software updates are installed on devices.	Use device SR requirements profiles to control how device software updates are installed on devices.
Configure how devices contact UEM for app and configuration updates.	Use Enterprise Management Agent profiles to configure how devices contact UEM for app or configuration updates.
Display organization information on devices.	Use organization notices and device profiles to display organization information on devices.
Use location services on devices.	Use location service profiles to request the location of devices and view their approximate locations on a map.

Task	Description
Enable Activation Lock for an iOS device.	Use the Activation Lock feature on iOS devices to allow 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.
Manage iOS features with custom payload profiles.	Use custom payload profiles to control features on iOS devices that aren't controlled by existing UEM policies or profiles.
Manage factory reset protection for Android devices.	Use factory reset protection profiles to control the factory reset protection feature for your organization's Android Enterprise and Android Management devices.
Configure attestation for devices.	Send challenges to test the authenticity and integrity of Samsung Knox, Android, iOS, and Windows 10 devices.
Set up Windows Information Protection for Windows 10 devices.	Use Windows Information Protection profiles to protect and manage work data on Windows 10 devices.
Move iOS or macOS devices to a hardened channel .	When you activate iOS or macOS devices, by default, the devices are assigned to a hardened data channel. If you have any iOS or macOS devices that are not currently using a hardened data channel, you can export a list of these devices and take action to move the devices to a hardened channel.

Using profiles to manage device features

BlackBerry UEM uses different types of profiles to manage a wide variety of device features and capabilities for iOS, macOS, Android, and Windows devices. You configure a profile to meet your organization's needs and then assign it to user accounts, user groups, and device groups to apply that configuration to devices.

To review a complete list of the available profiles, see BlackBerry UEM profiles.

Profiles can be ranked or unranked. For ranked profiles, UEM will assign one profile of that type to a device (for example, one compliance profile). If a ranked profile is assigned to a user directly, it takes precedence over any profiles of that type that are assigned to user groups that user belongs to. If a user belongs to multiple user groups with different profiles of that type assigned, ranking is used to determined which profile to assign. If a user's device belongs to a device group, the profile assigned to the device group takes precedence over the same profile of that type that is assigned directly to the user. If the device belongs to multiple device groups with different profiles of that type, ranking is used to determined which profile to assign.

For unranked profiles, more than one profile of that type can be a assigned to a device, either from direct assignment to a user account or through group assignment (for example, a device can be assigned more than one Wi-Fi profile).

For certain profile types, a profile must be assigned to devices. If a profile is not assigned to users directly or through group membership, UEM assigns a preconfigured default profile. UEM includes a default activation profile, default compliance profile, default enterprise connectivity profile, and default Enterprise Management Agent profile.

BlackBerry UEM profiles

Profile name	Description	Supported device types	Ranked or not ranked	For more information
Policy				
Knox Service Plugin	Set up and configure the Knox Service Plugin.	Android	Ranked	Managing Android devices with OEM app configurations
Activation	Configure device activation settings for users (for example, the activation type and the number and types of devices).	All devices	Ranked	Creating activation profiles
BlackBerry Dynamics	Enable BlackBerry Dynamics for users and configure standards for app access, data protection, and logging.	All devices	Ranked	Controlling BlackBerry Dynamics on devices

Profile name	Description	Supported device types	Ranked or not ranked	For more information
App lock mode	Configure a device to run only apps that you specify.	Supervised iOS devices Samsung Knox devices activated with MDM Windows 10 Education and Windows 10 Enterprise devices	Ranked	Limit the apps that can run on a device
Enterprise Management Agent	Configure how devices connect to UEM for app or configuration updates.	iOS Android Windows	Ranked	Configuring how devices contact BlackBerry UEM for app and configuration updates
Shared iPad	Configure an iPad device so that it can be shared by multiple users.	iOS	Ranked	Creating and managing shared iPad groups
Compliance				
Compliance	Define the device conditions that are not acceptable in your organization and configure enforcement actions.	All devices	Ranked	Enforcing compliance rules for devices
Compliance (BlackBerry Dynamics)	This is a read-only profile that displays the compliance settings that were imported from Good Control into an on-premises UEM environment.	All devices	N/A	N/A
Device SR requirements	Configure the software release versions that must be installed on devices.	Android	Ranked	Controlling how software updates are installed devices
Email, calendar, and contacts				
Email	Configure how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data.	All devices	Ranked	Creating email profiles

Profile name	Description	Supported device types	Ranked or not ranked	For more information
IMAP/POP3 email	Configure how devices connect to an IMAP or POP3 mail server and synchronize email messages.	All devices	Not ranked	Create an IMAP/POP3 email profile
Gatekeeping	Specify the Microsoft Exchange servers to use for automatic gatekeeping.	All devices	Ranked	Create a gatekeeping profile
CalDAV	Specify the server settings that devices can use to synchronize calendar information.	iOS macOS	Not ranked	Setting up CardDAV and CalDAV profiles
CardDAV	Specify the server settings that devices can use to synchronize contact information.	iOS macOS	Not ranked	Setting up CardDAV and CalDAV profiles
Networks and connections				
Wi-Fi	Configure how devices connect to a work Wi-Fi network.	All devices	Not ranked	Setting up work Wi-Fi networks for devices
VPN	Configure how devices connect to a work VPN.	All devices	Not ranked	Setting up work VPNs for devices
DNS	Specify the DNS servers that devices use to access specific domains.	iOS macOS	Ranked	Specify DNS servers for iOS and macOS devices
Proxy	Configure how devices use a proxy server to access web services on the Internet or a work network.	iOS macOS Android	Ranked	Setting up proxy profiles for devices
Enterprise connectivity	Configure how devices can connect to your organization’s resources using enterprise connectivity and whether devices can use BlackBerry Secure Connect Plus.	iOS Android	Ranked	Using BlackBerry Secure Connect Plus for connections to work resources

Profile name	Description	Supported device types	Ranked or not ranked	For more information
BlackBerry Dynamics connectivity	Configure the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps.	All devices	Ranked	Setting up network connections for BlackBerry Dynamics apps
BlackBerry 2FA	Enable two-factor authentication for users and configure pre-authentication and self-rescue features.	iOS Android	Ranked	Create a BlackBerry 2FA profile
Network usage	Configure whether work apps on iOS devices can use the mobile network or data roaming.	iOS	Ranked	Control network usage for apps on iOS devices
Web content filter	Limit the websites that a user can view on supervised iOS devices.	Supervised iOS devices	Not ranked	Create a web content filter profile on iOS devices
Single sign-on extension	Enable iOS devices to authenticate automatically with domains and web services in your organization's network.	iOS	Not ranked	Enable automatic authentication for iOS devices
Managed domains	Configure iOS devices to notify users about sending email outside of trusted domains and restrict the apps that can open documents downloaded from internal domains.	iOS	Not ranked	Specify email and web domains for iOS devices
AirPrint	Add printers to users' AirPrint printer lists.	iOS	Not ranked	Create an AirPrint profile for iOS devices
AirPlay	Add devices to users' AirPlay device lists.	iOS	Not ranked	Create an AirPlay profile for iOS devices
Access Point Name	Specify APNs for devices to use to connect to carriers.	Android	Not ranked	Create an Access Point Name profile for Android devices
Protection				

Profile name	Description	Supported device types	Ranked or not ranked	For more information
Windows Information Protection	Configure the Windows Information Protection setting in Windows 10.	Windows 10	Ranked	Set up Windows Information Protection for Windows 10 devices
Microsoft Intune app protection	Configure how to protect data in Office 365 apps.	iOS Android	Not ranked	Managing apps protected by Microsoft Intune
Location service	Request the location of devices and view approximate device locations on a map.	iOS Android Windows	Ranked	Using location services on devices
Do not disturb	Block BlackBerry Work notifications during off periods.	iOS Android	Ranked	Turn off notifications outside of work hours from BlackBerry Work
Factory reset protection	Control the factory reset protection feature on Android devices.	Android	Ranked	Managing factory reset protection for Android Enterprise and Android Management devices
CylancePROTECT	Configure the security features of CylancePROTECT Mobile for BlackBerry UEM.	iOS Android	Ranked	CylancePROTECT Mobile for BlackBerry UEM
Custom				
Device	Specify the information that displays on devices.	iOS Android Windows	Ranked	Displaying organization information on devices
Home screen layout	Configure the layout of apps on iOS devices.	iOS	Ranked	Configure the layout of apps on iOS devices
Custom payload	Specify custom device configuration information using payload code.	iOS	Not ranked	Managing iOS features with custom payload profiles
Per-app notification	Configure notification settings for system apps and apps that you manage with UEM.	Supervised iOS devices	Ranked	Manage app notifications on supervised iOS devices
Certificates				

Profile name	Description	Supported device types	Ranked or not ranked	For more information
CA certificate	Specify a CA certificate that devices can use to establish trust with a work network or server.	All devices	Not ranked	Sending CA certificates to devices and apps
Shared certificate	Specify a client certificate that devices can use to authenticate users with a work network or server.	iOS macOS Android	Not ranked	Send the same client certificate to multiple devices
User credential	Specify the CA connection that devices use to obtain a client certificate that is used to authenticate with a work network or server.	iOS macOS Android	Not ranked	Sending client certificates to devices and apps using user credential profiles
SCEP	Specify the SCEP server that devices use to obtain a client certificate that is used to authenticate with a work network or server.	All devices	Not ranked	Sending client certificates to devices and apps using SCEP
OCSP	Enable devices to check the status of S/MIME certificates.	iOS Android	Ranked	Determining the status of S/MIME certificates on devices
CRL	Configure UEM to search for the status of S/MIME certificates.	iOS Android	Ranked	Determining the status of S/MIME certificates on devices
Certificate mapping profile	Specify which client certificates apps must use.	Android	Ranked	Specify the certificate used by an app using a certificate mapping profile

Manage profiles

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click the appropriate profile type.
3. Do any of the following:

Task	Steps
Copy a profile.	**a.** Click the name of the profile that you want to copy. **b.** Click 🗐. **c.** Type a name and description for the profile. **d.** Configure the appropriate values for the profile. For more details about each type of profile, see BlackBerry UEM profiles. **e.** Click **Save**. **f.** Assign the profile to users and groups.
Change a profile.	**a.** Click the name of the profile that you want to change. **b.** Click ✎. **c.** Make changes to the profile. **d.** Click **Save**.
Rank profiles.	**a.** Click ↓↑. **b.** Use the arrows to move profiles up or down in the ranking. **c.** Click **Save**.
Remove a profile from user accounts.	**a.** Click the name of the profile that you want to remove. **b.** On the **Assigned to x users** tab, search for and select the user accounts that you want to remove the profile from. **c.** Click 👤.
Remove a profile from groups.	**a.** Click the name of the profile that you want to remove. **b.** On the **Assigned to x groups** tab, search for and select the groups that you want to remove the profile from. **c.** Click 👥.
Delete a profile.	You cannot delete a default profile. When you delete a custom profile, UEM removes it from the users and devices that it is assigned to. **a.** Select the profile that you want to delete. **b.** Click 🗑. **c.** Click **Delete**.

Using variables in profiles, emails, and notifications

BlackBerry UEM supports default and custom variables that you can use in profiles, compliance notifications, activation emails, and event notifications to customize configurations and messages for individual users. Default variables represent standard account attributes (for example, username, email) and other predefined attributes (for example, server address used for device activation). You can use custom variables to define additional attributes.

You can use a variable in any text field in a profile except for the name and description fields. For example, you can specify "%UserName%@example.com" in the email address field in an email profile.

You can view the list of default variables that are available for use in the management console in Settings > General settings > Default variables.

Note that IT policies and BlackBerry Dynamics app configurations do not support the use of variables.

Define custom variables

You can define up to five custom text variables and up to five masked text variables to represent sensitive information such as passwords. When you define a custom variable, you specify a label for the variable (for example, VPN password). When you create or update a user account, labels are used as field names in the Custom variables section and you can specify the appropriate values for that user. All user accounts support custom variables, including administrator accounts. You can use custom variables in the same ways that you use default variables.

1. In the management console, on the menu bar, click **Settings > General settings > Custom variables**.
2. Select the **Show custom variables when adding or editing a user** check box.
3. Specify a label for each custom variable that you want to use.
4. Click **Save**.

Using email templates to send messages to users

You can use email templates to customize and personalize email messages that BlackBerry UEM sends to users for various reasons, including providing instructions for device activation, notifying users about compliance issues, and providing access keys for BlackBerry Dynamics apps.

You can personalize email messages by using variables for items like the user's name, email address, or activation password, and you can customize the appearance of messages by using different fonts, colors, and images. You can create multiple templates to use for different device types or activation types. You can edit the default email templates or you can create new templates.

When you perform various tasks in the management console (for example, adding a user, creating a compliance profile, and so on), you can select the email template that you want UEM to use to send a message to device users.

You can view the available default templates in the management console in Settings > General settings > Templates.

Edit an email template

If you decide to change a default email template, it is recommended that you save a back-up of the original template text in case you want to restore it later.

1. In the management console, on the menu bar, click **Settings > General settings > Templates**.
2. Click the template that you want to edit.
3. Edit the **Name**, **Subject**, or **Message** fields as necessary.
4. Click **Save**.

Create an activation email template

1. In the management console, on the menu bar, click **Settings > General settings > Templates**.
2. Click + > **Device activation**.
3. In the **Name** field, type a name for the template.
4. In the **Subject** field, type the subject line of the activation email.
5. In the **Message** field, type the body text of the activation email.

   Use the HTML editor to customize formatting, insert images (for example, a corporate logo), and so on. You can insert variables to personalize portions of the email. See Using variables in profiles, emails, and notifications.
6. If you want users to activate their device using a QR Code instead of an activation password, select the **Append a QR code to email message for iOS and Android device activation** check box.
7. To send the activation password or QR Code separately from the activation instructions, select **Send two separate activation emails - first for complete instructions, second for password** and specify the content and options for the second activation email. If you decide to send only one activation email, verify that you include the activation password, the activation password variable, or the QR Code in the first email.
8. Click **Save**.

For more information about device activation, see Activating devices.

Create a template for compliance notifications

When a user's device does not comply with the requirements that you have configured in an assigned compliance profile, BlackBerry UEM can send a personalized email message to the user based on a specified template. UEM includes a default compliance violation email template that can be edited, but not deleted. If you don't assign a different template to a user account, UEM uses the default template.

1. In the management console, on the menu bar, click **Settings > General settings > Templates**.
2. Click + > **Compliance violation**.
3. In the **Name** field, type a name for the template.
4. In the **Subject** field, type a subject for the message.
5. In the **Message** field, type the body text of the compliance email message.

   Use the HTML editor to customize formatting, insert images (for example, a corporate logo), and so on. You can insert variables to personalize portions of the email. See Using variables in profiles, emails, and notifications.
6. Click **Save**.

For more information about device compliance, see Enforcing compliance rules for devices.

Create an event notification email template

You can create an event notification email template that BlackBerry UEM can use to send custom messages to administrators when certain events occur in your organization's UEM environment.

1. In the management console, on the menu bar, click **Settings > General settings > Templates**.
2. Click + > **Event notification**.
3. In the **Name** field, type a name for the template.
4. In the **Subject** field, type a subject line for the message. If you want to append the event type to the subject line, select the **Append event type to the email subject** check box.
5. In the **Message** field, type the body text of the event notification email.

   Use the HTML editor to customize formatting, insert images (for example, a corporate logo), and so on. You can insert variables to personalize portions of the email. See Using variables in profiles, emails, and notifications.
6. Click **Save**.

For more information about event notifications, see Creating event notifications.

Suggested template text

The suggested text below is used in the default email templates. If you edit the default email templates and later want to use the default text, you can copy and paste it from here.

Name	Suggested text
Android work profile activation code	**Subject: An Android work profile activation code has been created for you** %UserDisplayName%, To activate an Android device with a work profile only, your administrator has created an Android work profile activation code for you. You will receive your BlackBerry UEM activation password in a separate email message. Your Android work profile activation code: %GoogleActivationCode% Your Android work profile activation code will expire on %ActivationPasswordExpiry%. If you have any questions, contact your administrator.
Default managed Google account credentials	**Subject: A Google account has been created for you** %UserDisplayName%, To enable the work profile on your device, your administrator has created a Google account for you. You will need your Google account password when you activate the work profile. The Google account password displayed here is not the password that you use when you activate your device on BlackBerry UEM. You will receive your BlackBerry UEM activation password in a separate email message, or you can set your BlackBerry UEM activation password in BlackBerry UEM Self-Service. You will need the following information when you activate the work profile: • Your work email address: %UserEmailAddress% • Your Google account password: %Password% You can manage your Google Account at https://myaccount.google.com. If you change the password for your Google Account, the password included in this email will no longer apply, and you must use the new password instead. Please keep this information for your records. If you have any questions, contact your administrator.

Name	Suggested text
Apple DEP device activation email First email	**Subject: Activating your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your iOS device for BlackBerry UEM. To activate your device you need the following information: • Your work email address: %UserEmailAddress% • Your device activation password: Your activation password will be delivered in a separate email. You can manage your own device with BlackBerry UEM Self-Service at %UserSelfServicePortalURL%. To log in, use the following username: BlackBerry UEM Self-Service username: %UserName% Your BlackBerry UEM Self-Service password may have been delivered in a separate email. If you have not received it, contact your administrator. Please keep this information for your records. If you have any questions, contact your administrator.
Apple DEP device activation email Second email	**Subject: Password to activate your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your mobile device for BlackBerry UEM. To activate your device you need the following information: Your device activation password: %ActivationPassword% Your password will expire on %ActivationPasswordExpiry%. Please follow the instructions in the "Activating your device on BlackBerry UEM" email to activate your iOS device on BlackBerry UEM. If you have any questions, contact your administrator. Welcome to BlackBerry UEM!

Name	Suggested text
BlackBerry Dynamics access key email	**Subject: An access key for a BlackBerry Dynamics app has been created for you** %UserDisplayName%, Your administrator has created an access key for a BlackBerry Dynamics app. This email contains the access key and instructions to set up the app. If you have been given permission to use more than one app, you will receive more than one email. Each email has an access key that can be used to set up an app. You can use any of your access keys to set up any app, but you can only use each access key once. Before you begin, make sure you have mobile data or Wi-Fi coverage. **1.** Open the BlackBerry Dynamics app. **2.** When you are prompted, enter the following information. • Email address: %UserEmailAddress% • Access key: %AccessKeys% Your access key will expire on %AccessKeyExpiry%. **3.** You may be prompted to create a password. You will need to enter this password when you open the app. If you have any questions, contact your administrator.

Name	Suggested text
Default activation email First email	**Subject: Activating your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your mobile device for BlackBerry UEM. To activate your device you need some or all of the following information: • Your work email address: %UserEmailAddress% • Server name: %ActivationURL% • Activation username: %ActivationUserName% • Your device activation password: Your activation password will be delivered in a separate email. For Android devices: If you are using an Android device, you must install the BlackBerry UEM Client from Google Play. For iOS devices: If you are using an iOS device, you must install the BlackBerry UEM Client from the App Store. For iOS devices, open Safari and go to workspace://apps to install apps that your administrator has assigned to you. If available, you can also tap Work Apps on your device. For macOS devices: If you are using a macOS device, you must activate your device using BlackBerry UEM Self-Service. For devices running Windows 10 or later: You will need the following information to activate your device: • Server name: %ClientlessActivationURL% • Certificate server URL: %RsaRootCaCertUrl% • You must install the RSA certificate. Type the Certificate server URL in the address bar of the browser on your device. Follow the instructions and install the certificate into the Trusted Root Certification Authorities folder. • On your device, go to Settings > Accounts > Access work or school and tap Enroll only in device management. To manage your devices You can manage your own device with BlackBerry UEM Self-Service at %UserSelfServicePortalURL%. To log in, use the following username: BlackBerry UEM Self-Service username: %UserName% Your BlackBerry UEM Self-Service password may have been delivered in a separate email. Welcome to BlackBerry UEM!

Name	Suggested text
Default activation email Second email	**Subject: Password to activate your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your mobile device for BlackBerry UEM. To activate your device you need the following information: • Your device activation password: %ActivationPassword% • Your password will expire on %ActivationPasswordExpiry% Please follow the instructions in the "Activating your device on BlackBerry UEM" email to activate your iOS, Android, or Windows device on BlackBerry UEM. If you have any questions, contact your administrator. Welcome to BlackBerry UEM!
Default Android Management activation email	**Subject: Activating your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled Android Management on your device so that a work profile can be created. To create the work profile, you may click on the following link %ActivationAndroidManagementURL% from your device. You may also scan the QR code on your device. Navigate to Settings > Google Services > Set up & restore > Set up your work profile, then scan the following QR code. The activation link and QR code will expire on %ActivationPasswordExpiry% %ActivationAndroidManagementQRCode% Please keep this information for your records. If you have any questions, contact your administrator.
Default compliance email	**Subject: Notification of noncompliant device** Your device is not compliant with your organization's policies. If this condition persists your administrator might limit access to the organization's data from your device, delete the organization's data on your device, or delete all content and settings from your device.

Name	Suggested text
Default Work space only (Android Enterprise) activation email First email	**Subject: Activating your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your Android device (9.0 and later) for BlackBerry UEM. To activate your device, you need the following information: • Activation username: %ActivationUserName% • Your device activation password: Your activation password will be delivered in a separate email. To activate your device, perform the following actions: **1.** If you do not see the device setup Welcome screen, reset your device to the factory default settings. **2.** During the device setup, in the Add your account screen enter your Google account credentials. Wait while the device updates some important system apps and downloads the UEM Client. **3.** In the BlackBerry UEM Client, follow the instructions on the screen to activate your device. You can manage your own device with BlackBerry UEM Self-Service at %UserSelfServicePortalURL%. To log in, use the following username: BlackBerry UEM Self-Service username: %UserName% Your BlackBerry UEM Self-Service password may have been delivered in a separate email. If you have not received it, contact your administrator. Please keep this information for your records. If you have any questions, contact your administrator. Welcome to BlackBerry UEM!
Default Work space only (Android work profiles) activation email Second email	**Subject: Password to activate your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your Android device for BlackBerry UEM. To activate your device you need the following information: • Your device activation password: %ActivationPassword% • Your password will expire on %ActivationPasswordExpiry% Please follow the instructions in the "Activating your device on BlackBerry UEM" email to activate your device on BlackBerry UEM. If you have any questions, contact your administrator. Welcome toBlackBerry UEM!
BlackBerry UEM event notification email	**Subject: BlackBerry UEM event notification** The following event occurred: %AllEventVariables%

Name	Suggested text
Device activated notification	**Subject: Device activated on BlackBerry UEM** %UserDisplayName%, Your device has been activated on BlackBerry UEM. Device information Model: %DeviceModel% Serial Number: %SerialNumber% IMEI: %DeviceIMEI% If you did not activate this device, contact your administrator. **Subject: BlackBerry Dynamics device activated on BlackBerry UEM** %UserDisplayName%, Your BlackBerry Dynamics device has been activated on BlackBerry UEM. If you did not activate this device, contact your administrator.
Self-service login notification	**Subject: Self-service login notification** %UserDisplayName%, You have logged in to BlackBerry UEM Self-Service. IP address: %IPAddress% Time: %Timestamp% If you did not log in, contact your administrator.

Managing devices with IT policies

You can use IT policies to manage the security and behavior of devices in your organization's BlackBerry UEM environment. An IT policy is a set of rules that you can use to control device features and functionality. For example, you can use IT policy rules to enforce password requirements, prevent the use of certain device features (for example, the camera), and control the availability of certain apps.

You can configure rules for all device types in the same IT policy. The device OS determines the features that can be controlled using IT policy rules. The device activation type determines which rules apply to a specific device and whether you can use rules to control the entire device or the work space only. Devices ignore IT policy rules that are not applicable.

Download the IT policy rules spreadsheet for a comprehensive reference of all available IT policy rules for each device type that UEM supports.

UEM includes a default IT policy with preconfigured rules for each device type. You can change the default IT policy to meet your organization's needs. 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, UEM sends the default IT policy to a user's devices. 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.

UEM assigns only one IT policy to a device and uses predefined rules to determine which IT policy to assign. An IT policy assigned directly to a user takes precedence over an IT policy that is assigned through user group membership. If a user is a member of multiple user groups with different IT policies, ranking is used to determined which IT policy to assign. If a user's device belongs to a device group, the IT policy assigned to the device group takes precedence over an IT policy that is assigned directly to the user. If the device belongs to multiple device groups with different IT policies, ranking is used to determined which IT policy to assign.

Manage IT policies

You can change the default IT policy or you can create and assign custom IT policies.

1. In the management console, on the menu bar, click **Policies and profiles > Policy > IT policies**.
2. Do any of the following:

Task	Steps
Create an IT policy.	**a.** Click +. **b.** Type a name and description for the IT policy. **c.** Click the tab for each device type and configure the appropriate values for the IT policy rules. For more information about IT policy rules, see the IT policy rules spreadsheet. **d.** Click **Save**. **e.** Assign the IT policy to users and groups.

Task	Steps
Copy an IT policy.	**a.** Click the name of the IT policy that you want to copy. **b.** Click ⧉. **c.** Type a name and description for the IT policy. **d.** Click the tab for each device type and configure the appropriate values for the IT policy rules. For more information about IT policy rules, see the IT policy rules spreadsheet. **e.** Click **Save**. **f.** Assign the IT policy to users and groups.
Change an IT policy.	**a.** Click the name of the IT policy that you want to change. **b.** Click ✎. **c.** Make changes on the appropriate tab for each device type. **d.** Click **Save**.
Rank IT policies.	**a.** Click ↓↑. **b.** Use the arrows to move IT policies up or down in the ranking. **c.** Click **Save**.
Remove an IT policy from user accounts.	**a.** Click the name of the IT policy that you want to remove. **b.** On the **Assigned to x users** tab, search for and select the user accounts that you want to remove the IT policy from. **c.** Click 👤.
Remove an IT policy from groups.	**a.** Click the name of the IT policy that you want to remove. **b.** On the **Assigned to x groups** tab, search for and select the groups that you want to remove the IT policy from. **c.** Click 👥.
Delete an IT policy.	You cannot delete the default IT policy. When you delete a custom IT policy, UEM removes the IT policy from the users and devices that it is assigned to. **a.** Select the IT policy that you want to delete. **b.** Click 🗑. **c.** Click **Delete**.
Export IT policies to a .xml file.	**a.** Select the IT policies that you want to export. **b.** Click ➔.

Import IT policy and device metadata updates manually

BlackBerry regularly sends IT policy and device metadata updates to BlackBerry UEM. For example, when a vendor releases a new device model, BlackBerry may send updated device metadata to UEM so that activation and compliance profiles include the new device model. When a vendor releases an OS update, a new IT policy pack may be sent to UEM to allow you to manage new OS features.

By default, UEM receives and installs these updates automatically. If your organization's security policy does not allow automatic updates, and you have an on-premises UEM environment, you can turn off the automatic updates and import updates manually. Update files are cumulative. If you miss an update, the next update installs all previously updated IT policy rules or device metadata. You can set up event notifications to inform administrators when IT policy and device metadata updates are installed.

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

1. In the management console, on the menu bar, click **Settings > Infrastructure > Import configuration data**.
2. Do any of the following:
    - 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.
3. Click the appropriate **Browse** button to navigate to and select the data file that you want to import. Click **Open**.

Create device support messages for disabled features on Android devices

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.

1. In the management console, on the menu bar, click **Settings > General settings > Custom device support messages**.
2. In the **Device language** drop-down list, select the language that you want the notification to display in.
3. In the **Disabled feature notice** field, type the text that you want to display on devices when a feature is disabled.
4. Optionally, in the **Administrator support message** field, type a notice that displays in the Device administrators settings screen.
5. If you want to create a message in more than one language, click **Add an additional language** and repeat the previous steps.
6. If you added messages in more than one language, select the **Default language** radio button for the language that you want to use on devices that don’t use one of the specified languages.
7. 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 conditions that would make a device non-compliant, the notifications that a user receives when a device is non-compliant, and the actions that BlackBerry UEM will take if a compliance issue is not resolved (for example, limiting a user's access to the organization's resources, deleting work data from the device, or deleting all data from the device).

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.

For Samsung Knox devices, you can add a list of restricted apps to a compliance profile, but 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 Dynamics compliance profiles are imported from Good Control when you synchronize Good Control with UEM. You cannot edit BlackBerry Dynamics compliance profiles, but they can be used as a reference when you create new compliance profiles in UEM. Users that were assigned to a compliance profile in Good Control remain assigned to the same profile after they are synchronized with 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 UEM compliance profiles that might be assigned to a user.

Create a compliance profile

Before you begin:

- If you want to 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. 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 and iPadOS: 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 compliance email template.

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. In the management console, on the menu bar, click **Policies and profiles > Compliance > Compliance**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Email sent when violation is detected** drop-down list, select an email template.

   This is the default compliance email that UEM will send to a user when a compliance violation is detected. When you enable compliance rules in step 7, you have the option of selecting different email templates for each compliance rule, where applicable.

5. In the **Enforcement interval** drop-down list, select the frequency of compliance checks for BlackBerry Dynamics apps. You cannot configure the enforcement interval for non-BlackBerry Dynamics compliance checks, which occur at regular intervals.
6. Expand **Device notification sent out when violation is detected** and edit the message as necessary. You can use variables in the message to add specific user, device, and compliance information. See Using variables in profiles, emails, and notifications.
7. 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 the following:
    - Common: Compliance profile settings
    - iOS and iPadOS: Compliance profile settings
    - macOS: Compliance profile settings
    - Android: Compliance profile settings
    - Windows: Compliance profile settings
8. Click **Save**.

After you finish:

- Assign the profile to users and groups.
- If necessary, rank the profile.
- To monitor the compliance events that are detected by UEM, see Monitor compliance events.

Common: Compliance profile settings

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.

Compliance profile setting	Description
Prompt behavior	This setting specifies whether UEM prompts the user to correct a compliance issue and gives the user time to fix the issue before taking action, or whether UEM takes immediate action.
Prompt method	This setting specifies whether UEM prompts the user to correct a compliance issue by sending a device notification or an email message and a device notification. BlackBerry Dynamics apps provide only device notifications, regardless of this setting. Device notifications are not supported on Windows 10 devices. This setting is valid only if "Prompt behavior" is set to "Prompt for compliance."
Email template used when a compliance violation is detected	This setting specifies the email template to send to a user when the user's device is not compliant with the selected compliance rule. If you select "Use profile default", UEM sends the default email template that you configured for the profile (Email sent when violation is detected). This setting is valid only if "Prompt method" is set to "Email and device notification".

Compliance profile setting	Description
Prompt count	This setting specifies the number of times the user is prompted to correct a compliance issue. 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. This setting is valid only if "Prompt behavior" is set to "Prompt for compliance."
Enforcement action for device	This setting specifies the action that UEM takes on devices that are not compliant. The available options may differ depending on the OS and the type of compliance rule: • Monitor and log: UEM identifies the compliance violation but takes no enforcement action on the device. • Untrust: The user cannot access work resources and apps on the device. Data and apps are not deleted. 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 This setting does not apply to 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", UEM performs the same action as "Delete only work data". 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.
Enforcement action for BlackBerry Dynamics apps	This setting specifies what happens with BlackBerry Dynamics apps when a device is not in compliance: • Do not allow BlackBerry Dynamics apps to run • Delete BlackBerry Dynamics app data • Monitor and log: UEM identifies the compliance violation but takes no enforcement action.

iOS and iPadOS: Compliance profile settings

See Common: Compliance profile settings for descriptions of the enforcement actions that BlackBerry UEM can take if a device violates a compliance rule.

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 cannot complete new activations on a jailbroken device, regardless of the enforcement action that you set.
Managed device attestation failure	This setting creates a compliance rule that specifies the actions that occur when a device fails managed device attestation.
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. This setting does not apply to devices 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.
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 cannot 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 select the devices models that are allowed or restricted. If you select this setting, users cannot complete new activations for devices that are not compliant, regardless of the enforcement action that you set.
OS update not applied	This setting creates a compliance rule to execute compliance actions if a user does not apply a pending OS update within a time period that you specify.
Device is out of contact	This setting creates a compliance rule to ensure that devices are not out of contact with UEM for more than a specified amount of time. You specify the number days that a device can be out of contact with UEM before it is considered out of compliance.
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.

Compliance profile setting	Description
BlackBerry Dynamics connectivity verification	This setting creates a compliance rule to monitor whether BlackBerry Dynamics apps are out of contact with 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 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 UEM before the device is considered 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 screen capture detection on iOS devices	**Note:** This compliance rule has been replaced with the "Do not allow screenshots on iOS devices" option in BlackBerry Dynamics profiles. BlackBerry recommends using the profile setting and disabling this compliance rule. This compliance rule will be deprecated in a future UEM release. 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 a specified time period. The "Enforcement action for BlackBerry Dynamics apps" setting specifies the action that occurs if the user exceeds the allowed number of screen captures.
Restricted app is installed	This setting creates a compliance rule for UEM to periodically check for restricted apps, including marketplace apps. Add apps to the restricted apps list in the profile by selecting the apps from the UEM restricted app list or by selecting a built-in app (supervised devices only). When you select this setting and a restricted app is installed on a device, a warning message and a link is displayed in the Managed devices screen in the console. When you click the link, a list of apps that are putting the device out of compliance is displayed. The list of restricted apps is also sent to the user in the compliance notification. 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 can be installed on devices, including marketplace apps. All other apps are not allowed. Add apps to the allowed apps list in the profile by selecting apps from the UEM app list or by selecting built-in apps. Some apps are included in the allowed list by default. This setting is valid only for supervised devices.

macOS: Compliance profile settings

See Common: Compliance profile settings for descriptions of the enforcement actions that BlackBerry UEM can take if a device violates a compliance rule.

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 cannot 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 select the device models that are allowed or restricted. If you select this setting, users cannot 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 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 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 UEM before the device is considered out of compliance.

Android: Compliance profile settings

See Common: Compliance profile settings for descriptions of the enforcement actions that BlackBerry UEM can take if a device violates a compliance rule.

Compliance profile 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. If you select this setting, users will be unable to complete new activations for rooted devices, regardless of the enforcement action that you set. Selecting "Enable detection of debuggers and emulators when running BlackBerry Dynamics applications" stops BlackBerry Dynamics apps if the BlackBerry Dynamics Runtime detects an active debugging or emulation tool. Selecting "Enable detection of unlocked or unverified boot device detection for BlackBerry Dynamics apps" will enable UEM to check the boot state of the device.
SafetyNet or Play Integrity attestation failure	This setting creates a compliance rule that specifies the actions that occur if devices do not pass SafetyNet or Play Integrity attestation. When you use SafetyNet or Play Integrity attestation, UEM sends challenges to test the authenticity and integrity of Android devices and apps in your organization's environment. See Configure attestation for Android devices and BlackBerry Dynamics apps.
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 screen in the console. When you click the link, a list of non-assigned apps is displayed. For Android Enterprise, Android Management, 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 screen in the console. For Android Enterprise and Android Management 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.
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.

Compliance profile setting	Description
Restricted device model detected	This setting creates a compliance rule to restrict 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.
OS update not applied	This setting creates a compliance rule to execute compliance actions if a user does not apply a pending OS update within a time period that you specify.
Device out of contact	This setting creates a compliance rule to monitor whether devices are out of contact with 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 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".
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 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 UEM. This setting applies only if an authentication delegate is specified in an assigned BlackBerry Dynamics profile. The "Last contact time" setting specifies the number days a device can be out of contact with UEM before it is considered out of compliance.

Compliance profile setting	Description
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 and Android Management 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 devices with the Work and personal - full control (Samsung Knox) activation type, select "Enforce compliance actions in the personal space" to apply the rule to apps in both the work profile and the personal profile. 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 screen in the console. When you click the link, a list of restricted apps is displayed.
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 assigned IT policy.

Windows: Compliance profile settings

See Common: Compliance profile settings for descriptions of the enforcement actions that BlackBerry UEM can take if a device violates a compliance rule.

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. You can select the restricted OS versions.
Restricted device model detected	This setting creates a compliance rule to restrict 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 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 UEM for more than a specified amount of time. The enforcement action is applied to BlackBerry Dynamics apps.

Compliance profile setting	Description
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 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.
Windows device health attestation	
Grace period expired	This setting creates a compliance rule to specify actions that occur if the attestation grace period has expired.
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.

Compliance profile setting	Description
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. You specify 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. You specify 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. You specify the allowed values.
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. You specify the allowed values.
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. You specify the allowed values.

Monitor compliance events

After you configure and assign compliance profiles to users, you can use the compliance event screen to monitor and track compliance violations on users' iOS, Android, macOS, and Windows devices. This screen will also display any compliance events related to CylancePROTECT Mobile for UEM features.

Before you begin: Create and assign compliance profiles.

1. In the management console, on the menu bar, click **Users > Compliance violations**.
2. Do any of the following:
    - By default, this screen displays new compliance events from the indicated date range. To view resolved, ignored, or all alerts, or to change the date range, click **Edit**. Set the status and date range and click **Submit**.
    - In the **Filters** section, set the appropriate filters for the compliance events that you want to view and click **Submit**.
    - Click ⋮ to set the columns that you want to display.
    - Click a column to sort events by that criteria.

- Use the search field to search for specific compliance events.

3. If you want to remove an event from this view, select the event and click ⊘. Ignoring an event removes it from this view, it does not impact the associated device’s compliance status.
4. To export select events to a .csv file, select the events and click ➔.

Note that compliance events with any status are automatically deleted from this view after 120 days. Events with an ignored or resolved status are automatically deleted after 7 days.

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, 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 their 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 commands to users and devices

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Do one of the following:

Task	Steps
Send a command to a specific user or device	**a.** Search for and click a user. **b.** On the device tab, in the **Manage device** section, click the appropriate command.
Send a bulk command to multiple users or devices	**a.** Search for and select multiple users. **b.** From the command menu above the user list, click the appropriate command.

For more information about the available commands, see the following:

- Commands for iOS and iPadOS devices.
- Commands for macOS devices.
- Commands for Android devices.
- Commands for Windows devices.

After you finish: If you want to set an expiry period for the Delete all device data and Delete only work data commands, see Set an expiry time for commands.

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 UEM, the command remains in a pending status and the device is not removed from UEM unless you manually remove it. Alternatively, you can configure UEM to automatically remove devices when the commands do not complete after a specified amount of time.

1. In the management console, on the menu bar, click **Settings > General settings > Delete command expiration**.
2. For one or both commands, select **Automatically remove the device if the command expires**.
3. In the **Command expiration** field, type the number of days after which the command expires and the device is automatically removed from UEM.
4. Click **Save**.

Commands for iOS and 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.	MDM controls User privacy
View device actions	This command displays any actions that are in progress on a device.	MDM controls User privacy
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 UEM after you remove it, only the work data is deleted from the device. If you send the command to devices with iOS 17 or later, you can select the “Enable Return to Service” option and select a Wi-Fi profile to assign to the devices to assist the user in setting up the device again after data is deleted. If eSIM information is detected on one or more devices that you select, you are prompted to specify whether the data plan information must be preserved.	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 UEM when you send this command, you can either cancel the command or remove the device from the console. If the device connects to UEM after you remove it, the work data is deleted from the device.	MDM controls User privacy

Command	Description	Activation types
Lock device	This command locks a device. Apple appends "Lost iPhone" or "Lost iPad" to the title of the message you specify. The user must type the existing device password to unlock the device. 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 allows you to display a phone number and message on the device. After you send this command you can view the location of the device in the management console. This command is supported for supervised devices only. This command is not supported for Apple TV devices.	MDM controls
Deactivate BlackBerry 2FA	This command deactivates devices that are activated with the BlackBerry 2FA activation type. The device is removed from 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. This command is supported for supervised devices only. This command is not supported for Apple TV devices.	MDM controls
Restart device	This command forces the device to restart. This command is supported for supervised devices only. This command is not supported for Apple TV devices.	MDM controls
Turn off device	This command forces the device to turn off. This command is supported for supervised devices only. 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.	MDM controls

Command	Description	Activation types
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.	MDM controls User privacy
Update time zone	This command sets the device time according to the region that you select.	MDM controls
Remove device	This command removes the device from 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 UEM, the user receives a notification and the device won't be able to communicate with UEM unless it is reactivated.	MDM controls User privacy
Refresh eSIM	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.
View device actions	This command displays any actions that are in progress on a device.
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.
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 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.

Command	Description
Remove device	This command removes the device from UEM. The device may continue to receive email and other work data.

Commands for Android devices

For Android Management activation types, see Considerations for Android Management activation types.

Command	Description	Activation types
View device report	This command displays detailed information about a device. You can export and save the device report.	All (except BlackBerry 2FA)
View device actions	This command displays any actions that are in progress on a device..	All (except BlackBerry 2FA)
Lock device	This command locks the device. The user must type the existing device password to unlock the device. When you send this command, the device locks only if there is an existing device password. Otherwise, no action is taken on the device.	Work and personal - full control (Android Management) Work and personal - user privacy (Android Management) Work space only (Android Management) Work and personal - full control (Android Enterprise) Work and personal - user privacy (Android Enterprise) Work space only (Android Enterprise) MDM controls
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 UEM when you send this command, you can either cancel the command or remove the device from the console. If the device connects to UEM after you remove it, only the work data is deleted from the device, including the work space, if applicable.	Work and personal - full control (Android Management) Work space only (Android Management) Work and personal - full control (Android Enterprise) Work and personal - full control (Samsung Knox) MDM controls

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 is deleted from the device but all personal apps and data remain. 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. If the device is unable to connect to UEM when you send this command, you can either cancel the command or remove the device from the console. If the device connects to UEM after you remove it, the work data is deleted from the device, including the work space, if applicable.	Work and personal - full control (Android Management) Work and personal - user privacy (Android Management) Work and personal - full control (Android Enterprise) Work and personal - user privacy (Android Enterprise) Work and personal - full control (Samsung Knox) Work and personal - user privacy (Samsung Knox) MDM controls
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. This command is not supported by devices with Samsung Knox SDK 3.2.1 and later.	Work and personal - full control (Samsung Knox) Work and personal - user privacy (Samsung Knox) MDM controls (Samsung devices only)
Specify device password and lock	This command allows you to 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.	Work and personal - user privacy (Android Management) Work space only (Android Management) Work space only (Android Enterprise) Work and personal - full control (Samsung Knox)
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)

Command	Description	Activation types
Specify work space password and lock	This command allows you to 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 - full control (Android Enterprise) Work and personal - user privacy (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 (Android Management) Work and personal - user privacy (Android Management) Work space only (Android Management) Work and personal - full control (Samsung Knox) Work and personal - user privacy - (Samsung Knox)
Deactivate BlackBerry 2FA	This command deactivates devices that are activated with the BlackBerry 2FA activation type. The device is removed from 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.	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.	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)
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 Management) Work space only (Android Enterprise)

Command	Description	Activation types
Remove device	This command removes the device from 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 UEM, the user receives a notification and the device won't be able to communicate with UEM unless it is reactivated.	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.
View device actions	This command displays any actions that are in progress on a device.
Lock device	This command locks a device. The user must type the existing device password to unlock the device. 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.
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 UEM. If the device is unable to connect to UEM, you can remove it from UEM. If the device connects to UEM after you removed it, only the work data is deleted from the device, including the work space, if applicable.

Command	Description
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 UEM. After you send this command, you are given the option of deleting the device from UEM. If the device is unable to connect to UEM, you can remove it from UEM. If the device connects to UEM after you removed it, only the work data is deleted from the device, including the work space, if applicable.
Restart desktop/device	This command forces the device 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.
Remove device	This command removes the device from UEM. The device may continue to receive email and other work data.

Controlling how software updates are installed devices

You can use device SR requirements profiles to control how device software updates are installed on Android Enterprise, Android Management, and Samsung Knox devices, as well as how app updates are managed for apps running in the foreground.

You can use IT policy rules to control software updates on iOS devices. For more information, see the IT policy reference spreadsheet. You can also use the management console to update the OS on supervised iOS devices.

Create a device SR requirements profile for Android Enterprise and Android Management devices

OS update rules apply only to Android Enterprise and Android Management devices with Work space only and Work and personal - full control activation types. App update rules apply to all Android Enterprise devices. Currently, suspending OS updates and automatic app updates are not supported for Android Management devices. See Considerations for Android Management activation types.

1. In the management console, on the menu bar, click **Policies and profiles > Compliance > Device SR requirements**.
2. Click +.
3. Type a name and description for the profile.
4. To configure OS update rules for Work space only and Work and personal - full control devices, in the **OS update rule** section, click + and do the following:
   a) In the **Device model** drop-down list, select a device model.
   b) In the **OS version** drop-down list, select the installed OS version.
   c) In the **Update rule** drop-down list, select one of the following:
      - **Default**: The user can choose when to install updates. Users with the Work space only (fully managed device) activation type cannot choose when to install updates.
      - **Update automatically**: Updates are installed without prompting the user.
      - **Update automatically between**: Updates are installed in a time frame that you specify, without prompting the user. The user can choose to install updates outside of this window.
      - **Postpone up to 30 days**: 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.

   d) Click **Add**.
5. To specify time periods when OS updates should not occur for Work space only and Work and personal - full control devices, in the **Suspend OS updates** section, click +. Select the month and day that the suspension period starts and the duration of the suspension period.

   If you specify more than one suspension period, there must be at least 60 days between periods.
6. 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**. Select the start time and duration.
7. To specify how Google Play applies the changes to apps running in the foreground (the Auto-Update Apps setting in Google Play), in the **App auto update policy** drop-down list, select one of the following:
   - **Always**: Apps will always update. For apps that are always running (for example, the 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 it.

- **Wi-Fi only**: Apps will update only when the device is connected to a Wi-Fi network. For apps that are always running (for example, the 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 it.
- **User can allow**: The user is prompted to allow apps to update on the device.
- **Disable**: Apps will never update.

If you select **Always**, **Wi-Fi only**, or **Disable**, the user cannot select a different option on the device. Users can still manually update apps in Google Play.

8. Click **Add**.

After you finish:

- Assign the profile to users and groups.
- If necessary, rank the profile.
- To view a list of users who are running a revoked software release (a software release that is no longer accepted by a service provider), in **Policies and profiles > Compliance > Device SR requirements**, click a profile, then click the **x users running revoked SR** tab.

Create a device SR requirements profile for Samsung Knox devices

On Samsung Knox devices, you can use Knox E-FOTA One (Enterprise Firmware Over the Air) to control when firmware updates from Samsung are installed. If your organization uses Samsung E-FOTA (end of service July 31, 2022) and you need to migrate to E-FOTA One, see KB 69901.

Samsung Knox devices that are activated as 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 One.

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

Before you begin:

- In the management console, on the menu bar, go to **Settings > Licensing summary** to add an E-FOTA license to BlackBerry UEM.
- To use E-FOTA, you must enable the Android global "Allow OTA updates" rule in the IT policy that you assign to devices.

1. In the management console, on the menu bar, click **Policies and profiles > Compliance > Device SR requirements**.
2. Click +.
3. Type a name and description for the profile.
4. If you want to allow Android OS update rules to be applied to Samsung devices, select the **Apply restriction to all Android devices** check box.

   The firmware rules you will configure in the following steps take precedence over these rules. Suspend OS updates settings do not apply to Samsung Knox devices that use E-FOTA.
5. In the **Samsung device firmware rules** section, click +.
6. In the **Device model** drop-down list, type the device model or select a model from the list.
7. In the **Language** drop-down list, select a language.
8. In the **Carrier code** field, type the CSC code for the wireless service provider.
9. Click **Get firmware version**.

10. Repeat the previous steps for each firmware rule that you want to add.
11. When you are done, click **Add**.
12. If you want to schedule a forced update, click **Schedule** beside a firmware version that you added. In the **Schedule forced update** dialog box, do the following:

    a) In the **Schedule forced update between** fields, select a date range when the update must be installed.
    b) In the **Schedule forced update during the hours of** drop-down lists, specify when the forced update must be installed.

    If you schedule a forced update, the Knox device is no longer restricted to the firmware version and you can manually update it if a later version is available.
13. Click **Save**.

After you finish:

- Assign the profile to users and groups.
- If necessary, rank the profile.
- To view a list of users who are running a revoked software release (a software release that is no longer accepted by a service provider), in **Policies and profiles > Compliance > Device SR requirements**, click a profile, then click the **x users running revoked SR** tab.

Update the OS on supervised iOS devices

You can use the management console to force supervised iOS devices to install an available OS update.

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Do any of the following:

Task	**Steps**
Update the OS on a specific supervised iOS device	**a.** Search for and click the name of a user account. **b.** On the appropriate device tab, if a software update is available, click **Update now**. **c.** Configure the appropriate OS update settings. **d.** Click **Update**.
Update the OS on multiple supervised iOS devices	**a.** Select the user accounts. **b.** Click . **c.** Configure the appropriate OS update settings. **d.** Click **Update**.

Configuring how devices contact BlackBerry UEM for app and configuration updates

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, UEM prompts the device to contact 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 UEM at an interval that you specify.

In on-premises environments, you can also use the Enterprise Management Agent profile to allow UEM to collect a list of personal apps on users' devices.

Create an Enterprise Management Agent profile

1. In the management console, on the menu bar, click **Policies and profiles > Policy > Enterprise Management Agent**.
2. Click +.
3. Type a name and description for the profile.
4. Configure the settings for each device type. For more information about the settings, see the following:
   - iOS: Enterprise Management Agent profile settings
   - Android: Enterprise Management Agent profile settings
   - Windows: Enterprise Management Agent profile settings
5. Click **Add**.

After you finish:

- Assign the profile to users and groups.
- If necessary, rank the profile.

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.
Allow personal app collection	Specify whether BlackBerry UEM receives a list of personal apps that are installed on a user's device. 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.

Setting	Description
Battery level threshold	Specify the percentage of battery level change that is required before the device sends information back to BlackBerry UEM.
RAM free space threshold	Specify the required change in the amount of free memory in megabytes before the device sends information back to 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 UEM.
Memory card threshold	Specify the required change in the amount of external free space in megabytes before the device sends information back to UEM.
Enterprise Management Agent poll rate	Specify how often, in seconds, the device polls for Enterprise Management Agent server commands.
Allow personal app collection	Specify whether UEM receives a list of personal apps that are installed on a user's device. 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.
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.

Setting	Description
Allow personal app collection	Specify whether BlackBerry UEM receives a list of personal apps that are installed on a user's device.

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 to display during the activation process (for example, you can display a notice about 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 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. 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.

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

Create organization notices

1. In the management console, on the menu bar, click **Settings > General settings > Organization notices**.
2. Click +.
3. Type a name for the organization notice.
4. Optionally, you can reuse text from an existing organization notice by selecting it in the **Text copied from organization notice** drop-down list.
5. In the **Device language** drop-down list, select the default language for the notice.
6. In the **Organization notice** field, type the content of the notice.
7. Optionally, click **Add an additional language** as needed to post the organization notice in more languages.
8. 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.
9. 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.

1. In the management console, on the menu bar, click **Policies and profiles > Custom > Device**.
2. Click +.
3. Type a name and description for the profile.

4. Perform one of the following tasks:

Task	Steps
Assign an organization notice to display on Samsung Knox devices when a user restarts their device.	On the **Android** tab, in the **Assign organization notice** drop-down list, select the appropriate organization notice.
For iOS and Android devices, define the organization information to display in the BlackBerry UEM Client. For Windows 10, define the phone number and email address to display in the support information on devices.	On the appropriate OS tab, specify the name, address, phone number, and email address.

5. Optionally, do any of the following:

Task	Steps
Add a wallpaper image to the work space on Samsung Knox devices.	**a.** On the **Android** tab, in the **Work space wallpaper** section, click **Browse**. **b.** Navigate to and select the image.
Add a wallpaper image to supervised iOS devices.	On the **iOS** tab, in the **Device wallpaper** section, do any of the following: • To set wallpaper for the lock screen, next to **Lock screen image**, click **Browse**. Navigate to and select the image. • To set wallpaper for the home screen, next to **Home screen image**, click **Browse**. Navigate to and select the image.

6. Click **Add**.

After you finish:

- Assign the profile to users and groups.
- If necessary, rank the profile.

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 you 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.

To enable and use location services, do the following:

Step	Action
1	Configure location service settings.
2	Create a location service profile.
3	Locate a device.
4	Optionally, Turn on Lost Mode for supervised iOS devices.

Configure location service settings

1. In the management console, 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 how long you want BlackBerry UEM to store the location history for devices. By default, UEMwill store the history for 1 month.
3. In the **Displayed unit of speed** drop-down list, click **km/h** or **mph**.
4. Click **Save**.

After you finish: Create a location service profile.

Create a location service profile

Before you begin: Configure location service settings.

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

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

6. Click **Add**.

After you finish:

- Assign the profile to users and 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.
- If necessary, rank the profile.
- Locate a device.

Locate a device

Before you begin: Create a location service profile.

1. In the management console, 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 current location icon (📍) and last known location icon (📍). 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.
5. Click or hover over an icon to display location information, such as latitude and longitude and when the location was reported.
6. To view the location history for an iOS or Android device, click **View location history**, select a date and time range, and click **Submit**.

Turn on Lost Mode for supervised iOS devices

You can enable and manage Lost Mode for supervised iOS devices. When a device is lost, you can turn on Lost Mode to lock the device and set a message to display, and you can view the current location of the device without using a location service profile.

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

After you finish:

- To locate a device that is in Lost Mode, on the device tab, click **Get device location**.
- To turn off Lost Mode, on the device tab, click **Turn off Lost Mode**.

Enable Activation Lock for an iOS device

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.

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 enable it for multiple devices using the associated IT policy rule. When you enable Activation Lock, 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.

Complete the following steps to enable Activation Lock for each device individually.

Before you begin:

- The device must be supervised.
- The device must be associated with an iCloud account.
- The device must have Find My iPhone or Find My iPad enabled.

1. In the management console, on the menu bar, click **Users**.
2. Search for and click a user account.
3. On the device tab, in the **Manage device** section, click **Enable Activation Lock**.

After you finish:

- To disable Activation Lock for a device, click **Disable Activation Lock**. If Activation Lock is enabled using the IT policy rule, you cannot use this option to disable it.
- To view the bypass code for a device, navigate to **Users > Apple Activation Lock**, then search for and click a device.

Managing iOS features with 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. If a feature is controlled by an existing 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 UEM custom payload profiles. You can assign custom payload profiles to users, user groups, and device groups.

For example, you want to control a new feature that will be available to devices when they upgrade to a new iOS update, but UEM won't have an IT policy rule for that new feature until a future UEM software release. To solve this, you can create a custom payload profile that controls the feature until it is officially supported by UEM.

Create a custom payload profile

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

1. In the Apple Configurator, create an Apple configuration profile.
2. 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>
```

3. In the UEM management console, on the menu bar, click **Policies and profiles > Custom > Custom payload**.
4. Click +.
5. Type a name and description for the profile.
6. In the **Custom payload** field, paste the XML code you copied in step 2.
7. Click **Add**.

After you finish: Assign the profile to users and groups.

Managing factory reset protection for Android Enterprise and Android Management devices

You can use the factory reset protection profile to control the factory reset protection feature for your organization’s Android Enterprise and Android Management 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.

Factory reset protection profiles provide the following options:

Option	Description	Supported activation types
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.	Android Enterprise
Enable and use previous Google account credentials when the device is reset to factory settings	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 in to 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.	Android Enterprise
Enable and specify Google account credentials when the device is reset to factory settings	You can specify Google account credentials that a user can use to log in to the device after it has been reset to factory settings. This option allows your organization to control who can log in to a device after it is reset to factory settings. BlackBerry recommends that you use this option only if you fully understand the device user experience. If your organization uses a Managed Google Play account, you may want to use this option because a Google account does not exist on your organization's devices and therefore factory reset protection is not available on the device.	Android Enterprise Android Management

There are several ways that a device can be reset to the default factory settings. Factory reset protection responds differently depending on the method used. For more information about trusted and untrusted resets, see KB 56972.

Create a factory reset protection profile

1. In the management console, on the menu bar, click **Policies and profiles > Managed devices > Protection > Factory reset protection**.
2. Click +.
3. Type a name and description for the profile.
4. In the **Factory reset protection setting** drop-down list, click one of the following:
   - **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. This option is supported for Android Enterprise devices (Work and personal - full control and Work space only).
   - **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. This option is supported for Android Enterprise devices (Work and personal - full control and Work space only).
   - **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 in to 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. This option is supported for Android Enterprise and Android Management devices (Work and personal - full control and Work space only).

     If you want to use a managed Google Play account, in the IT policy assigned to users, turn off the "Allow factory reset" option. This disables the factory reset option in the device settings and disables the deactivate button in the UEM Client. This ensures that users do not use the untrusted deactivation option in the UEM Client that triggers factory reset protection on the device.
5. If you selected **Enable and specify Google account credentials when the device is reset to factory settings**, click + and do one of the following to add Google accounts (you can add up to 20):
   - To use Google authentication, click **Add using Google authentication** and sign in to the Google account that you want to use to log in to devices that have been reset.
   - To specify accounts manually, click **Manual**. Specify the email address and Google ID. To obtain the Google ID, do the following in the Google developers People API site:

     a. For the **resourceName**, type people/me.
     b. For the **personalFields**, type metadata.
     c. Click **Execute**.
     d. On the **Choose an account** screen, select an account to use to set up the factory reset protection profile.
     e. On the **Google APIs Explorer wants to access your Google Account** screen, click **Allow**.
     f. On the **People ID** page, note the 21-digit user ID.
6. If you selected **Enable and specify Google account credentials when the device is reset to factory settings** and your organization has a Google Workspace 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.
7. Click **Save**.

After you finish:

- Assign the profile to users and groups.
- If necessary, rank the profile.

- When factory reset protection is triggered on the device, enterprise activation on BlackBerry UEM will not work. You must first clear factory reset protection using the Android out-of-box experience. See Clear factory reset protection from a device.

Clear factory reset protection from a device

When factory reset protection is triggered on the device, enterprise activation on BlackBerry UEM will not 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. When 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. After the user enters 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 the enterprise Google account details to install the BlackBerry UEM Client and re-activate the device on 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 reactivate.
    - 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.

Configuring 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 Samsung Knox, Android, iOS, and Windows 10 devices.

Configuring attestation for Android devices and BlackBerry Dynamics apps

You can use SafetyNet or Google Play Integrity attestation to have BlackBerry UEM send challenges to test the authenticity and integrity of Android devices and BlackBerry Dynamics apps. SafetyNet and Play Integrity help you assess the security and compatibility of the environments in which your organization's apps run. You can use SafetyNet or Play Integrity attestation in addition to BlackBerry's existing root and exploitation detection. You can configure and assign a UEM compliance profile to carry out appropriate compliance actions when devices or apps fail attestation.

UEM uses the Play Integrity API with UEM Client versions that support it to provide additional protection from application tampering. Play Integrity will replace SafetyNet based on the migration schedule that is determined by Google. SafetyNet will continue to be supported for older versions of the UEM Client. For more information about migrating from SafetyNet, see Google Play: Migrating from the SafetyNet Attestation API.

UEM performs SafetyNet or Play Integrity attestation in the following circumstances:

- After device activation when the BlackBerry UEM Client is installed.
- During and after the activation of BlackBerry Dynamics apps. Note that UEM does not trust old versions of apps. To pass attestation challenges, devices must have the latest available version of BlackBerry Dynamics apps.
- On demand using REST APIs.
- If the UEM Client is activated, when a device is restarted.
- Periodic attestation challenges using the challenge frequency that you specify.

The UEM Client is not required for you to enable SafetyNet or Play Integrity attestation. The UEM Client does not appear in the list of BlackBerry Dynamics apps that you can configure for SafetyNet or Play Integrity attestation, but it does receive and respond to attestation challenges from UEM.

If a user's device is out of coverage, turned off, or has a dead battery, it cannot respond to attestation challenges. In these circumstances, UEM will consider the device to be out of compliance and will carry out the actions you've configured in the assigned compliance profile.

Configure attestation for Android devices and BlackBerry Dynamics apps

Before you begin: The latest version of Google Play services must be installed on users' devices.

1. In the management console, on the menu bar, click **Settings > General settings > Attestation**.
2. Select the **Enable attestation challenges using SafetyNet or Play Integrity** check box.
3. If you want to enable the Google Compatibility Test Suite, select the **Enable CTS profile matching** check box.
4. In the **Challenge frequency** section, specify how often the device must return an attestation response to BlackBerry UEM. The default and minimum value is 24 hours.
5. In the **Grace period** section, specify the grace period for devices. When the grace period expires with no successful attestation response, a device is considered out of compliance and is subject to the actions that you specify in the assigned compliance profile.

6. In the **App grace period** section, specify a grace period for BlackBerry Dynamics apps. When the grace period expires with no successful attestation response, a BlackBerry Dynamics app is subject to the actions that you specify in the assigned compliance profile. The grace period is enforced on a per-app basis.
7. To specify the BlackBerry Dynamics apps that will be subject to attestation challenges, click +.
8. Select the apps and click **Select**.
9. Click **Save**.

After you finish:

- In the compliance profile assigned to devices, enable the "SafetyNet or Play Integrity attestation failure" rule and configure the actions that you want UEM to carry out when devices or BlackBerry Dynamics apps fail attestation.
- In the management console, you can view a device's attestation status in the device details.

Configure attestation for iOS devices

When you enable attestation for iOS devices, it ensures that only authorized and uncompromised devices are being used in your organization. During attestation, the device's properties (for example, its serial number) or identifiers are verified to be legitimate and not spoofed. This feature requires unsupervised devices to be running iOS 16 or iPadOS 16.1 or later. For supervised devices, iOS 17 or iPadOS 17 or later is required.

1. In the management console, on the menu bar, click **Settings > General settings > Attestation**.
2. Select the **Enable periodic attestation challenges for Apple devices that are running iOS 16 or later** check box.
3. In the **Challenge frequency** section, specify how often the device must return an attestation response to UEM. The minimum challenge frequency is 9 days.
4. In the **Grace period** section, specify the grace period for devices. When the grace period expires with no successful attestation response, a device is considered out of compliance and is subject to the actions that you specify in the assigned compliance profile.
5. Click **Save**.

After you finish:

- In the activation profile, specify whether the attestation occurs during device activation and/or periodically. Managed device attestation applies to the MDM controls and the User privacy activation types, but not the User privacy - User enrollment activation type. When you select the User privacy activation type in the activation profile, you must select at least one of the management options (such as "Allow VPN management").
- In the compliance profile, select the "Managed device attestation failure" rule and specify the compliance actions that you want carried out against devices that fail attestation.
- In the management console, you can view a device's attestation status in the device details.

Configure attestation for Samsung Knox devices

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

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

1. In the management console, on the menu bar, click **Settings > General settings > Attestation**.
2. Select the **Enable periodic attestation challenges for KNOX Workspace devices** check box.

3. In the **Challenge frequency** section, specify how often the device must return an attestation response to UEM.
4. In the **Grace period** section, specify the grace period for devices. When the grace period expires with no successful attestation response, a device is considered out of compliance and is subject to the actions that you specify in the assigned compliance profile.
5. Click **Save**.

After you finish: In the compliance profile assigned to devices, enable the "Rooted OS or failed Knox attestation" rule and configure the actions that you want UEM to carry out when devices fail attestation.

Configure attestation for Windows 10 devices

When you enable attestation, BlackBerry UEM sends challenges to test the authenticity and integrity of Windows 10 devices. Note that the Windows 10 attestation settings do not apply to BlackBerry Desktop (BlackBerry Access + BlackBerry Work).

1. In the management console, on the menu bar, click **Settings > General settings > Attestation**.
2. Select **Enable periodic attestation challenges for Windows 10 devices** check box.
3. In the **Challenge frequency** section, specify how often the device must return an attestation response to UEM.
4. In the **Grace period** section, specify the grace period for devices. When the grace period expires with no successful attestation response, a device is considered out of compliance and is subject to the actions that you specify in the assigned compliance profile.
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

After you finish:

- In the compliance profile assigned to devices, configure the Windows device health attestation rules and configure the actions that you want UEM to carry out when devices fail attestation.
- In the management console, you can view a device's attestation status in the device details.

Set up Windows Information Protection for Windows 10 devices

You can set up Windows Information Protection (WIP) for Windows 10 devices to do the following:

- Separate personal and work data on devices.
- Wipe only work data on devices.
- 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 (for example, with 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. 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. 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 create and access work data only.

1. In the management console, on the menu bar, click **Policies and profiles > Protection > Windows Information Protection**.
2. Click +.
3. Type a name and description for the profile.
4. Configure the appropriate values for each profile setting. See Windows Information Protection profile settings.
5. Click **Add**.

After you finish:

- Assign the profile to users and groups.
- If necessary, rank the profile.

Windows Information Protection profile settings

rofile setting	Description
Windows Information Protection settings	This setting specifies whether Windows Information Protection is enabled and the level of enforcement. • Off: Data is not encrypted and audit logging is turned off. • Silent: Data is encrypted and any attempts to share protected data are logged. • Override: Data is encrypted, the user is prompted when they attempt to share protected data, and any attempts to share protected data are logged. • Block: Data is encrypted, users cannot share protected data, and any attempts to share protected data are logged.
Enterprise protected domain names	This setting specifies the work network domain names that your organization uses for its user identities. 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).

rofile setting	Description
Data recovery certificate file (.der, .cer)	This setting specifies the data recovery certificate file that you use to recover files that were locally protected on a device. The file must be a PEM encoded or DER encoded certificate with a .der or .cer file extension.
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.
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.
Enterprise internal proxy servers	This setting specifies the internal proxy servers that are used when connecting to work network locations. These proxy servers are used only 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.

<table>
<tr><th>rofile setting</th><th>Description</th></tr>
<tr><td>Enterprise network domain names</td><td>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.</td></tr>
<tr><td>Desktop app payload code</td><td>

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>
```

</td></tr>
</table>

<table>
<thead>
<tr><th>rofile setting</th><th>Description</th></tr>
</thead>
<tbody>
<tr><td>Universal Windows Platform app payload code</td><td>

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>
```

</td></tr>
<tr><td>Associated VPN profile</td><td>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."</td></tr>
<tr><td>Collect device audit logs</td><td>This setting specifies whether to collect device audit logs.</td></tr>
</tbody>
</table>

Move iOS or macOS devices to a hardened channel

When you activate iOS or macOS devices, by default, the devices are assigned to a hardened data channel. If you have any iOS or macOS devices that are not currently using a hardened channel, you can export a list of these devices and take action to move the devices to a hardened channel. When you move devices to a hardened channel, the devices must be reactivated.

If you move a device that is enrolled in Apple DEP, the device will lose the DEP enrollment configuration. Device users will need to factory reset the device and activate it with BlackBerry UEM again.

Before you begin: In the app settings for all applicable apps, clear the **Remove the app from the device when the device is removed from BlackBerry UEM** option. If you attempt to move devices to a hardened channel without clearing this option, the app is removed and the device may be unenrolled from UEM. Note that even if you clear this check box, an app may still be removed during the move if the setting has not been delivered to the device. For more information on tracking commands that are being delivered to a device, see KB 102688.

1. In the management console, on the menu bar, click **Settings > Migration > iOS Hardened Channel** or **Settings > Migration > macOS Hardened Channel**.

   If you do not see one of these menu options, your UEM environment does not have any iOS or macOS devices that need to be moved to a hardened channel.
2. Click **Export** to download a list of devices that are not currently using a hardened channel.
3. Do any of the following:

Task	Steps
Move multiple iOS devices to a hardened channel.	Click **Browse** and navigate to and select the file you downloaded in step 2. Devices that belong to shared device groups are included in the file for information purposes only, and will not be moved to a hardened channel with this method. For any devices that belong to shared device groups, the user must factory reset the device and activate it with UEM again. This method can process a maximum of 1000 entries at a time. If the file you downloaded contains more than 1000 entries, divide them into separate files that contain a maximum of 1000 entries each.
Move a specific iOS device to a hardened channel.	**a.** On the menu bar, click **Users > Managed devices**. **b.** Search for and click the iOS device. **c.** On the device tab, click **Migrate to iOS hardened channel**. **d.** Click **Submit**.
Move macOS devices to a hardened channel.	Contact device users and instruct them to reactivate their device with UEM Self-Service.

Legal notice

Patents, as applicable, identified at: www.blackberry.com/patents.

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada