CylancePROTECT

Overview and Administration Guide

Contents

What is CylancePROTECT? 5
What is CylanceINFINITY? 6
Architecture: CylancePROTECT 6

Software requirements: CylancePROTECT 9

Enable CylancePROTECT in your UEM domain 10

Detecting malware when deploying Android apps from BlackBerry UEM 11
Upload apps that you want to deploy using BlackBerry UEM 11
Add an app or signing certificate to the approved app list 11

Detecting malware on Android devices 13
Malware scanning behavior by activation type 13
Prerequisites to support malware detection on Android devices 14
Enable malware detection for Android devices 15
Add an app or signing certificate to the approved app list 16
Add an app or signing certificate to the restricted app list 17
Configure compliance actions to take when malware is detected 18

Detecting sideloaded apps on iOS devices 21
Enable sideload detection on iOS devices 21
Add a signing certificate to the approved app list 21
Configure compliance actions to take when a sideloaded app is detected 22

Safe browsing with BlackBerry Dynamics apps 23
Enable and configure safe browsing for BlackBerry Dynamics apps 23
Approve or block a domain 24

Checking the integrity of BlackBerry Dynamics apps for iOS 26
Considerations for enabling integrity checking for BlackBerry Dynamics apps 26
Add Apple DeviceCheck keys for custom BlackBerry Dynamics apps 26
Enable app integrity checking 27
Configure compliance actions to take when a device fails an integrity check 28

Using hardware certificate attestation for BlackBerry Dynamics apps on Android devices 29
Enable hardware certificate attestation for BlackBerry Dynamics apps 29

Configure the frequency of hardware certificate attestation..... 29
Configure compliance actions to take when a device fails attestation..... 30

Legal notice..... 31

What is CylancePROTECT?

CylancePROTECT is a suite of features that enhances BlackBerry UEM's ability to detect, prevent, and resolve security threats without disrupting the productivity of your workforce.

CylancePROTECT uses a combination of advanced technologies, including:

- The cloud-based CylanceINFINITY service that uses sophisticated AI and machine learning to identify malware and unsafe URLs
- The UEM server that provides a complete device management and compliance infrastructure for your organization
- BlackBerry apps that monitor and enforce security standards at the device and user level

The seamless integration of these technologies establishes a secure ecosystem where data is protected and malicious activities are identified at all endpoints and eliminated proactively.

The features are fully integrated into the existing components of the overall UEM server and device architecture, so no additional software footprint or user actions are required to benefit from CylancePROTECT. Your valuable data and resources are protected continuously without intruding on the daily activity of your device users.

Feature	Platform	Description
Malware detection for internally deployed apps	Android	When you upload a hosted app to UEM to deploy it to your users, UEM leverages CylanceINFINITY to scan the app and detect potential malware.
Detecting malware on devices	Android	The UEM Client or a BlackBerry Dynamics app uploads app files to CylanceINFINITY to identify whether malicious apps are present on a user's device. UEM takes a compliance action that you specify if malware is detected.
Detecting sideloaded apps	iOS	UEM, the UEM Client, and BlackBerry Work can detect sideloaded apps on iOS devices and take a compliance action that you specify.
Safe browsing with BlackBerry Dynamics apps	Android iOS	When a user navigates to a URL in a BlackBerry Dynamics app (for example, BlackBerry Access), the app sends the URL to CylanceINFINITY in real-time to determine if it is safe. You can choose the user experience when a user tries to navigate to an unsafe URL. For example, the app can permit access and log information, warn the user and give an option to continue, or block access.
App integrity checking	iOS	UEM can leverage the Apple DeviceCheck framework to verify the integrity of BlackBerry or ISV authored BlackBerry Dynamics apps. UEM also supports partial integrity checking for custom BlackBerry Dynamics apps, based on the Apple team ID that is associated with the app, without leveraging the DeviceCheck framework.
Hardware certificate attestation	Android	CylancePROTECT extends security patch level enforcement to BlackBerry Dynamics apps. If the security patch level is not satisfied, UEM takes a compliance action that you specify.

What is CylanceINFINITY?

CylanceINFINITY is a cloud-based platform that uses sophisticated AI and machine learning to determine whether software and websites are potentially malicious and a threat to the security of device endpoints in a UEM domain.

CylanceINFINITY is the evolution of traditional approaches towards cybersecurity, such as whitelisting or blacklisting, that are based on the classification of digital signatures and blind trust. As cyber threats have evolved in both scope and sophistication, the use of signatures as a foundation for threat detection and resolution is not as reliable as it used to be.

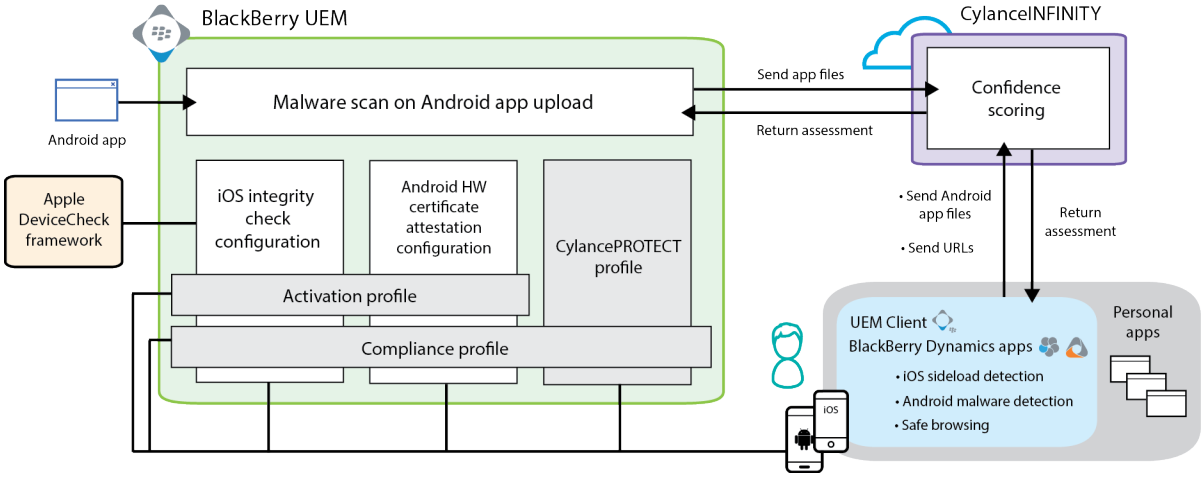
Instead of relying on signatures, the CylanceINFINITY service leverages advanced machine learning and efficient mathematical models to process large volumes of data from global sources, retains and continuously learns from the patterns and properties of that data, and uses that data to make intelligent predictions and decisions about the risk potential of software and URLs in near real-time. The design of CylanceINFINITY ensures that it will constantly evolve and train itself to address new cyber threats.

CylanceINFINITY is a core component of several CylancePROTECT features, including malware detection for internally deployed Android apps, malware detection on Android devices, and safe browsing. At its core, it enables an aggressive and proactive security strategy, identifying and blocking malicious software and websites before they can have any impact on your organization's infrastructure or device users.

The APK files that are uploaded to CylanceINFINITY are kept private and anonymous, with no links back to users, devices, or organizations. CylanceINFINITY does not store any user data. The app packages that are uploaded to CylanceINFINITY are never shared with a third party. The UEM connection to CylanceINFINITY is end-to-end TLS encrypted. For more details about Cylance privacy policies, see the Cylance Privacy Notice.

For more information about the design methodology of CylanceINFINITY, see the CylanceINFINITY White Paper.

Architecture: CylancePROTECT



Component	Description
BlackBerry UEM management console	Use the UEM management console to: • Scan hosted Android apps for malware when you upload the app files to UEM for deployment • Maintain a list of approved apps that are exempt from Android malware detection and iOS sideload detection • Maintain a list of approved and blocked domains for safe browsing • Enable and configure integrity checking for BlackBerry Dynamics apps on iOS devices • Enable and configure hardware certificate attestation for BlackBerry Dynamics apps on Android devices
CylancePROTECT profile	Create a CylancePROTECT profile and assign it to users to enable CylancePROTECT features on iOS and Android devices.
Activation profile	Create and assign a UEM activation profile to users to enable iOS integrity checking and Android hardware certificate attestation for BlackBerry Dynamics apps at activation time.
Compliance profile	Create and assign a UEM compliance profile to users to take the appropriate management actions when: • Malware is detected on an Android device • A sideloaded app is detected on an iOS device • A BlackBerry Dynamics app on an iOS device fails an integrity check • A BlackBerry Dynamics app on an Android device fails hardware certificate attestation
CylanceINFINITY	CylanceINFINITY is a cloud-based platform that uses sophisticated AI and machine learning to determine whether software and websites are potentially malicious and a threat to the security of device endpoints in a UEM domain. When you upload an Android app that you want to deploy with UEM, UEM sends the app files to CylanceINFINITY for analysis and risk assessment. CylanceINFINITY returns a confidence score that identifies the app as safe or as malware. The UEM Client and BlackBerry Dynamics apps on Android devices send app files to CylanceINFINITY for analysis and risk assessment. CylanceINFINITY returns a confidence score that identifies the app as safe or as malware. When a user navigates to a URL in a BlackBerry Dynamics app, the app sends the URL to CylanceINFINITY in real-time to determine if it is safe. You can choose the user experience when a user tries to navigate to an unsafe URL.
Apple DeviceCheck framework	The iOS integrity check feature allows you to leverage the Apple DeviceCheck framework to periodically verify the integrity of BlackBerry Dynamics apps on users' iOS devices.

Component	Description
BlackBerry UEM Client and BlackBerry Dynamics apps	UEM communicates with the UEM Client on a user's device to apply configuration settings and profiles. BlackBerry Dynamics apps are productivity apps that give users secure access to work resources. The BlackBerry Dynamics SDK and the CylancePROTECT library are integrated with the UEM Client and BlackBerry Dynamics apps, supporting additional functionality that allows these apps to detect malware on Android devices, sideloaded apps on iOS devices (UEM Client and BlackBerry Work only), and unsafe URLs when using BlackBerry Access and other BlackBerry Dynamics apps.

Software requirements: CylancePROTECT

Requirement	Description
BlackBerry UEM	CylancePROTECT is supported in: • BlackBerry UEM Cloud • BlackBerry UEM version 12.12 MR1 or later See the UEM Planning and Installation content for planning information, software requirements, and installation or upgrade instructions. You must purchase CylancePROTECT licenses to enable the service for users in your organization's UEM domain. Contact your BlackBerry representative or complete a contact form for more information. After you install UEM and BlackBerry applies the licenses, Enable CylancePROTECT in your UEM domain.
Network requirements	Some CylancePROTECT features require a secure, direct connection from devices to the CylanceINFINITY cloud service. If devices are connected to your organization's Wi-Fi network, your network configuration must allow connections to **score.cylance.com:443**.
BlackBerry UEM Client and BlackBerry Dynamics apps	To support CylancePROTECT features, install the following versions of BlackBerry apps on users' devices: • BlackBerry UEM Client version 12.36.1 or later for Android, version 12.42.2716 or later for iOS • BlackBerry Work version 3.1 or later • BlackBerry Tasks version 3.1 or later • BlackBerry Notes version 3.1 or later • BlackBerry Connect version 3.1 or later • BlackBerry Access version 3.0.1 or later for Android, 3.0.2 or later for iOS To ensure the proper compliance enforcement for CylancePROTECT features (for example, blocking BlackBerry Dynamics apps until compliance is restored), you must upgrade all BlackBerry Dynamics apps to the versions listed above.

Enable CylancePROTECT in your UEM domain

Before you begin: Contact your BlackBerry representative to purchase CylancePROTECT licenses. After BlackBerry adds the licenses for your organization, complete the steps below.

1. In the management console, on the menu bar, click **Settings > Services**.
2. Locate the CylancePROTECT service in the table and click **Enable**.
3. When you are prompted, click **Enable**.

After you finish:

- Log out of the management console and log in again with the same administrator account.
- If you disable the CylancePROTECT service, devices are no longer protected with CylancePROTECT. After you disable the service, all CylancePROTECT profiles and settings are removed from the management console.

Detecting malware when deploying Android apps from BlackBerry UEM

You can use BlackBerry UEM to distribute hosted Android apps to users' devices. CylancePROTECT adds a new layer of security to this feature by giving UEM the ability to scan hosted Android apps (.apk) that are uploaded to UEM to detect potential malware.

When you upload an app to the management console, the app hash is sent to CylanceINFINITY. If CylanceINFINITY does not recognize the hash because it has not analyzed the app previously, the app files are uploaded. CylanceINFINITY analyzes the app files and generates a confidence score that it returns to UEM.

The app appears in the app list while the scan is in progress. If the app is not identified as malware, it remains on the app list. If the app is identified as malware, the app is automatically removed from the app list. If an app is assigned to a user or group while the scan is in progress, it will not be sent to devices until the scan is complete.

CylanceINFINITY retains app binaries and a corresponding confidence score for security purposes. The confidence score for an app can change if the same app is processed again. Whenever you upload a new version of an app, UEM sends the app files to CylanceINFINITY for analysis and scoring.

Upload apps that you want to deploy using BlackBerry UEM

Malware scanning for Android apps that you upload to the management console is enabled by default. If you want to turn off this feature, on the menu bar, navigate to **Settings > CylanceProtect**, clear the **Enable malware scanning for apps uploaded to UEM** check box, and click **Save**.

When the feature is enabled, UEM will automatically perform a malware scan on any Android app (including custom BlackBerry Dynamics apps) that you upload to the management console. No additional steps are required. If you want to prevent UEM from performing malware scanning for a specific app or for all apps that use a developer's signing certificate, see Add an app or signing certificate to the approved app list.

After you upload an app, you can open the app details (Android tab) to view the status of the malware scan. An app that has been scanned and determined to be safe has a status of "Verified safe". An app has a status of "Unverified" if it has not been scanned, either because the feature was disabled, the app was on the approved app list, or the app was uploaded before the upgrade to UEM version 12.12 or before the UEM Cloud update that added support for CylancePROTECT. If a scan is in progress for a BlackBerry Dynamics app, the status is "Scanning". For apps with an Unverified state, you can initiate a malware scan by uploading the app again.

After an app has been scanned, you receive a notification with information about whether the app was identified as malware and whether it has been added to UEM.

For more information about deploying internal apps from UEM, see Steps to add internal apps to the app list in the UEM Administration content.

Add an app or signing certificate to the approved app list

To prevent UEM from performing malware scanning for a specific Android app or for all apps that use a developer's signing certificate, you can add the app or certificate to the approved app list. Note that all apps on the approved app list are also exempt from malware scanning on Android devices.

You cannot add apps or app certificates that have already been added to the restricted app list.

1. In the management console, on the menu bar, click **Settings > CylancePROTECT > Approved apps**.
2. Click ✎.

3. Do one of the following:

Task	Steps
Add an app to the approved app list	**a.** On the **Approved apps** tab, click +. **b.** Do one of the following: • To select an app file, click **Select an app file**. Click **Browse** and navigate to and select the .apk file. Click **Upload**. • To manually enter the app information, click **Manually enter the app's hash info**. Specify the app details. Click **Add**. **Note:** If an app contains multiple .apk files, you must upload each .apk file or manually enter the hash of each file. Optionally, you can add the app's signing certificate (see the following row) instead of uploading or specifying the hash of each file.
Add a signing certificate to the approved app list	**a.** On the **Approved developers** tab, click +. **b.** Do one of the following: • To add the signing certificate from an app file, click **Select an app for certificate information**. Click **Browse** and navigate to and select the .apk file. Click **Upload**. • To manually enter the certificate information, click **Manually enter certificate information**. Specify the certificate details (in the **OS** drop-down list, click **Android**). When generating the apk hash or certificate thumbprint, use SHA256 hashing algorithms. Click **Add**.

4. Repeat step 3 as necessary to add additional apps or signing certificates to the approved app list.
5. Click **Save**.

Detecting malware on Android devices

CylancePROTECT enables the UEM Client and BlackBerry Dynamics apps to detect malware on Android devices and to enforce a compliance action until the malware is removed. For example, UEM can prevent all BlackBerry Dynamics apps on the device from running until the malicious app is removed from the user's device.

The UEM Client and BlackBerry Dynamics apps include the BlackBerry Dynamics SDK and the CylancePROTECT library. These apps use these technologies to scan the work and personal apps on a user's Android device and upload the app files to the CylanceINFINITY cloud service. Whether the scan is initiated by the UEM Client or a specific BlackBerry Dynamics app depends on the device activation type and authentication delegate configured in the BlackBerry Dynamics profile. CylanceINFINITY uses AI and machine learning to analyze the app package and produce a confidence score that it returns to the UEM Client or the BlackBerry Dynamics app. The confidence score indicates whether the app is safe or potentially malicious.

If the device has one or more malicious apps and "Malicious app package detected" is enabled in the compliance profile, UEM considers the device to be out of compliance, and the UEM Client or BlackBerry Dynamics app take the management action that is configured in the user's compliance profile.

An app is uploaded to CylanceINFINITY if it has a hash that CylanceINFINITY has not processed previously. Whenever an app has a new hash (for example, for a new version) the app is uploaded to CylanceINFINITY for analysis and scoring (if it has not already been uploaded from another device).

This feature applies to the Android Enterprise, Samsung Knox, MDM controls, and User privacy activation types.

Malware scanning behavior by activation type

The scope of the malware scan depends on the user's activation type:

Activation type	Scope of malware scanning
Android Enterprise: Work and personal - user privacy (Android Enterprise with work profile)	• Apps in the work profile only
Android Enterprise: Work and personal - full control (Android Enterprise fully managed device with work profile)	• Apps in the work profile only
Android Enterprise: Work space only (Android Enterprise fully managed device)	• All apps on the device
MDM controls	• All apps on the device (work and personal)

Activation type	Scope of malware scanning
User privacy	• All apps on the device (work and personal) • The UEM Client or a BlackBerry Dynamics app must be installed on the device • The user is prompted with a request to allow malware scanning on the device. If the user does not accept, malware scanning does not occur and the user's device is considered out of compliance.
Samsung Knox (all types)	• Apps in the Knox work space only

Note: For user privacy activation types, the name, package name, and hash of malicious apps are partially obfuscated in the management console, UEM logs, and device logs for privacy purposes. For fully managed devices, you can view the full details of malicious apps in the management console. For more information about data collection for different activation types, visit support.blackberry.com/community to read article 60890 (note that you require a BlackBerry Online Account and an active support entitlement to view KB articles).

Prerequisites to support malware detection on Android devices

- Install the UEM Client and/or BlackBerry Dynamics apps on users' devices (see the software requirements). Whether the malware scan is initiated by the UEM Client or a specific BlackBerry Dynamics app depends on the device activation type and the authentication delegate configured in the BlackBerry Dynamics profile.
- The following settings are recommended based on device activation types:

Activation type	Recommended settings
Android Enterprise	In the BlackBerry Dynamics profile that is assigned to users: • Enable "Enable UEM Client to enroll in BlackBerry Dynamics". This setting is enabled by default in new BlackBerry Dynamics profiles that you create. • Enable "Do not require password" for Android devices. This allows the UEM Client to run malware scanning in the background without prompting the user for a BlackBerry Dynamics password. • Configure the UEM Client as the authentication delegate. If malware is detected and the configured compliance action is to prevent BlackBerry Dynamics apps from running, the UEM Client can block all BlackBerry Dynamics apps until compliance is restored. Note that for this activation type, malware scanning is always performed by the UEM Client.
Samsung Knox	In the BlackBerry Dynamics profile that is assigned to users, configure a BlackBerry Dynamics app that runs in the work space as the authentication delegate. This enables one BlackBerry Dynamics app to manage authentication, malware scanning, and compliance enforcement on behalf of all BlackBerry Dynamics apps.

Activation type	Recommended settings
MDM controls	In the BlackBerry Dynamics profile that is assigned to users: • Enable "Enable UEM Client to enroll in BlackBerry Dynamics". This setting is enabled by default in new BlackBerry Dynamics profiles that you create. • In the BlackBerry Dynamics profile that is assigned to users, configure the UEM Client as the authentication delegate. This enables the UEM Client to manage malware scanning and compliance enforcement on behalf of all BlackBerry Dynamics apps. This configuration is not required if no BlackBerry Dynamics apps (aside from the UEM Client) are installed on a device. Note that with this activation type, device-level compliance actions (for example, Untrust) are not applicable. Compliance actions for BlackBerry Dynamics apps are applicable.
User privacy	In the BlackBerry Dynamics profile that is assigned to users: • Enable "Enable UEM Client to enroll in BlackBerry Dynamics". This setting is enabled by default in new BlackBerry Dynamics profiles that you create. • Verify that “Do not require password” for Android devices is not enabled, for security purposes. Notify users that they will have to specify a BlackBerry Dynamics password when prompted. • Configure the UEM Client or a specific BlackBerry Dynamics app as the authentication delegate. The UEM Client is recommended because it can run in the background. The authentication delegate can authenticate any BlackBerry Dynamics app on the device and will manage malware scanning on behalf of all BlackBerry Dynamics apps. If malware is detected and the configured compliance action is to prevent BlackBerry Dynamics apps from running, the authentication delegate can block all BlackBerry Dynamics apps until compliance is restored. • If you do not configure an authentication delegate, malware scanning will be performed by the UEM Client and each BlackBerry Dynamics app, which can consume device resources.
Device registration for BlackBerry 2FA only	Malware scanning is not applicable to this activation type.

Enable malware detection for Android devices

Before you begin: Verify that you've met the prerequisites to support malware detection on Android devices.

1. In the management console, on the menu bar, click **Policies and profiles > Protection > CylancePROTECT**.
2. Create a new CylancePROTECT profile or select and edit an existing CylancePROTECT profile.
3. On the **Android** tab, in the **Malicious app package detection** section, verify that the **Scan new and existing app packages from device for safety check** check box is selected.
4. To exempt apps on the approved app list from malware scanning, verify that the **Always allow apps in approved app list** check box is selected.

You can view the approved app list in the management console at Settings > CylancePROTECT > Approved apps.

5. To block apps that you added to the restricted apps list, verify that the **Always block apps in restricted app list** check box is selected.

   You can view the restricted app list in the management console at Settings > CylancePROTECT > Restricted apps.
6. If you want to scan system apps, verify that the **Scan system apps** check box is selected.

   System apps are preinstalled in the system partition on a user's device.
7. Under **Upload app packages for safety check over a Wi-Fi connection**, specify the following:

   - The maximum size, in MB, of an app that can be uploaded to CylanceINFINITY.
   - The maximum size, in MB, of all apps that can be uploaded to CylanceINFINITY in a month (30 days).

   A value of 0 means there is no limit. If the maximum app size or monthly maximum would be exceeded, the upload does not occur and an error is added to the device log.
8. If you want to allow the UEM Client or a BlackBerry Dynamics app to upload app packages to CylanceINFINITY over a mobile network connection, select the **Upload app packages for safety check over a mobile network connection** check box. Specify the following:

   - The maximum size, in MB, of an app that can be uploaded to CylanceINFINITY.
   - The maximum size, in MB, of all apps that can be uploaded to CylanceINFINITY in a month (30 days).

   A value of 0 means there is no limit. If the maximum app size or monthly maximum would be exceeded, the upload does not occur and an error is added to the device log.
9. Click **Save**.

After you finish:

- Assign the profile to users and groups. Instruct users to open the authentication delegate app (the UEM Client or a BlackBerry Dynamics app) to initiate the malware scanning process for the first time. After the initial acceptance, malware scanning occurs in the background and is invisible to users.
- Optionally, you can add apps or signing certificates to the approved app list to prevent malware scanning for those apps.
- Optionally, you can add apps or signing certificates to the restricted app list to identify specific apps as malware without requiring a malware scan.
- Configure compliance actions to take when malware is detected.

Add an app or signing certificate to the approved app list

To prevent malware scanning for a specific Android app or for all apps that use a developer's signing certificate, you can add the app or certificate to the approved app list. If you added an app or certificate to the approved app list for malware detection for internally deployed Android apps, those apps are exempt from malware scanning on Android devices.

You cannot add apps or app certificates that have already been added to the restricted app list.

1. In the management console, on the menu bar, click **Settings > CylancePROTECT > Approved apps**.
2. Click ✎.
3. Do one of the following:

Task	Steps
Add an app to the approved app list	**a.** On the **Approved apps** tab, click +. **b.** Do one of the following: • To select an app file, click **Select an app file**. Click **Browse** and navigate to and select the .apk file. Click **Upload**. • To manually enter the app information, click **Manually enter the app's hash info**. Specify the app details. Click **Add**. **Note:** If an app contains multiple .apk files, you must upload each .apk file or manually enter the hash of each file. Optionally, you can add the app's signing certificate (see the following row) instead of uploading or specifying the hash of each file.
Add a signing certificate to the approved app list	**a.** On the **Approved developers** tab, click +. **b.** Do one of the following: • To add the signing certificate from an app file, click **Select an app for certificate information**. Click **Browse** and navigate to and select the .apk file. Click **Upload**. • To manually enter the certificate information, click **Manually enter certificate information**. Specify the certificate details (in the **OS** drop-down list, click **Android**). Click **Add**.

4. Repeat step 3 as necessary to add additional apps or signing certificates to the approved app list.
5. Click **Save**.

Add an app or signing certificate to the restricted app list

To identify a specific Android app or all apps that use a developer's signing certificate as malware without sending the files to CylanceINFINITY for scanning, you can add the app or certificate to the restricted app list.

You cannot add apps or app certificates that have already been added to the approved app list.

1. In the management console, on the menu bar, click **Settings > CylancePROTECT > Restricted apps**.
2. Do one of the following:

Task	Steps
Add an app to the restricted app list	**a.** On the **Restricted apps** tab, click +. **b.** Do one of the following: • To select an app file, click **Select an app file**. Click **Browse** and navigate to and select the .apk file. Click **Upload**. • To manually enter the app information, click **Manually enter the app's hash info**. Specify the app details. Click **Save**. **Note:** If an app contains multiple .apk files, you must upload each .apk file or manually enter the hash of each file. Optionally, you can add the app's signing certificate (see the following row) instead of uploading or specifying the hash of each file.

Task	Steps
Add a signing certificate to the restricted app list	**a.** On the **Restricted developers** tab, click +. **b.** Do one of the following: • To add the signing certificate from an app file, click **Select an app for certificate information**. Click **Browse** and navigate to and select the .apk file. Click **Upload**. • To manually enter the certificate information, click **Manually enter certificate information**. Specify the certificate details. Click **Save**.

3. Repeat step 3 as necessary to add additional apps or signing certificates to the restricted app list.
4. Click **Save**.

Configure compliance actions to take when malware is detected

When malware is detected on a user's device, UEM considers the device to be out of compliance. You can configure and assign a compliance profile to users so that UEM can take the appropriate action. For more information about creating and configuring compliance profiles, see Enforcing compliance rules for devices in the UEM Administration content.

When you first implement malware detection, it is recommended to use the monitor and log option before you implement actions that are potentially more disruptive. After monitoring compliance activity for an appropriate amount of time, you can then implement the desired actions (for example, preventing users from using BlackBerry Dynamics apps until the device is compliant).

Note: If the UEM Client or the BlackBerry Dynamics app that performs malware scanning is a version that was released in February or March 2020 but does not meet the latest CylancePROTECT software requirements, note the following:

- System apps are scanned by default on the user's device regardless of the "Scan system apps" setting in the CylancePROTECT profile.
- The "Malicious app package detected" compliance settings apply to both system apps and non-system apps.
- The "Malicious system app detected" compliance settings are not applicable.

Before you begin: Enable malware detection for Android devices.

1. In the management console, on the menu bar, click **Policies and profiles > Compliance > Compliance**.
2. Create a new compliance profile or select and edit an existing compliance profile.
3. On the **Android** tab, in the **CylancePROTECT** section, do any of the following:

Task	Steps
Configure the actions for system apps that are identified as malware	**a.** Select the **Malicious system app detected** check box. **b.** Configure the prompt settings. **c.** In the **Enforcement action for device** drop-down list, choose one of the following: • To log information about the compliance issue without taking a compliance action, click **Monitor and log**. • To prevent the user from accessing work resources and apps on the device while it is out of compliance, click **Untrust**. Note that this option does not impact BlackBerry Dynamics apps. Data and apps are not deleted from the device. **d.** In the **Enforcement action for BlackBerry Dynamics apps** drop-down list, choose one of the following options: • To log information about the compliance issue without taking a compliance action for BlackBerry Dynamics apps, click **Monitor and log**. • To prevent the user from accessing BlackBerry Dynamics apps while the device is out of compliance, click **Do not allow BlackBerry Dynamics apps to run**.
Configure the actions for non-system apps that are identified as malware	**a.** Select the **Malicious app package detected** check box. **b.** Configure the prompt settings (behavior, method, count, and interval). **c.** In the **Enforcement action for device** drop-down list, choose one of the following: • To log information about the compliance issue without taking a compliance action, click **Monitor and log**. • To prevent the user from accessing work resources and apps on the device while it is out of compliance, click **Untrust**. Note that this option does not impact BlackBerry Dynamics apps. Data and apps are not deleted from the device. **d.** In the **Enforcement action for BlackBerry Dynamics apps** drop-down list, choose one of the following options: • To log information about the compliance issue without taking a compliance action for BlackBerry Dynamics apps, click **Monitor and log**. • To prevent the user from accessing BlackBerry Dynamics apps while the device is out of compliance, click **Do not allow BlackBerry Dynamics apps to run**.

4. Click **Add** or **Save**.

After you finish:

- Assign the profile to users and groups.
- Optionally, configure event notifications so that when a malware app is detected on a user's device, administrators receive an email notification that identifies the user and the malware app. If the user removes the malware app from the device, or if the app is no longer considered to be malware (for example, it was added to the approved app list), UEM sends another notification.

- You can view information about compliance violations on the Managed devices screen (filter by compliance violations) or in a user's device details.

Detecting sideloaded apps on iOS devices

Sideloaded apps represent a potential security threat because they don't follow the same restrictions or protections as apps distributed through the App Store or deployed internally from UEM.

CylancePROTECT enables the UEM server, the UEM Client, and BlackBerry Work to detect the presence of sideloaded apps on users' iOS devices. The UEM server can detect sideloaded apps on devices with the MDM controls activation type. The UEM Client and BlackBerry Work can detect sideloaded apps on devices with any activation type.

For devices with the MDM controls activation type, when you use the management console to view details about the apps installed on the user's device, a new Source column indicates whether the app was installed from the App Store, TestFlight (for beta apps), or UEM, or if the app was sideloaded.

When a sideloaded app is detected, UEM considers the device to be out of compliance. You can configure and assign a compliance profile to users so that UEM can take an appropriate management action when a sideloaded app is detected. For example, you can prevent BlackBerry Dynamics apps from running on the device until the sideloaded app is removed and the device returns to compliance.

Apps that you upload to the management console and add to the app list are approved automatically (regardless of whether you have deployed the app from UEM) and do not cause compliance violations.

Enable sideload detection on iOS devices

To enable sideload detection for iOS devices, you must create and assign a CylancePROTECT profile to users. Note that currently there are no additional settings that you need to configure in the profile.

If you have already created and assigned a CylancePROTECT profile to enable and configure other CylancePROTECT features, sideload detection is already enabled for those users. You can assign the same profile to additional user accounts.

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

After you finish:

- Assign the profile to users and groups.
- Optionally, create an event notification for when a sideloaded app is detected on a device.
- Configure compliance actions to take when a sideloaded app is detected.

Add a signing certificate to the approved app list

To prevent sideload detection for all apps that use a developer's signing certificate, you can add the certificate to the approved app list. Note that all apps that you upload to the management console are approved automatically (regardless of whether you have deployed the app from UEM) and do not cause compliance violations.

1. In the management console, on the menu bar, click **Settings > CylancePROTECT > Approved apps**.
2. Click ✎.
3. On the **Approved developers** tab, click +.
4. Click **Manually enter certificate information**.

5. In the **OS** drop-down list, click **iOS**.
6. Specify the certificate details.
7. Click **Add**.
8. Repeat steps 3 to 7 to add additional signing certificates to the approved app list.
9. Click **Save**.

Configure compliance actions to take when a sideloaded app is detected

When a sideloaded app is detected on a user's device, UEM considers the device to be out of compliance. You can configure and assign a compliance profile to users so that UEM can take the appropriate action. For more information about creating and configuring compliance profiles, see Enforcing compliance rules for devices in the UEM Administration content.

When you first implement sideload detection, it is recommended to use the monitor and log option before you implement actions that are potentially more disruptive. After monitoring compliance activity for an appropriate amount of time, you can then implement the desired actions (for example, preventing users from using BlackBerry Dynamics apps until the device is compliant).

Before you begin: Enable sideload detection on iOS devices.

1. In the management console, on the menu bar, click **Policies and profiles > Compliance > Compliance**.
2. Create a new compliance profile or select and edit an existing compliance profile.
3. On the **iOS** tab, in the **CylancePROTECT** section, select the **Sideloaded app is installed** check box.
4. Configure the prompt settings (behavior, method, count, and interval) as desired.
5. In the **Enforcement action for device** drop-down list, choose one of the following:
   - To log information about the compliance issue without taking a compliance action, click **Monitor and log**.
   - To prevent the user from accessing work resources and apps on the device while it is out of compliance, click **Untrust**. Note that this option does not impact BlackBerry Dynamics apps. Data and apps are not deleted from the device.
6. In the **Enforcement action for BlackBerry Dynamics apps** drop-down list, choose one of the following options:
   - To log information about the compliance issue without taking a compliance action for BlackBerry Dynamics apps, click **Monitor and log**.
   - To prevent the user from accessing BlackBerry Dynamics apps while the device is out of compliance, click **Do not allow BlackBerry Dynamics apps to run**.
7. Click **Add** or **Save**.

After you finish:

- Assign the profile to users and groups.
- Optionally, configure event notifications so that when a sideloaded app is detected on a user's device, administrators receive an email notification that identifies the user, sideloaded apps, and trusted developers on the device. If the sideloaded apps on the device change (for example, it is removed from the device or added to the approved apps list) UEM sends another notification.
- In the management console, you can view information about compliance violations on the Managed devices screen (filter by compliance violations) or in a user's device details.

Safe browsing with BlackBerry Dynamics apps

CylancePROTECT allows your organization to leverage the real-time risk assessment capabilities of CylanceINFINITY to protect BlackBerry Dynamics app users from malicious websites, phishing attempts, malware, adware, and other web sources that pose a threat to your valuable data.

When a user tries to navigate to a website or open a web link in a BlackBerry Dynamics app, the unaltered URL is sent to CylanceINFINITY in real-time. CylanceINFINITY uses advanced machine-learning capabilities and accumulated knowledge from threat intelligence feeds to provide an instant assessment of the safety of the URL. The CylancePROTECT library that is embedded in the UEM Client and BlackBerry Dynamics apps on the device also leverages local machine learning models to identify unsafe URLs. If the CylancePROTECT library cannot use CylanceINFINITY for URL scoring, the local machine learning models are used automatically. This ensures a secure browsing experience regardless of the device's current context or network connectivity.

You have full control over the user experience in the BlackBerry Dynamics app when an unsafe URL is detected: you can allow the user to proceed and log information, you can provide a warning and give the user the option to continue, or you can block access to the URL.

You can also add specific domains to the approved list or blocked list in the management console. A BlackBerry Dynamics app will check a URL against the approved domains list and the blocked domains list before sending it to CylanceINFINITY or using local machine learning models.

The BlackBerry Dynamics app keeps a local cache of the recent URLs that have been assessed and uses the cached evaluation (safe or unsafe) if the user tries to access the URL again. Each URL in the cache expires after 7 days or after the user restarts the device. The cache is unique to each BlackBerry Dynamics app and is not shared between apps.

When the user chooses to proceed to a URL after they receive a warning, that URL is also stored in a local cache. If the user tries to navigate to that URL again while it is cached, access is allowed without a warning. These URLs are removed from the cache when the user closes the app.

Note: CylanceINFINITY collects plain text URLs for analysis and risk assessment. No additional metadata or user identifiers are collected or stored with the URL. The URLs are never shared with a third party or used by BlackBerry for any purpose other than providing a safe browsing experience to BlackBerry customers. For more information about Cylance privacy policies, see the Cylance Privacy Notice.

Enable and configure safe browsing for BlackBerry Dynamics apps

By default, safe browsing protection is enabled for BlackBerry Access, BlackBerry Work, BlackBerry Tasks, and BlackBerry Connect. You must assign a CylancePROTECT profile to user accounts to enable the feature on users' devices.

Before you begin:

- Check the software requirements to verify that the required versions of BlackBerry Dynamics apps are installed on users' devices.
- To extend safe browsing to other BlackBerry Dynamics apps, in **Settings > CylancePROTECT > Safe browsing**, on the **Protected BlackBerry Dynamics apps** tab, edit the list to add additional apps.

1. In the management console, on the menu bar, click **Policies and profiles > Protection > CylancePROTECT**.
2. Create a new CylancePROTECT profile or select and edit an existing CylancePROTECT profile.
3. Select the **iOS** or **Android** tab to configure safe browsing for that platform.
4. Verify that the **Check for unsafe web resources within the BlackBerry Dynamics apps** check box is selected.
5. In the **Action for unsafe web resources** drop-down list, choose one of the following:

- To take no action and log information, click **Monitor and log**.
- To block access to unsafe URLs, click **Block**.

6. In the **Scanning option** drop-down list, choose one of the following:
   - If you want BlackBerry Dynamics apps to send URLs to CylanceINFINITY to determine if they are safe, click **Cloud scanning**.
   - If you want to use only the local machine learning models of the CylancePROTECT library to identify unsafe URLs, click **On device scanning**.
   - If you want to disable URL scanning, click **No scanning**.

   The approved and blocked domains that you configure are enforced regardless of the option that you choose.
7. If you selected cloud or on-device scanning, and you want to give the user a warning and the option to proceed when a URL has been identified as unsafe, select the **Allow users to override blocked resources and enable access to the requested domain** check box.

   Note that users cannot choose to proceed to a URL in a blocked domain. This bypass feature does not apply to sub-resource URLs.
8. If necessary, repeat steps 3 to 7 to configure safe browsing for the remaining OS platform.
9. Click **Save**.

After you finish:

- Assign the profile to users and groups.
- Optionally, approve or block web domains.

Approve or block a domain

You can add domains to the approved domains list if you want websites in those domains to be considered safe. You can add domains to the blocked domains list to prevent users from accessing any websites in those domains. If a domain is on both lists, the approved list takes precedence.

1. In the management console, on the menu bar, click **Settings > CylancePROTECT > Safe browsing**.
2. Click ✎.
3. Do any of the following:

Task	Steps
Approve a domain	**a.** On the **Approved domains** tab, click +. **b.** In the **Domain name** field, type the domain. BlackBerry Dynamics apps will look for an exact match with the last portion of the authority in the domain (for example, example.net will match www.example.net and another.example.net, but not thisexample.net). Wildcard characters such as * and ? are not valid. **c.** In the **Description** field, type a description of the approved domain. **d.** Repeat the previous steps to add additional domains.

Task	Steps
Block a domain	**a.** On the **Blocked domains** tab, click +. **b.** In the **Domain name** field, type the domain. BlackBerry Dynamics apps will look for an exact match with the last portion of the authority in the domain (for example, example.net will match www.example.net and another.example.net, but not thisexample.net). Wildcard characters such as * and ? are not valid. **c.** In the **Description** field, type a description of the blocked domain. **d.** Repeat the previous steps to add additional domains.

4. Click **Save**.

Checking the integrity of BlackBerry Dynamics apps for iOS

CylancePROTECT allows you to leverage the Apple DeviceCheck framework to periodically verify the integrity of BlackBerry Dynamics apps on your users' iOS devices. The DeviceCheck framework verifies that the app is running on a valid Apple device and is signed with the developer's signing key. This feature applies to BlackBerry Dynamics apps that are released by BlackBerry and custom BlackBerry Dynamics apps that your organization or an ISV has developed using the BlackBerry Dynamics SDK and published to the App Store.

UEM also supports a partial integrity check for custom BlackBerry Dynamics apps, based on the Apple team ID that is associated with the app, without leveraging the DeviceCheck framework.

This feature applies to all iOS activation types.

Considerations for enabling integrity checking for BlackBerry Dynamics apps

- Integrity checking for BlackBerry Dynamics apps is supported for iOS 11 and later.
- Full integrity checking leverages the Apple DeviceCheck framework and is supported for custom BlackBerry Dynamics apps that are published to the App Store. You cannot use full integrity checking for apps that are distributed using the Apple Enterprise Distribution program.
- Partial integrity checking uses the Apple team ID without leveraging the Apple DeviceCheck framework and is supported for BlackBerry Dynamics apps that are distributed using the Apple Enterprise Distribution program.
- The BlackBerry UEM Client is not required for app integrity checking.
- If you enable the "Perform app integrity check on BlackBerry Dynamics app activation" option in an activation profile and configure integrity checking for BlackBerry Dynamics apps, those apps require the BlackBerry Dynamics SDK version 6.0 or later. Activation will fail if the apps use an earlier version of the SDK. All of the BlackBerry Dynamics apps released by BlackBerry in July 2019 or later have the required version of the SDK.
- If a BlackBerry Dynamics app with SDK version 5.0 or earlier is already activated, and you enable "Perform periodic app integrity checks" in the activation profile, the app will fail the periodic attestation check and UEM will take the compliance action specified in the user's compliance profile.
- If the time on the device is incorrect, UEM might not recognize integrity check responses from BlackBerry Dynamics apps as valid. If the time on the device is not corrected, UEM considers the device to be out of compliance after the grace period expires.

Add Apple DeviceCheck keys for custom BlackBerry Dynamics apps

To enable app integrity checking for a custom BlackBerry Dynamics app that your organization or an ISV has developed and published to the App Store, you must add the app's DeviceCheck key in the UEM management console. After you add the key, you can add the app to the attestation list.

You do not need to add a key for apps released by BlackBerry. UEM will automatically use BlackBerry's own DeviceCheck key when you add a BlackBerry app to the attestation list (see Enable app integrity checking).

1. In the management console, click **Settings > General settings > Attestation**.
2. In the **iOS app integrity check frequency** section, in the **Apple DeviceCheck keys** table, click **+**.
3. In the **DeviceCheck key name** field, type a name for the key.

4. In the **Apple team ID** field, type your team ID. For more information, see "Locate your Team ID" in the Apple Developer Portal.

   If you want a partial integrity check that does not use the Apple DeviceCheck framework, you can skip step 5.
5. If you want to verify that the app is running on a valid Apple device and is signed with the developer's signing key, select the **Use Apple DeviceCheck to validate device and app signature** check box. Do the following:
   a) In the **Key ID** field, type the key ID. For more information, see "Create a DeviceCheck private key" in the Apple Developer Portal.
   b) In the **DeviceCheck key file** field, click browse and navigate to the key file.
6. Click **Add**.
7. Click **Save**.

After you finish: Enable app integrity checking

Enable app integrity checking

Before you begin:

- If applicable, Add Apple DeviceCheck keys for custom BlackBerry Dynamics apps.
- In the activation profiles that are assigned to users, on the **iOS** tab, enable any of the following settings:
  - To perform an app integrity check when a BlackBerry Dynamics app is activated, select **Perform app integrity check on BlackBerry Dynamics app activation**.
  - To perform regular app integrity checks for BlackBerry Dynamics apps, select **Perform periodic app integrity checks**.

1. In the management console, click **Settings > General settings > Attestation**.
2. In the **iOS app integrity check frequency** section, select the **Enable iOS app integrity check on devices** check box.
3. In the **Challenge frequency** section, specify how often apps must return an attestation response.
4. In the **App grace period** section, specify a grace period.

   If the grace period expires without a successful attestation response, a device is considered out of compliance and UEM will take the compliance action specified in the user's compliance profile.
5. In the **Apps to receive attestation challenges** table, click **+**.
6. To use a full integrity check with the DeviceCheck framework, verify that the **Use Apple DeviceCheck to validate device and app signature** check box is selected. For a partial integrity check, clear the check box.
7. If you want to add a custom app to the attestation list, in the **DeviceCheck key name** drop-down list, select the key for the app.
8. Search for and select the app that you want to receive attestation challenges. Click **Select**. You do not need to add a key for apps released by BlackBerry. UEM will automatically use the BlackBerry DeviceCheck key when you select an app released by BlackBerry.
9. Repeat steps 5 to 8 to add additional apps to the list.
10. Click **Save**.
11. Create a CylancePROTECT profile and assign it to user accounts and groups to enable the feature on users' devices. You can create a new CylancePROTECT profile (Policies and profiles > Protection > CylancePROTECT) or use a CylancePROTECT profile that you created previously. Note that currently there are no settings that you need to configure in the profile for integrity checking.

After you finish:

- Configure compliance actions to take when a device fails an integrity check.

- To manually start an app integrity check, navigate to a user's device details. Under **App integrity status**, click **Details**, then click .

Configure compliance actions to take when a device fails an integrity check

Before you begin: Enable app integrity checking.

1. In the management console, on the menu bar, click **Policies and profiles > Compliance > Compliance**.
2. Create a new compliance profile or select and edit an existing compliance profile.
3. On the **iOS** tab, in the **CylancePROTECT** section, select the **App integrity failed** check box.
4. Configure the prompt settings (behavior, method, count, and interval) as desired.
5. In the **Enforcement action for BlackBerry Dynamics apps** drop-down list, choose one of the following options:
   - To log information about the compliance issue without taking a compliance action for BlackBerry Dynamics apps, click **Monitor and log**.
   - To prevent the user from accessing BlackBerry Dynamics apps while the device is out of compliance, click **Do not allow BlackBerry Dynamics apps to run**.
6. Click **Add** or **Save**.

After you finish:

- Assign the profile to users and groups.
- You can view information about integrity checks on the Managed devices screen (filter by iOS app integrity) or in a user's device details. For example, you can filter for devices that have a compliance violation because of a potential malware app that is not responding to attestation even though the user actively uses the app, or if the app is not responding to attestation because it hasn't been used.

Using hardware certificate attestation for BlackBerry Dynamics apps on Android devices

You can use a UEM compliance profile to set a security patch level that each user's Android device must satisfy to comply with your organization's security standards. CylancePROTECT extends security patch level enforcement to BlackBerry Dynamics apps. If the security patch level is not satisfied, you can choose the compliance action that you want UEM to take (for example, do not allow BlackBerry Dynamics apps to run on the device).

Note that this feature is in addition to the periodic attestation of Android devices that UEM carries out automatically. Hardware certificate attestation is supported for BlackBerry Dynamics apps that use the BlackBerry Dynamics SDK version 6.0 or later. All of the BlackBerry Dynamics apps released by BlackBerry in July 2019 or later have the required version of the SDK. If this feature is enabled, activation for BlackBerry Dynamics apps that use an earlier version of the SDK will fail.

Hardware certificate attestation applies to BlackBerry Dynamics apps on devices with any Android activation type.

Enable hardware certificate attestation for BlackBerry Dynamics apps

1. In the management console, on the menu bar, click **Settings > General Settings > Attestation**.
2. In the **Android hardware attestation frequency** section, select the **Enable hardware patch level attestation challenges for Android devices** checkbox. You can use the default settings and modify the frequency of hardware certificate attestation later. Save the settings.
3. Create a new activation profile or edit an existing activation profile.
4. On the **Android** tab, in the **Hardware attestation options** section, select the **Enforce attestation compliance rules during activation** check box.
5. Configure other settings in the activation profile as desired and save the profile. For more information about the settings, see "Create an activation profile" in the UEM Administration content.
6. Assign the activation profile to user accounts and groups.
7. Create and assign a CylancePROTECT profile to user accounts and groups to enable the feature on users' devices. You can create a new CylancePROTECT profile (Policies and profiles > Protection > CylancePROTECT) or use a CylancePROTECT profile that you created previously. Note that currently there are no settings that you need to configure in the profile for hardware certificate attestation.

After you finish:

- Configure the frequency of hardware certificate attestation.
- Configure compliance actions to take when a device fails attestation.
- In the management console, you can navigate to a device details page to view status information about hardware attestation.

Configure the frequency of hardware certificate attestation

Before you begin: Enable hardware certificate attestation for BlackBerry Dynamics apps

1. In the management console, click **Settings > General Settings > Attestation**.
2. In the **Android hardware attestation frequency** section, in the **Challenge frequency** drop-down list, specify how often the device must return an attestation response.
3. In the **Device grace period** drop-down list, specify a grace period.

If the grace period expires without a successful attestation response, BlackBerry Dynamics apps are considered out of compliance and UEM will take the compliance action specified in the user's compliance profile (see Configure compliance actions to take when a device fails attestation).

4. Click **Save**.

After you finish: Configure compliance actions to take when a device fails attestation

Configure compliance actions to take when a device fails attestation

Before you begin:

- Enable hardware certificate attestation for BlackBerry Dynamics apps
- Configure the frequency of hardware certificate attestation

1. In the management console, on the menu bar, click **Policies and profiles > Compliance > Compliance**.
2. Create a new compliance profile or select and edit an existing compliance profile.
3. On the **Android** tab, in the **CylancePROTECT** section, select the **Hardware attestation failed** check box.
4. onfigure the prompt settings (behavior, method, count, and interval) as desired.
5. In the **Enforcement action for BlackBerry Dynamics apps** drop-down list, choose one of the following actions to take when a device fails attestation or does not respond in the configured grace period:
   - To log information about the compliance issue without taking a compliance action for BlackBerry Dynamics apps, click **Monitor and log**.
   - To prevent the user from accessing BlackBerry Dynamics apps while out of compliance, click **Do not allow BlackBerry Dynamics apps to run**.
6. On the **Android** tab, select the **Required security patch level is not installed** check box.
7. Add the required device models and corresponding security patches.
8. Configure the prompt settings and enforcement settings for the device and BlackBerry Dynamics apps if the device does not satisfy the required patch level.
9. Click **Add** or **Save**.

After you finish:

- Assign the profile to users and groups.
- You can view information about compliance violations on the Managed devices screen (filter by compliance violations) or in a user's device details.

Legal notice

©2020 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada