



# **BlackBerry Protect Mobile**

## **Overview and Administration Guide**

April 2021



# Contents

- What is BlackBerry Protect Mobile?..... 4**
  - Architecture: BlackBerry Protect Mobile..... 4
  - Malware detection for Android devices..... 5
  - Sideload detection for iOS and Android devices..... 5
  - Scanning URLs in SMS text messages for iOS and Android..... 6
  - Device security checks..... 6
  - Attestation for the Protect Mobile app..... 7
  - What is CylanceINFINITY?..... 7
  - BlackBerry Protect anonymous data collection..... 8
  
- BlackBerry Protect Mobile use cases..... 9**
  - Use case: Detecting malware on an Android device..... 9
  - Use case: Detecting sideloaded apps..... 9
  - Use case: Scanning SMS text messages..... 9
  - Use case: Device security..... 9
  
- Steps to set up BlackBerry Protect Mobile..... 11**
  - Software requirements: BlackBerry Protect Mobile..... 11
  - Create a Protect Mobile policy..... 12
  - Add Protect Mobile users..... 12
  
- Installing the BlackBerry Protect Mobile app..... 14**
  - Install and activate the Protect Mobile app..... 14
  - Features of the Protect Mobile app..... 14
  - Threats detected by the BlackBerry Protect Mobile app..... 17
  
- Managing Protect Mobile features..... 19**
  - View and manage Protect Mobile users..... 19
  - View Protect Mobile alerts..... 19
  - Add an app or developer certificate to the safe list..... 19
  - View Protect Mobile events in the audit log..... 20
    - Protect Mobile audit log information..... 20
  - Send mobile events to a SIEM solution or syslog server..... 21
  
- Legal notice..... 23**

# What is BlackBerry Protect Mobile?

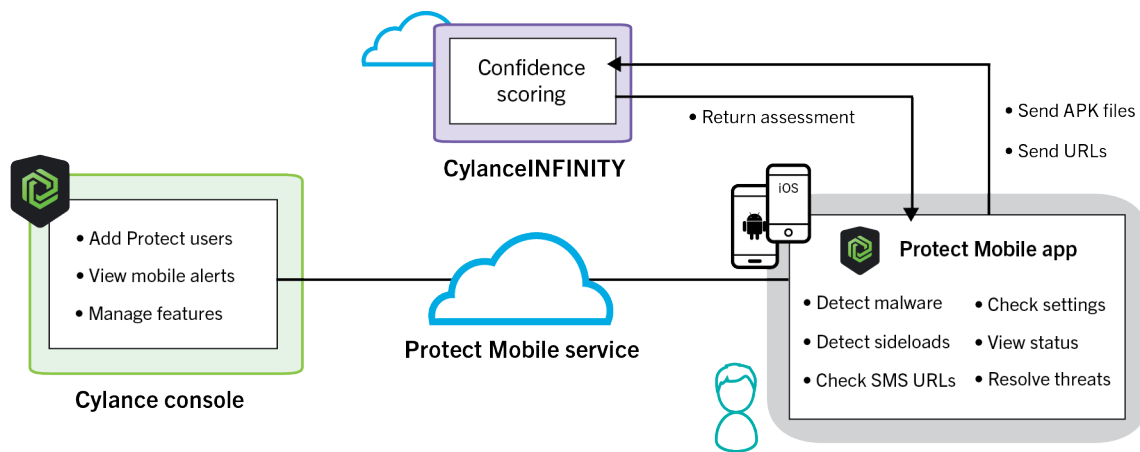
BlackBerry Protect Mobile is an advanced security solution that proactively identifies and prevents cyber threats on mobile devices in real time without disrupting the productivity of your workforce.

Protect Mobile uses a combination of leading-edge technologies, including:

- The web-based Cylance console that administrators use to manage mobile devices, manage Protect Mobile features, and view details about mobile threats
- The Protect Mobile app on users' devices that detects and alerts the user to mobile threats and guides the user to resolve threats without administrator intervention
- The Protect Mobile cloud service that manages user, app, and service configuration and data management in a way that is invisible to administrators and end-users
- The CylanceINFINITY cloud service that uses sophisticated AI and machine learning to support key Protect Mobile features, including the real-time identification of malware and unsafe URLs in text messages

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. Protect Mobile is easy for administrators to configure, easy for end users to understand and use, and leverages hosted and cloud technologies that are always improving and getting smarter.

## Architecture: BlackBerry Protect Mobile



Item	Description
Cylance console	Administrators use the Cylance console to manage mobile devices, configure and manage Protect Mobile features, and view device status and the mobile alerts that are detected by the Protect Mobile app.
Protect Mobile service	The Protect Mobile service is a cloud service that is hosted and maintained by BlackBerry. The Cylance console and the Protect Mobile app on users' devices use a secure connection to communicate with the Protect Mobile service, which is responsible for creating and configuring user accounts, applying Protect Mobile features and settings to devices, and processing events and alerts in real time.

Item	Description
Protect Mobile app	The Protect Mobile app scans the device in regular intervals and checks device settings and conditions to identify threats. When the app detects a threat, the user can view details in the app. Whenever possible, the app gives the user direction to resolve a threat and guides the user to the device settings where they can address the issue. For more information, see <a href="#">Features of the BlackBerry Protect app</a> .
CylanceINFINITY	<p>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 a device endpoint.</p> <p>CylanceINFINITY is a core component of several Protect Mobile features, including <a href="#">malware detection</a> and <a href="#">SMS message scanning</a>. At its core, it enables an aggressive and proactive security strategy, identifying malicious software and websites before they can have any impact on your organization's infrastructure or device users.</p>

## Malware detection for Android devices

The BlackBerry Protect Mobile app can detect malware on an Android device and give the user the option to uninstall malicious apps.

The Protect Mobile app scans the apps on a user's device, including apps preinstalled in the system partition, and uploads the app files to the [CylanceINFINITY cloud service](#). CylanceINFINITY uses AI and machine learning to analyze the app package and produce a confidence score that it returns to the Protect Mobile app. The confidence score determines whether the scanned app is safe or potentially malicious. When CylanceINFINITY determines that an app is potentially malicious, the app notifies the user and provides further details. The user can tap a fix option in the app to navigate to the device settings and uninstall the malicious app.

An app is uploaded to CylanceINFINITY if it has a hash that CylanceINFINITY has not processed previously. If the device scan finds an app that CylanceINFINITY has analyzed previously, it uses the confidence score that CylanceINFINITY has already generated for that unique app hash. 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).

The Protect Mobile app will only upload app files to CylanceINFINITY over a Wi-Fi connection. If the device is currently using a mobile network connection, the app will queue the app packages and upload them when the device is connected to a Wi-Fi network.

If you want to exempt a specific app or all of the apps that use a developer's signing certificate from malware detection, you can [add the app or certificate to the safe list](#).

## Sideload detection for iOS and Android devices

Sideloaded apps represent a potential security threat because they don't follow the same restrictions or protections as apps distributed through official app stores. The Protect Mobile app can detect the presence of a sideloaded app on a user's iOS or Android device, alert the user, and guide the user to uninstall it.

The Protect Mobile app identifies whether an app is sideloaded based on the installation source. The Protect Mobile cloud service and the Protect Mobile app consider official app sources, including the App Store, TestFlight,

Google Play, the Amazon Appstore, and the Samsung Galaxy Store (among other official sources) to be trusted. Apps that were installed from other sources are considered sideloaded.

If you want to exempt a specific app or all of the apps that use a developer's signing certificate from sideload detection, you can [add the app or certificate to the safe list](#).

## Scanning URLs in SMS text messages for iOS and Android

BlackBerry Protect Mobile allows your organization to leverage the real-time risk assessment capabilities of [CylanceINFINITY](#) to warn users of potentially malicious URLs in SMS text messages.

OS	Description
iOS	<ul style="list-style-type: none"><li>• New incoming text messages from known contacts are automatically considered to be safe and only messages from unknown contacts are scanned and assessed.</li><li>• When a user receives an SMS text message that contains a URL, the entire message is sent to CylanceINFINITY in real time.</li><li>• CylanceINFINITY uses advanced machine-learning capabilities and accumulated knowledge from threat intelligence feeds to provide an instant assessment of the safety of the message.</li><li>• When an unsafe URL in a text message is detected, the message is filtered to the junk folder.</li></ul>
Android	<ul style="list-style-type: none"><li>• When a user receives an SMS text message that contains a URL, the unaltered URL is sent to CylanceINFINITY in real time.</li><li>• SMS scanning is limited to the default SMS app on the device.</li><li>• New incoming text messages from known and unknown contacts are scanned and assessed.</li><li>• CylanceINFINITY uses advanced machine-learning capabilities and accumulated knowledge from threat intelligence feeds to provide an instant assessment of the safety of the URL.</li><li>• If a URL is determined to be unsafe, the Protect Mobile app alerts the user, provides details, and guides the user to delete the text message.</li></ul>

To protect user privacy, only messages that contain URLs are assessed.

**Note:** For Android, CylanceINFINITY collects plain text URLs for analysis and assessment. For iOS, CylanceINFINITY collects the contents of messages from unknown contacts that contain URLs. No additional metadata or user identifiers are collected or stored. The data that is collected is never shared with a third party or used by BlackBerry for any purpose other than providing protection from malicious URLs. For more information about Cylance privacy policies, see the [Cylance Privacy Notice](#).

## Device security checks

The Protect Mobile app checks specific device conditions and security settings and notifies the user about potential vulnerabilities to cyber threats. The app checks the following:

- Whether developer mode is enabled (Android only)
- Whether disk encryption is enabled (Android only)

- Whether a screen lock is enabled (for example, a password or fingerprint)
- Whether the device is rooted or jailbroken
- Whether the device is running an OS version that is not permitted (you can specify unsupported versions in the user's Protect Mobile profile)

If the app detects a vulnerability (for example, the device does not have a screen lock enabled or has developer mode on), it indicates the potential risk level (yellow for caution, red for high risk) and provides guidance for the user to resolve the issue. For more information, see [Features of the Protect Mobile app](#).

## Attestation for the Protect Mobile app

The Protect Mobile cloud service regularly performs attestation checks to verify the integrity and security of the Protect Mobile app on each user's device.

On Android devices, the Protect Mobile cloud service uses SafetyNet attestation and hardware certificate attestation to validate the Protect Mobile app. SafetyNet attestation occurs daily. Hardware certificate attestation occurs weekly and uses a minimum Software security level (for more information about the security level, see [SecurityLevel on the Android Developers site](#)).

On iOS devices, the Protect Mobile cloud service checks the integrity of the app using the Apple DeviceCheck framework. Integrity checks occur daily.

Once a user activates the Protect Mobile app, attestation is always enabled, and cannot be disabled. If an attestation failure occurs, administrators can view details in the Cylance console.

## 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 a device endpoint.

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 Protect Mobile features, including [malware detection](#) and [SMS message scanning](#). At its core, it enables an aggressive and proactive security strategy, identifying 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 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](#).

# BlackBerry Protect anonymous data collection

BlackBerry Protect Mobile collects anonymous data and statistics from users' devices. This data allows BlackBerry to improve the Protect Mobile product by:

- Contributing to the discovery of new, previously undetected threats
- Providing increased confidence in detecting threats and improving the quality of future static checks
- Contributing to the training of machine learning models

BlackBerry does not collect any information that can be used to identify an individual user, device, or organization. There is no way for BlackBerry to process the data to identify or determine its source.

Every app that Protect Mobile collects data from uses a unique, randomly generated Anonymous App Identifier that is used to collate data collected over time. The Anonymous App Identifier is unique from any identifier that the user, organization, or BlackBerry is aware of, and is encrypted and stored in the secure container that protects all Protect library data on a device. The Anonymous App Identifier is deleted when the app is uninstalled or is no longer managed by BlackBerry. Because each app uses a unique Anonymous App Identifier, data from apps on the same device cannot be associated.

The data is reported every 6 hours, or the next time a reporting app starts if more than 6 hours have passed. The data is uploaded to BlackBerry over a Wi-Fi connection only, to a maximum of 250 MB each month. The following data is collected:

- Anonymous identity
- Battery status information
- Protect Mobile application information
  - Process and thread information
  - Libraries information
- Apps information
- System files and properties information
- Network events information
- Certificate information

BlackBerry controls the frequency of the collection, the types of anonymous data collected, and the limits on monthly collection through a configuration that is sent to the Protect Mobile app. BlackBerry reserves the right to change the configuration on an ongoing basis to best target advanced threat detection and bring the most value to the solution.

The data is used internally by BlackBerry's R&D organization, with access limited to employees with a genuine need to access the data and who are granted access through an approval process. The data is not available in any form to anyone outside of BlackBerry, and it is stored in Amazon Web Services S3 storage for analysis and processing. The data is collected and stored in compliance with the [General Data Protection Regulation](#).

Any sensor that may be added in the future will undergo security and privacy reviews to ensure that there is no way that any data that is collected can be used to identify a user, device, or organization.



# BlackBerry Protect Mobile use cases

The following use cases demonstrate the value of BlackBerry Protect Mobile in everyday situations. In the cases that follow, an administrator has enabled the Protect Mobile service for the user, and the user has installed and activated the Protect Mobile app on their device.

## Use case: Detecting malware on an Android device

Jack uses his personal Android device for work as part of a bring-your-own-phone policy. A friend tells Jack about a new fitness app from a website that offers free apps from independent developers. Jack downloads and installs the app on his device and starts to use it.

The Protect Mobile app is installed and activated on Jack's device. The Protect Mobile app scans the device, identifies the new fitness app, and sends the .apk files to the CylanceINFINITY cloud service. CylanceINFINITY analyses the app files and returns a confidence score to the Protect Mobile app. The confidence score indicates that the app is potentially malicious.

The Protect Mobile app notifies Jack that the fitness app has been identified as malicious. Jack taps the Fix option in the app to navigate to the device settings and uninstall the fitness app.

## Use case: Detecting sideloaded apps

Megan uses her iOS device for work as part of a bring-your-own-phone policy. A friend tells her about a new music app that is available for free from the developer's own website. Megan visits the site on her device and follows the developer's instructions to download and install the app.

Megan has the Protect Mobile app installed and activated on her device. When the Protect Mobile app scans the device, it detects that the music app has been installed from an unofficial source. The Protect Mobile app alerts Megan that the music app is sideloaded and presents a potential security risk.

Megan taps the Fix option in the Protect Mobile app for instructions to remove a sideloaded app, and follows them to uninstall the music app.

## Use case: Scanning SMS text messages

Jake uses his personal iOS device for work as part of a bring-your-own-phone policy. Jake receives a text message from an unknown number that contains a web link.

When he receives the text, the Protect Mobile app sends the entire message to CylanceINFINITY. CylanceINFINITY analyzes the message and returns a real-time assessment to the Protect Mobile app that the URL it contains is potentially malicious. The Protect Mobile app filters the message to the SMS junk folder.

Jake goes into his junk folder and permanently deletes the message with the malicious URL from his device.

## Use case: Device security

Jessica uses her personal Android device for work as part of a bring-your-own-phone policy. Jessica currently has developer mode enabled on her device because a friend recommended it to adjust some settings to speed

up device animations. Also, Jessica uses her phone frequently, so she decided not to turn on a screen lock option (for example, a password or PIN).

Following the instructions from her administrator, Jessica installs and activates the Protect Mobile app on her device. The Protect Mobile app regularly checks device conditions and security settings to identify potential security risks. The Protect Mobile app detects that developer mode is on and that a screen lock is not enabled and displays a medium (yellow) risk in the app, with additional details and information about how to resolve these risks.

Jessica follows the guidance in the app to turn off developer mode and enable a screen lock.

# Steps to set up BlackBerry Protect Mobile

Step	Action
1	Review the <a href="#">software requirements</a> .
2	Create a <a href="#">Protect Mobile policy</a> .
3	Add <a href="#">Protect Mobile users</a> .
4	Device users <a href="#">install and activate the Protect Mobile app</a> .

## Software requirements: BlackBerry Protect Mobile

Item	Description
Protect Mobile licenses	To use the Protect Mobile service, your organization must purchase Protect Desktop licenses, which allow you to use Protect Mobile features. These licenses are included in the BlackBerry Cyber Suite and BlackBerry Spark Suite packages. For more information, see <a href="#">BlackBerry Spark Suites</a> and the <a href="#">BlackBerry Enterprise Licensing Guide</a> .
Cylance console	This guide will explain how to use the console screens that are relevant for the Protect Mobile service. For more information about the other features and components of the Cylance console, see the <a href="#">Protect Desktop Administration Guide</a> .
Administrator permissions	To manage Protect Mobile, Cylance administrators require the Administrator role or a custom role with the "Threat protection", "Device policy", and "Devices" permissions.
Protect Mobile app	The Protect Mobile app is supported for: <ul style="list-style-type: none"><li>• Android OS 8 or later</li><li>• iOS 12 or later</li><li>• iPad OS 13 or later</li><li>• Chrome OS 84.x or later; Chrome OS supports the following features only:<ul style="list-style-type: none"><li>• <a href="#">Malware detection for Android devices</a></li><li>• <a href="#">Sideload detection for iOS and Android devices</a></li><li>• <a href="#">Device security checks</a>: developer options, root detection, and screen lock only</li><li>• <a href="#">Attestation for the Protect Mobile app</a></li></ul></li></ul>

Item	Description
Network requirements	<p>The Protect Mobile app requires a secure, direct connection to the following URLs to communicate with the Protect Mobile cloud service and CylanceINFINITY. If devices are connected to your organization's Wi-Fi network, your network configuration must allow connections to:</p> <ul style="list-style-type: none"> <li>• Protect Mobile cloud service: <ul style="list-style-type: none"> <li>• US: mps.cylance.com:443</li> <li>• JP: mps-apne1.cylance.com: 443</li> <li>• EU: mps-euc1.cylance.com: 443</li> <li>• AU: mps-apse2.cylance.com: 443</li> <li>• SP: mps-sae1.cylance.com: 443</li> </ul> </li> <li>• score.cylance.com:443</li> <li>• idp.blackberry.com:443</li> </ul>

## Create a Protect Mobile policy

You can create and assign a Protect Mobile policy to users so that you can control which features you want to enable. When you [add a Protect Mobile user](#), the user is automatically assigned the Default policy with all features enabled, with the exception of unsupported OS which is optional and requires configuration based on your organization's standards. You can change the Default policy but you cannot delete it. Follow the steps below if you want to create and assign a custom policy to users.

1. In the Cylance console, on the menu bar, click **Settings > Policy**.
2. On the **Mobile** tab, click **Add New Policy**.
3. Turn on the features that you want to enable in the policy.

You cannot disable attestation checks for the Protect Mobile app or device security checks for encryption and a screen lock.
4. If you enabled **Unsupported operating system**, for the required platforms, add the OS versions that you do not want to support to the **Chosen** list and select them.
5. Click **Create**.

In the list of policies, click the filter icon next to a column name to type filtering criteria. If a sort arrow displays when you hover over a column name, click it to sort policies by ascending or descending order.

### After you finish:

- [Add Protect Mobile users and assign a Protect Mobile policy](#). The policy is assigned to all devices that are associated with that user.
- To change a policy, in **Settings > Policy**, click the policy. Make your changes and click **Save**. After you save the changes, the Protect Mobile cloud service sends the updated configuration to the devices that are assigned that policy.

## Add Protect Mobile users

To enable the BlackBerry Protect Mobile service for device users, you must add the users in the Cylance console. When you add a user, the user is automatically assigned the default Protect Mobile policy with all features enabled.

Each user can be associated with multiple devices. A user can use the same activation password or QR code to activate the Protect Mobile app on multiple devices.

**Before you begin:**

- If you want to control which Protect Mobile features are enabled, [create a custom Protect Mobile policy](#).
- If you want to add multiple users at once, prepare a .csv file with following fields: FIRST NAME, LAST NAME, and EMAIL ADDRESS. To download an empty .csv file that you can populate, click **Assets > Mobile > Add Mobile User > Bulk Add**, then click **Download Sample CSV**.

1. In the Cylance console, on the menu bar, click **Assets > Mobile**.
2. Do one of the following:

Task	Steps
Add one user	<ol style="list-style-type: none"><li>a. Click <b>Add Mobile User &gt; Individual Add</b>.</li><li>b. Specify the user's first name, last name, and email address.</li><li>c. Click <b>Add</b>.</li></ol>
Add multiple users	<ol style="list-style-type: none"><li>a. Click <b>Add Mobile User &gt; Bulk Add</b>.</li><li>b. Browse to or drag and drop the .csv file with user information.</li><li>c. Click <b>Add</b>.</li></ol>

The Protect Mobile cloud service will send each user an email with instructions to download, install, and activate the Protect Mobile app. The activation QR code and password that the user receives are valid for 2 weeks. If a user activates the app on multiple devices, each device displays as a separate row on the **Assets > Mobile** tab.

**After you finish:**

- If you want to assign a custom Protect Mobile policy to one or more users, select the users and click **Assign Policy**. Select the policy and click **Assign Policy**. Each user can be assigned one policy only. The policy is assigned to all devices that the user installs and activates the Protect Mobile app on. If a user activates the app on multiple devices and you assign a new policy to any of those devices, the new policy is applied to every device the user activated.
- Instruct users to [Install and activate the Protect Mobile app](#) on one or more mobile devices. Until a user activates the app, their enrollment status is "Pending". After a user activates the app, their status is "Enrolled". The Invitation Status column indicates whether the QR code and password are still valid ("Pending") or expired, and provides the expiry date.  
You can view users' status and device information on the **Assets > Mobile** tab. After the user is activated, the New Alerts column displays a count of the total number of active threats that the Protect Mobile app has detected on the device. A status icon indicates whether the device is currently protected or unsafe.
- To send the user a new activation password and QR code, select any of the user's devices and click **Resend Invitation**.
- To remove the Protect Mobile service from a device, on the **Assets > Mobile** tab, select the device and click **Remove**. When prompted, click **Remove** again. This removes all Protect Mobile data from the user's device and all events related to that device from the Protect Mobile cloud service and from the Cylance console. If the user opens the Protect Mobile app on that device, the app displays a notification that the service is no longer active. If all of the devices that are associated with a user are removed, the user's data is also removed from the console and the Protect Mobile service.
- If a user removes the Protect Mobile app, and at a later date chooses to install and activate the app again, it is a best practice to remove the device to delete all previous event data and then activate the app on the device again. If you don't, the data and threats from the previous activation will remain in the Protect Mobile service.

# Installing the BlackBerry Protect Mobile app

The Protect Mobile app provides users with increased awareness of the security of their mobile device and empowers the user to take action to resolve threats without administrator intervention.

The BlackBerry Protect Mobile app provides users with:

- An overall security assessment of the device
- A list of malicious or sideloaded apps that have been detected
- Alerts about device settings or conditions that pose a security risk
- User-friendly options to guide the user to uninstall malicious or sideloaded apps and to correct device settings or conditions
- The ability to detect malicious URLs in text messages

The Protect library that is integrated with the app scans the device in regular intervals to identify threats. When the app detects a threat, the user can view details in the app. Whenever possible, the app gives the user direction to resolve a threat, and guides the user to the device settings where they can address the issue. For more information, see [Features of the Protect Mobile app](#).

## Install and activate the Protect Mobile app

**Before you begin:** [Add Protect Mobile users](#).

Send the following instructions to Protect Mobile users:

1. When you receive an email notifying you that Protect Mobile has been enabled for your mobile device, click the link in the email to install the app from the appropriate app store.
2. Open and activate the app using the QR code or activation password that you received in the email message.
3. Do the following to enable SMS message scanning:
  - a) In the app, click **View Details > Message scanning > Enable**. Click **OK**. When prompted, click **Allow**.
  - b) If you are using an iOS device, go to **Settings > Messages > Unknown & Spam**. Turn on **Filter Unknown Senders**. Under **SMS Filtering**, turn on **Protect**.
  - c) If you are using the iMessage app, enable the **Send as SMS** option.

You have the option to turn off SMS scanning at any time.

**After you finish:** You can repeat these steps to install and activate the Protect Mobile app on additional devices. The password and QR code are valid for 2 weeks. If the password and QR code are expired, you can request a new invitation from your administrator.

## Features of the Protect Mobile app

If you turn off a Protect Mobile feature in the Protect Mobile policy, the feature is greyed out in the app and users cannot interact with it.

If a more recent version of the app is available, the user receives a message in the app that indicates how many days the user has to update the app. The message includes an Update link to open the appropriate app store. If the update grace period expires, the user cannot dismiss the message and must update if they want to continue to use the app.

Feature	Platform	Description	Possible user action
<b>Application security features</b>			
Malicious apps	Android	Displays a list of any malicious apps that the Protect Mobile app has detected.	The user can tap Fix to uninstall a malicious app from the device OS.
Sideloaded apps	Android iOS	Displays a list of any sideloaded apps that the Protect Mobile app has detected.	The user can tap Fix to view instructions for removing the sideloaded app.  On Android devices, there is an option to go to the device settings to uninstall the app.
<b>Device security features</b>			
Developer options	Android	Indicates whether developer mode is enabled on the device.	The user can tap Fix to view instructions for turning off developer mode. There is an option to go to the device settings to turn off developer mode.
Disk encryption	Android	Indicates whether disk encryption is enabled on the device.	The user can tap Fix to view instructions for turning on disk encryption. There is an option to go to the device settings to turn on disk encryption.
Screen lock	Android iOS	Indicates whether a screen lock option (for example, a password or fingerprint) is currently enabled on the device.	The user can tap Fix to view instructions for turning on a screen lock.  On Android devices, there is an option to go to the device settings to turn on a screen lock.
Compromised device and root detection	Android iOS	A notification displays only if the app detects that the device is rooted or jailbroken.	No action in the app; the user must contact their administrator for a resolution.

Feature	Platform	Description	Possible user action
Device attestation	Android iOS	<p>For Android devices, a notification displays if the Protect Mobile app fails any of the following:</p> <ul style="list-style-type: none"> <li>• SafetyNet attestation</li> <li>• Hardware certificate attestation</li> <li>• Hardware attestation security level lower than Software</li> <li>• Hardware attestation boot state of unverified</li> </ul> <p>For iOS devices, a notification displays if the Protect Mobile app fails an integrity check using the Apple DeviceCheck framework.</p>	No action in the app; the user must contact their administrator for a resolution.
Unsupported OS	Android iOS	Indicates whether the device OS meets the requirements that are configured in the Protect Mobile policy that is assigned to the user.	<p>The user can tap Fix to view instructions for upgrading the OS.</p> <p>On Android devices, there is an option to go to the device settings to upgrade the OS.</p>
App out of date	Android iOS	<p>Indicates that a new version of the Protect Mobile app is available in the appropriate app store.</p> <p>When the user opens the app, a message indicates how many days the user has to update the app. If the update grace period expires, the user cannot dismiss the message and must update if they want to continue to use the app.</p>	The user can tap Update to navigate to the appropriate app store to update the app.
<b>Message scanning features</b>			
Malware messages detected	Android iOS	<p>Identifies SMS text messages with potentially malicious URLs.</p> <p>For more information about the feature differences by platform, see <a href="#">Scanning URLs in SMS text messages for iOS and Android</a>.</p>	<p>On Android devices, the user can tap Fix to go to the default messaging app to delete text messages.</p> <p>On iOS devices, the message is automatically filtered to the junk folder.</p>

## Home screen menu



Feature	Description
About	View the user's email and user ID, the app version, the version of the BlackBerry Dynamics SDK that is integrated with the app, and the license agreement.
Logs	Send the Protect Mobile app log to BlackBerry. BlackBerry Support can retrieve the app log as necessary to assist with troubleshooting. Note that sending the app log does not alert BlackBerry. To resolve issues you must contact BlackBerry Support.
Send Feedback	Send feedback or report app or security issues to BlackBerry.

## Threats detected by the BlackBerry Protect Mobile app

### Threats displayed in the BlackBerry Protect Mobile app

Mobile security threat	Risk level	Color
Malicious application	High	Red
Sideloaded application	High	Red
SMS message scanning	Medium	Yellow
Device security: Developer options	Medium	Yellow
Device security: Screen lock	Medium	Yellow
Device security: Rooted or compromised device	High	Red
Device security: Full disk encryption	Medium	Yellow
Device security: Attestation	High	Red
Device Security: Unsupported OS	Medium	Yellow
Device Security: App out of date	Medium	Yellow

### Threats displayed in the Cylance console (Protection > Mobile Alerts)

Mobile security threat	UI alert type	UI alert name	UI description
Malicious application	Malicious app	App name	Package name, package version, SHA256 hash

Mobile security threat	UI alert type	UI alert name	UI description
Sideloaded application	Sideloaded app	Android: App name iOS: Common name of the developer certificate	Android: Package name, package version, installer source, SHA256 hash
SMS message scanning	NA	NA	NA
Device security: Developer options	NA	NA	NA
Device security: Screen lock	Device configuration	Screenlock disabled	OS name, OS version
Device security: Rooted/Jailbroken	Privilege escalation	Android: Rooted iOS: Jailbroken	OS name, OS version
Device security: Full disk encryption	Device configuration	Encryption disabled	OS name, OS version
Device security: iOS integrity check	Attestation failure	iOS App Integrity Check	Attestation type, attestation state
Device security: Android SafetyNet attestation	Attestation failure	Android SafetyNet	Attestation type
Device security: Android hardware certificate attestation	Attestation failure	Android Hardware	Attestation type, attestation state, rule failure
Device security: Unsupported OS	Device configuration	Unsupported OS	OS name, OS version

# Managing Protect Mobile features

This section gives you information about how you can view useful details in the Cylance console and configure Protect Mobile features to meet your organization's needs.

## View and manage Protect Mobile users

1. In the Cylance console, on the menu bar, click **Assets**.
2. Click the **Mobile** tab to view device, status, and alert information for Protect Mobile users and devices.
3. Select one or more devices to do any of the following:
  - If you want to assign a different Protect Mobile policy, click **Assign Policy**. Select the policy and click **Assign Policy**. Note that if a user activated the app on multiple devices, the new policy is applied to every device the user activated. Each user can be associated with one policy only across all activated devices.
  - To send a new activation password and QR code, click **Resend Invitation**.
  - To remove the Protect Mobile service from a device, select the device and click **Remove**. When prompted, click **Remove** again. This removes all Protect Mobile data from the user's device and all events related to that device from the Protect Mobile cloud service and from the Cylance console. If the user opens the Protect Mobile app on that device, the app displays a notification that the service is no longer active. If all of the devices that are associated with a user are removed, the user's data is also removed from the console and the Protect Mobile service.

**After you finish:** To export the results to a .csv file, click the Export icon. Select the scope of the export and click **Export**.

## View Protect Mobile alerts

1. In the Cylance console, on the menu bar, click **Protection**.
2. Click the **Mobile Alerts** tab to [view any threats that have been detected](#) by the Protect Mobile app on users' devices.

You can use the following information to [Add an app or developer certificate to the safe list](#):

  - For iOS sideloaded app threats, the **Alert Name** column displays the common name of the developer certificate.
  - For Android malicious and sideloaded app threats, the **Description** column displays the SHA256 hash of the app.
3. If you want to ignore one or more alerts, select the alerts and click **Ignore**. Click **Ignore** again to confirm.

This changes the alert status to **Ignored**.

**After you finish:** To export the results to a .csv file, click the Export icon. Select the scope of the export and click **Export**.

## Add an app or developer certificate to the safe list

If you want to exempt a specific app or all of the apps that use a developer's signing certificate from [malware scanning](#) and [sideload detection](#), you can add the app or signing certificate to the safe list.

**Before you begin:**

- To add an app or iOS developer certificate to the safe list, you need the app hash or the certificate common name. You can get this information from the **Protection > Mobile Alerts** tab. See [View Protect Mobile alerts](#).
- If you want to add an Android developer certificate to the safe list, you need to get the thumbprint of the certificate from the app binary. For instructions, visit [support.blackberry.com/community](http://support.blackberry.com/community) to read article 70577.

1. In the Cylance console, on the menu bar, click **Settings > Global List**.
2. On the **Safe** tab, do one of the following:

Task	Steps
Add an Android app to the safe list	<ol style="list-style-type: none"> <li>a. On the <b>Mobile Apps</b> tab, click <b>Add App</b>.</li> <li>b. Specify the app details.</li> <li>c. Click <b>Add</b>.</li> </ol> <p><b>Note:</b> If an app contains multiple .apk files, you must manually enter the hash of each file. Optionally, you can add the app's signing certificate instead.</p>
Add a developer's signing certificate to the safe list	<ol style="list-style-type: none"> <li>a. On the <b>Mobile Developers</b> tab, click <b>Add</b>.</li> <li>b. Select the appropriate OS and specify the details for the developer's signing certificate.</li> <li>c. Click <b>Add</b>.</li> </ol>



3. Repeat step 2 to add additional apps or certificates to the safe list.

**After you finish:** To remove an app or certificate from the safe list, on the **Safe > Mobile Apps** or **Safe > Mobile Developers** tab, select the app or certificate and click **Remove**. When you are prompted, click **Remove** again.

## View Protect Mobile events in the audit log

You can view and export details for Protect Mobile administrative actions in the Cylance console's audit log. For more information about what is added to the audit log for Protect Mobile actions, see [Protect Mobile audit log information](#).

**Note:** At this time, you must contact BlackBerry Support to enable audit logging for Protect Mobile administrative actions. This feature will be enabled automatically in an upcoming release.

1. In the Cylance console, click  > **Audit Log**.
2. In the filter fields, specify the criteria that you want to use to filter the audit log information.
3. To export the results to a .csv file, click . Select the scope of the export and click **Export**.

### Protect Mobile audit log information

The following table lists the information that is added to the audit log for Protect Mobile administrative actions. You can use the filtering options in the console to filter the audit log results.

Category	Action	Details
End User	Add	User: <i>&lt;email&gt;</i> , Type: local
End User	Import	Success count: <i>&lt;count&gt;</i> , Failed count: <i>&lt;count&gt;</i>

Category	Action	Details
End User	Remove	User: <i>&lt;email&gt;</i> A log entry is generated for each removed user.
End User	Assign policy	Policy: <i>&lt;policy name&gt;</i> , Users: <i>&lt;email addresses&gt;</i>
End User	Send invitation	Users: <i>&lt;email addresses&gt;</i> , Success count: <i>&lt;count&gt;</i> , Failed count: <i>&lt;count&gt;</i>
Mobile Device	Remove	User: <i>&lt;email&gt;</i> , Device: <i>&lt;device name&gt;</i> , OS: <i>&lt;OS family&gt;</i> , OS version: <i>&lt;version&gt;</i> A log entry is generated for each removed device.
Mobile Device	Export	Filter: <i>&lt;filter fields and values&gt;</i> If "Everything" was selected, the Filter value is None. If "Current filter" was selected, the name and value of each field is listed.
Mobile Policy	Add	Source: Protect Mobile, Policy: <i>&lt;policy name&gt;</i> , <i>&lt;setting names and values&gt;</i>
Mobile Policy	Edit	Source: Protect Mobile, Policy: <i>&lt;policy name&gt;</i> , <i>&lt;changed setting names and values&gt;</i>
Mobile Policy	Remove	Source: Protect Mobile, Policy: <i>&lt;policy name&gt;</i> A log entry is generated for each removed policy.
Mobile Exclusions	Add	Source: Protect Mobile, Type: <i>&lt;App / Developer / Domain / IP&gt;</i> , Category: <i>&lt; Approved / Restricted&gt;</i> , Name: <i>&lt;name&gt;</i> , Platform: <i>&lt;platform&gt;</i> , Identifier: <i>&lt;identifier&gt;</i> , Issuer: <i>&lt;issuer&gt;</i>
Mobile Exclusions	Remove	Source: Protect Mobile, Type: <i>&lt;App / Developer / Domain / IP&gt;</i> , Name: <i>&lt;name&gt;</i> A log entry is generated for each removed exclusion.
Mobile Alerts	Ignore	Source: Protect Mobile, ID: <i>&lt;ID&gt;</i> , Type: <i>&lt;alert_type&gt;</i> , Name: <i>&lt;alert_name&gt;</i> , Description: <i>&lt;device_OS&gt;</i> A log entry is generated for each ignored alert.
Mobile Alerts	Export	Source: Protect Mobile, Filter: <i>&lt;filter fields and values&gt;</i> If "Everything" was selected, the Filter value is None. If "Current filter" was selected, the name and value of each field is listed.

## Send mobile events to a SIEM solution or syslog server

Security Information and Event Management (SIEM) software collects, analyzes, and aggregates security data from multiple sources to detect potential security threats. You can choose to send the [alerts that are detected by](#)

the [Protect Mobile app](#) to your organization's SIEM software or syslog server. The alert data that is sent to a SIEM or syslog server is the same alert data that is displayed in the Cylance console.

1. In the Cylance console, on the menu bar, click **Settings > Application**.
2. Select the **Syslog/SIEM** check box.
3. Select the **Mobile Alerts** check box.
4. Select other event types as desired and configure the appropriate settings for your organization's SIEM solution or syslog server. For more information about each event type, see the [Syslog Guide](#).
5. Click **Save**.

# Legal notice

©2021 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