Lookout® Mobile Endpoint Security

Deploying Lookout with BlackBerry Unified Endpoint Management

June 2018

Lookout

Copyright and disclaimer

Table of contents

Preface

Lookout Mobile Endpoint Security (MES) provides comprehensive risk management across iOS and Android devices to secure against app, device, and network-based threats while providing visibility and control over data leakage. With a seamless integration to your EMM solution, Lookout empowers your organization to adopt secure mobility without compromising productivity.

About this guide

This guide describes how to deploy and integrate Lookout MES with your existing BlackBerry Enterprise Server Unified Endpoint Management (BlackBerry UEM) environment. It covers initial deployment for both the Lookout MES Console and the Lookout for Work mobile app.

Note that some screenshots may differ from your own UEM configuration.

To provide feedback on this guide, please contact documentation@lookout.com.

Audience

This guide is for administrators, business users, and mobile security engineers who administer and support Lookout with BlackBerry UEM.

Typographic conventions

The following table describes the typographic conventions used in this document.

Typeface	Meaning
User interface elements	This formatting is used for graphical user interface elements such as pages, dialog boxes, buttons, and field labels.
`Code sample`	This formatting is used for sample code segments.
<*Variable*>	This formatting is used for variable values. For variables within a code sample the formatting is <*`Variable`*>.
`File/path`	This formatting is used for filenames and paths.
>	The right angle bracket, or greater-than sign, indicates menu item selections in a graphic user interface, e.g., **File > New > Tag**.

Overview

1. Create an API user in UEM.
2. Create UEM User Groups to sync Lookout device state and enrollment information.
3. Retrieve the BlackBerry Secure Workspace SRP ID.
4. Configure the UEM Connector from the Lookout MES Console.
5. Add the Lookout for Work app to UEM and deploy it to your users.
6. Monitor device status in Lookout MES to see when users activate Lookout for Work on their devices.
7. Create security policies and apply them to the User Groups you created in Step 2.

Requirements

See the Lookout Mobile Endpoint Security Supported Platforms document for supported platform information.

BlackBerry UEM requirements:

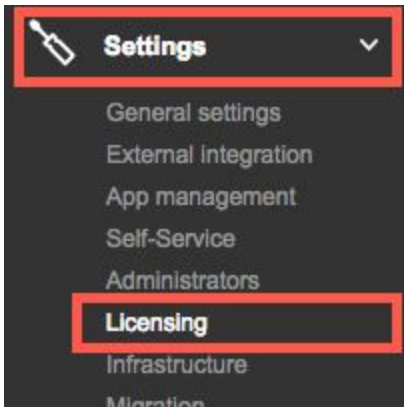
- **BlackBerry UEM** version **12.7** or **12.8**.
- **Security Administrator** access to UEM.
- Whitelist and/or open the Lookout ports documented in the MDM Service IP Whitelisting article.
    - Open the Device API port, typically **TCP port 8095**.
    - Open the UEM SOAP API port, typically **TCP port 18084**.
- Verify that your BlackBerry server is licensed for **BlackBerry Enterprise Mobility Suite** (Management Edition or higher).

Lookout MES Console requirements:

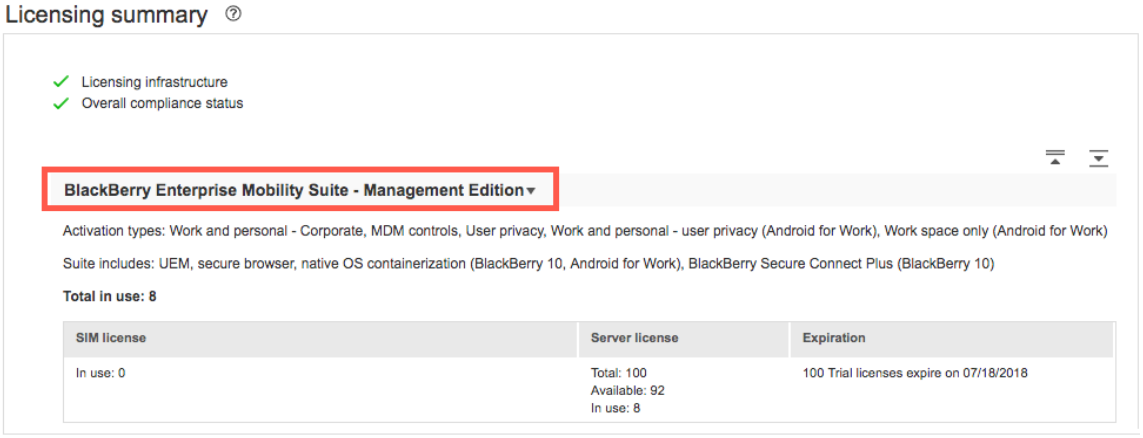
- Verify that the Lookout Enterprise Support team has enabled Privacy Controls for your Lookout MES tenant.

Verifying BlackBerry Enterprise Mobility Suite Licenses

1. In the BlackBerry UEM menu bar, navigate to **Settings > Licensing**:



2. Confirm that you are licensed for BlackBerry Enterprise Mobility Suite:



Preparing BlackBerry UEM for Integration

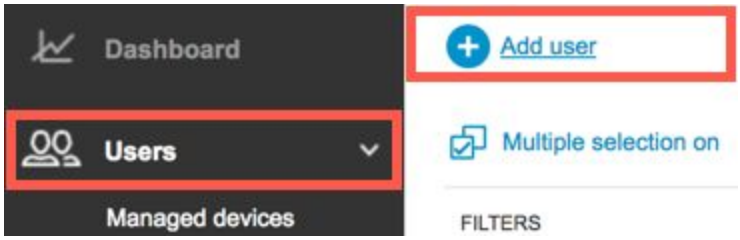
Before integrating Lookout with BlackBerry UEM:

1. Create an API user for communication between Lookout and UEM.
2. Create User Groups in UEM that map to the different Lookout risk levels.

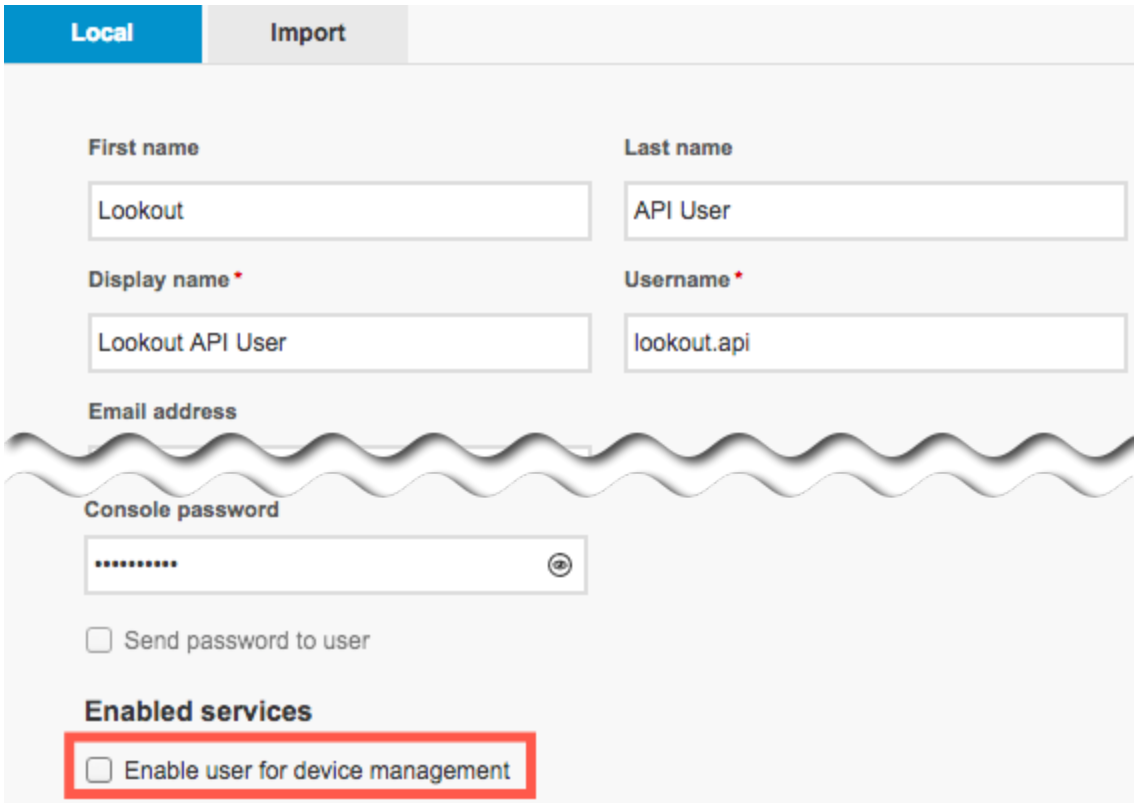
Creating an API User

IMPORTANT: You must log into UEM on an account with the Security Administrator role to create a new admin user.

1. In the BlackBerry UEM menu bar, navigate to **Users** and click **+ Add User**:



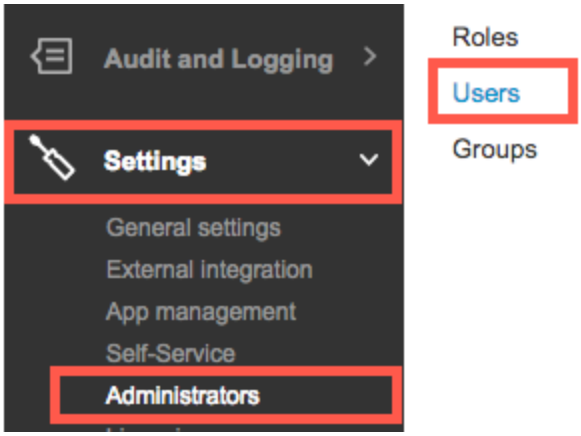
   The **Add a user** window displays.
2. Set the following:



Field	Value

Display Name	`Lookout API User`
Username	`lookout.api`
Email address	Input the email address for your UEM administrator.
User Groups	If you have User Groups for different levels of administrator access, add the API User to your **Enterprise Administrator** level group. Otherwise, continue as documented to add the role to the user instead of assigning a group.
Console password	Set a password. This must meet any complexity requirements you have configured in UEM, as described in Set the minimum password complexity for local administrators in the BlackBerrry UEM documentation.
Enable user for device management	Uncheck this setting.

3. Click **Save**.
4. In the menu bar, click **Settings > Administrators**, then click **Users**:



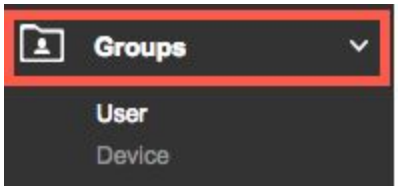
5. Click the Add Administrator icon in the upper-right corner of the **Administrator users** table:

   The Add an administrator window appears.
6. Search for and click on the Lookout API User you created in Step 2.
7. Assign the **Enterprise Administrator** role and click **Save**.

For more information, see Create an administrator in the BlackBerry UEM documentation.

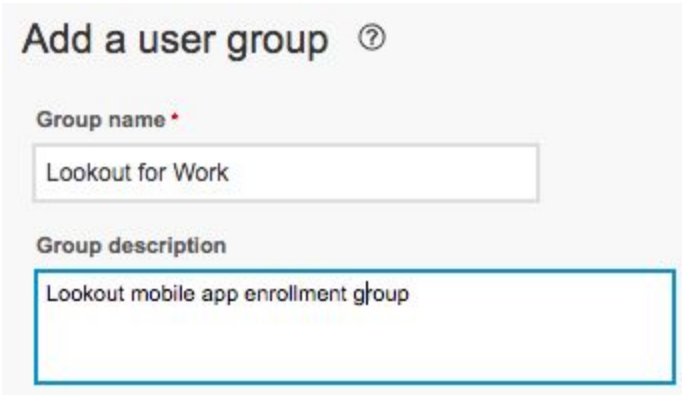
Creating User Groups for Enrollment and Device State Sync

1. In the BlackBerry UEM menu bar, click **Groups**:



2. Click the Add User Group icon to the right of the search bar:

3. Add the following groups one at a time:



Name	Description
Lookout for Work	Lookout mobile app enrollment group
Lookout MES - Deactivated	Deactivated devices
Lookout MES - Disconnected	Devices that have lost connectivity with Lookout
Lookout MES - Pending	Devices that have not activated Lookout yet
Lookout MES - Threats Present	Compromised devices
Lookout MES - Secured	Secured devices
Lookout MES - Low Risk	Low risk devices
Lookout MES - Moderate Risk	Moderate risk devices
Lookout MES - High Risk	High risk devices

Setting up your BlackBerry UEM Connector in the Lookout Mobile Endpoint Security Console

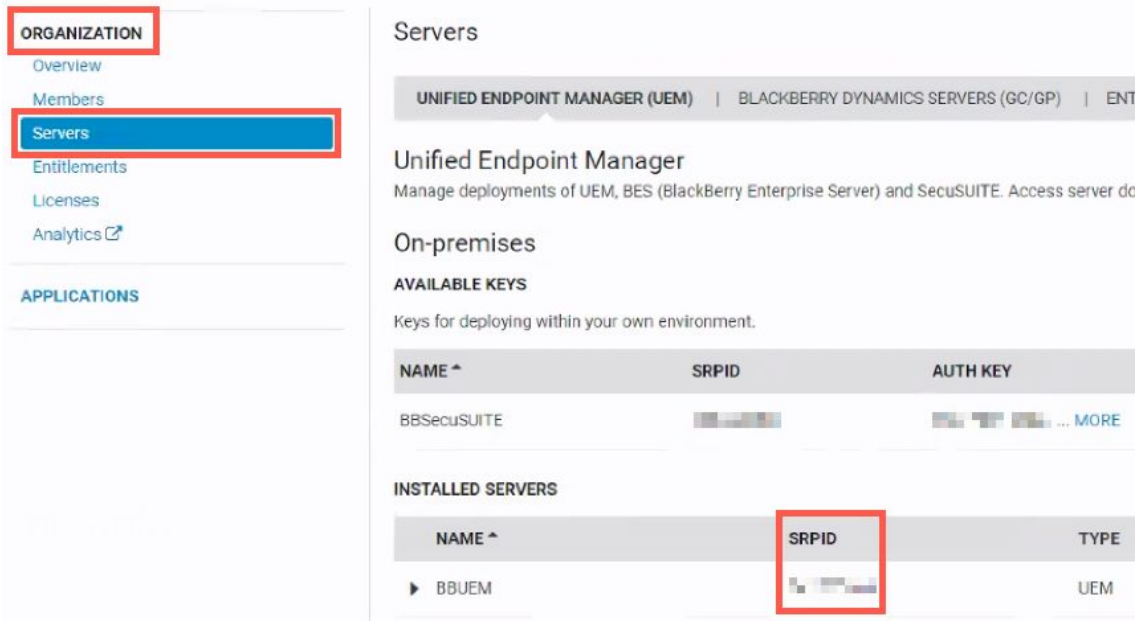
Once you have created an API user and UEM User Groups for device state sync and enrollment, you can create your Blackberry UEM Connector in the Lookout Mobile Endpoint Security (MES) Console

Retrieving the BlackBerry SRP ID

The Blackberry UEM Connector in the Lookout MES Console requires your BlackBerry SRP ID. For BlackBerry UEM 12.8, you retrieve this ID from https://my.blackberry.com. For BlackBerry UEM 12.7, you retrieve this ID from your Secure Work Space settings page in UEM, or from a device activation email.

BlackBerry UEM 12.8

1. Log in to https://my.blackberry.com
2. Under **ORGANIZATION**, click **Servers**.
   The ID is listed in the **SRPID** column:

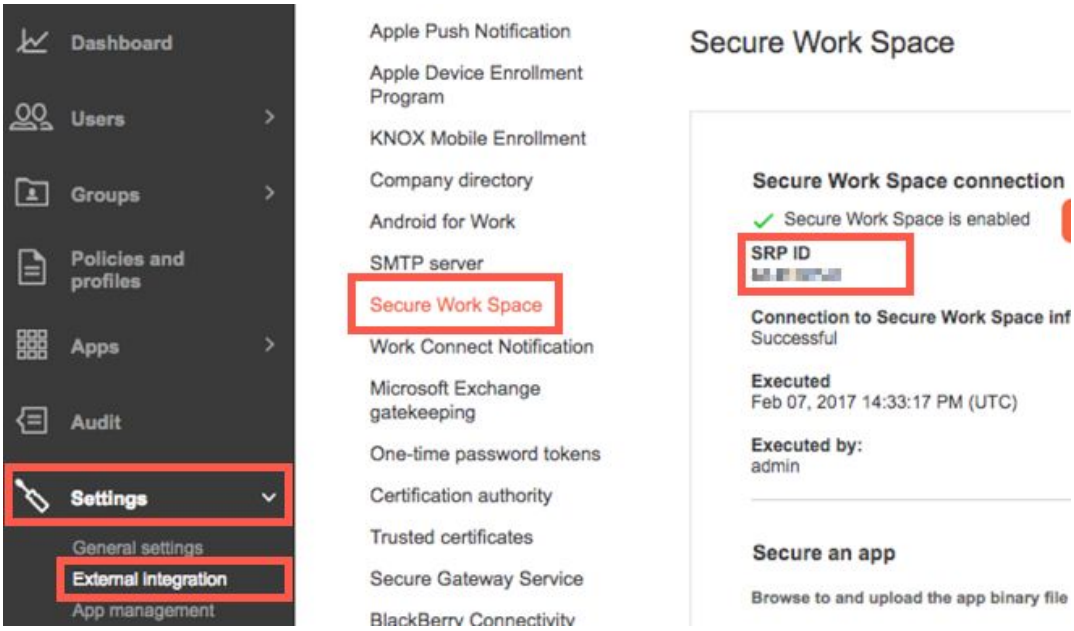


BlackBerry UEM 12.7

1. To retrieve the ID from your Secure Work Space settings page:

   a. In the BlackBerry UEM menu bar, navigate to **Settings > External Integration** and click **Secure Work Space**.

   Your SRP ID is listed at the top of the Secure Work Space page:



NOTE: If you do not see Secure Work Space listed, follow Step 2 to retrieve the ID from an activation email.

2. To retrieve the ID from an activation email:

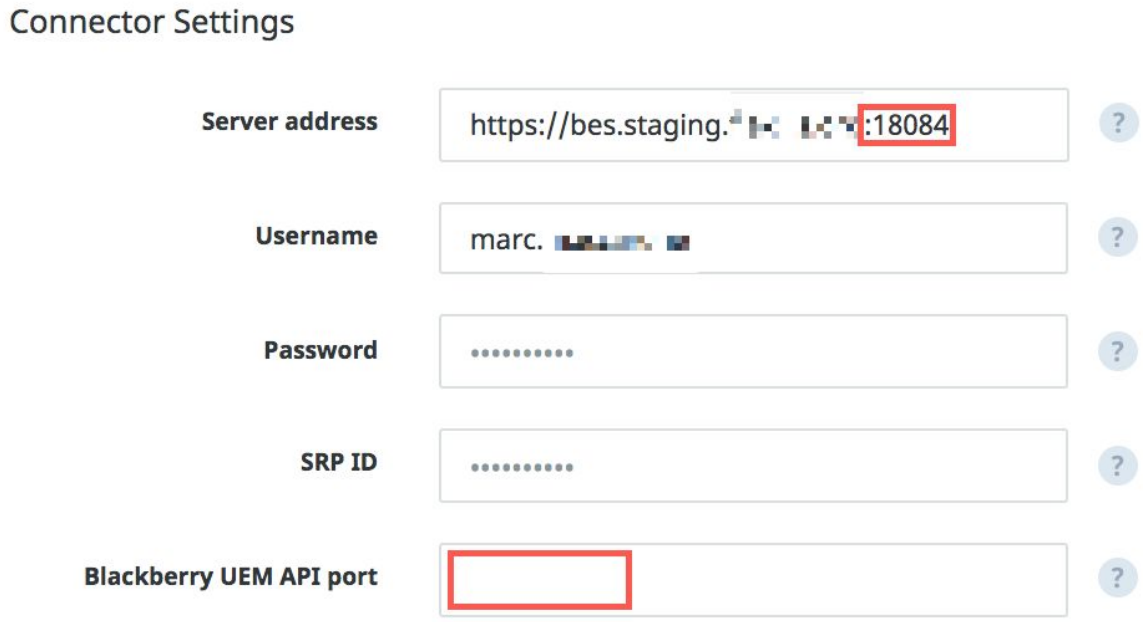
    a. Open the activation email you received when enrolling in BlackBerry UEM. It should be titled “Activating your device on BlackBerry UEM.”

    Your SRP ID is listed at the end of the **Server name** URL, after the slash:

Configuring the Connector in the Lookout MES Console

1. Log in to the Lookout MES Console at https://app.lookout.com.
2. In the left sidebar, click **System > Connectors** then click **Add Connector**.
3. Click **Blackberry UEM**.

4. Enter the following:



Field	Value
Server address	The public fully qualified domain name of your BlackBerry UEM server.
Username	The API User username and password from Creating an API User.
Password	
SRP ID	The SRP ID from Retrieving the BlackBerry SRP ID.
BlackBerry UEM API port	By default, the SOAP API port is **18084**. Ensure the ports is not blocked by your firewall. For additional information, see BlackBerry UEM listening ports in the BlackBerry documentation. Optionally, you can append the BlackBerry UEM API port to the **Server address** field and leave the configuration field for the port empty, as in the example above.

5. Click **Create Connector**.
   If creation is successful, the other configuration tabs become enabled.
6. Click **State Sync** and enter the user groups you created in Creating User Groups for Enrollment and Device State Sync:

Field	Value	Enabled?
Synchronize device status to BES	(toggle)	**ON**

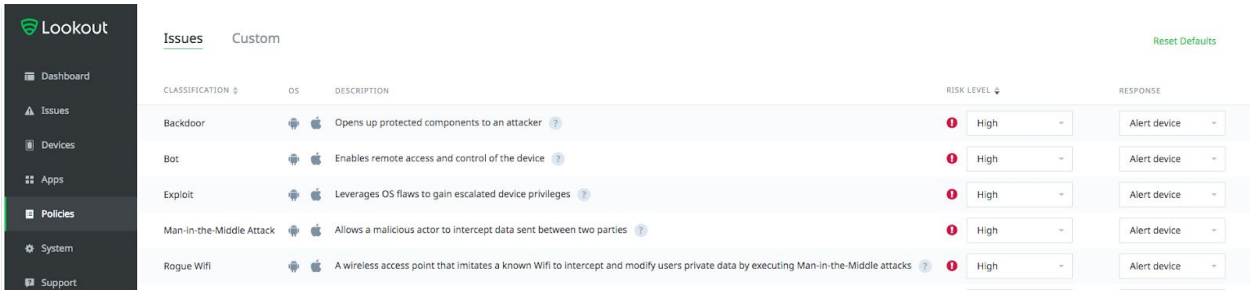
Devices that have not activated Lookout yet	`Lookout MES - Pending`	**ON**
Devices with Lookout activated	`Lookout MES - Secured`	**ON**
Devices on which Lookout is deactivated	`Lookout MES - Deactivated`	**ON**
Devices that have lost connectivity with Lookout	`Lookout MES - Disconnected`	**ON**
Devices with any issues present	`Lookout MES - Threats Present`	**ON**
Devices with Low Risk issues present	`Lookout MES - Low Risk`	**ON**
Devices with Medium Risk issues present	`Lookout MES - Moderate Risk`	**ON**
Devices with High Risk issues present	`Lookout MES - High Risk`	**ON**

If you choose not to synchronize a specific state, toggle off the corresponding item.

7. Click **Save Changes**.
8. Click **Error Management** and enter an email address for error reporting.
9. Click **Save Changes**.
   Once configured, you can view connector settings in MES on the **System > Connectors** page.

Configuring Threat Classification in Lookout Mobile Endpoint Security

Lookout classifies mobile threats of various types, so that you can match different classifications to the risk levels they represent for your organization. All threat classifications initially reflect the default threat levels assigned by Lookout. Users with Full Access to the Lookout MES Console can modify the settings from the Policies page:



When a device has issues present, Lookout adds it to the relevant user groups in UEM:

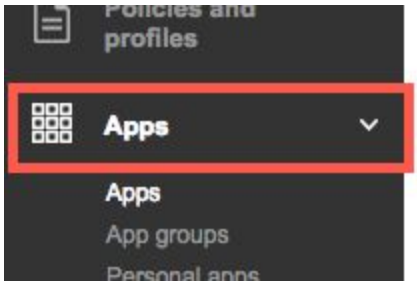
- **Lookout MES - Threats Present** (for any level of issue)
  and one of:
- **Lookout MES - High Risk**

- **Lookout MES - Moderate Risk**
- **Lookout MES - Low Risk**

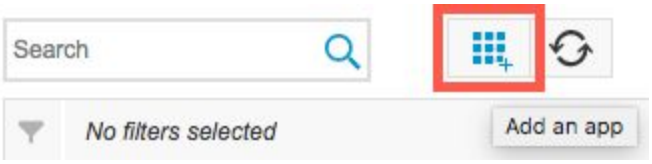
Adding Lookout for Work to BlackBerry UEM

Adding the Android Lookout for Work App

1. In the BlackBerry UEM menu bar, click **Apps**:

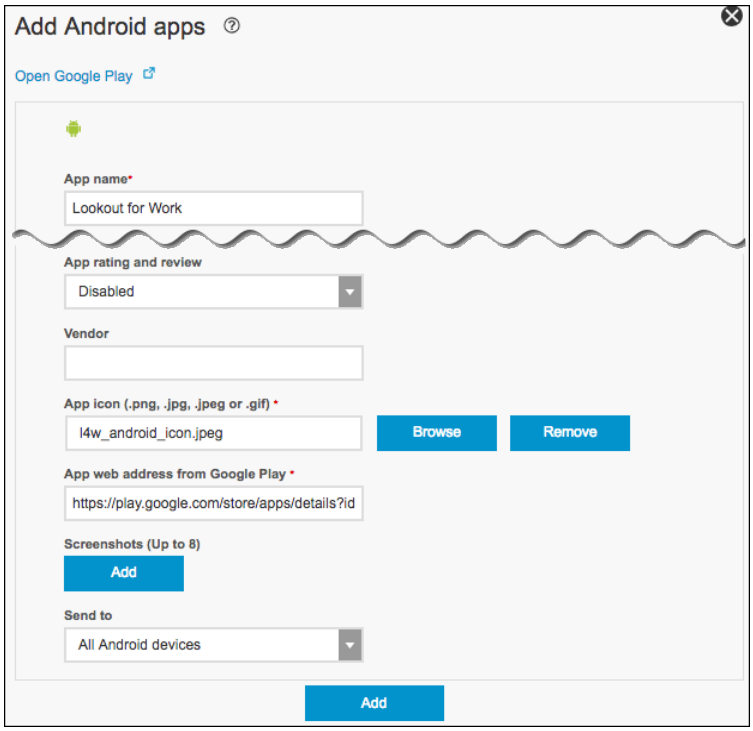


2. Click the Add App icon to the right of the search bar:



3. Select **Google Play**:

4. Set the following:

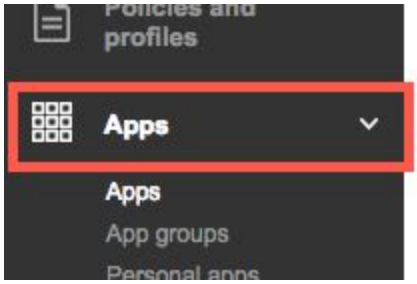


Field	Value
App name	`Lookout for Work`
Category	(Optional) Use an existing category or enter the name of a new one. Using categories allows you to filter the Apps list in UEM, and it organizes the Work Apps list by category on end user devices.
App rating and review	**Disabled**
App icon	Use the Lookout for Work icon from the Google Play link below.
App web address from Google Play	https://play.google.com/store/apps/details?id=com.lookout.enterprise
Send to	**All Android Devices**

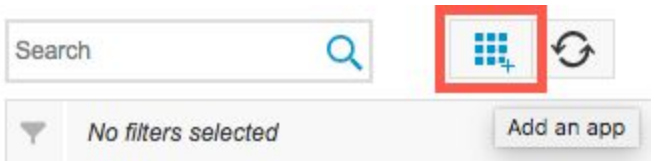
5. Click **Add**.

Adding the iOS App Store Lookout for Work App

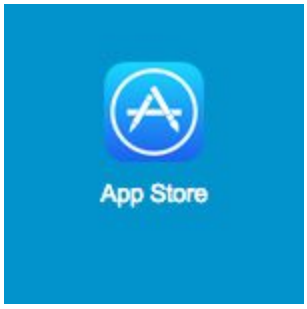
1. In the BlackBerry UEM menu bar, click **Apps**:



2. Click the Add App icon to the right of the search bar:

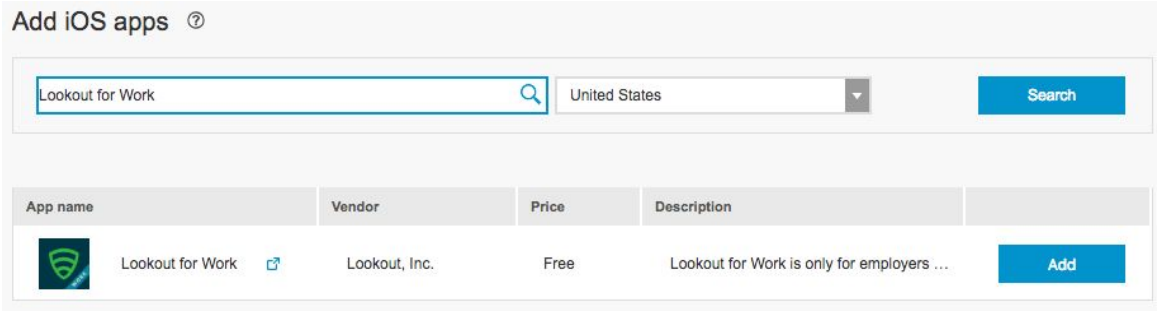


3. Select **App Store**:



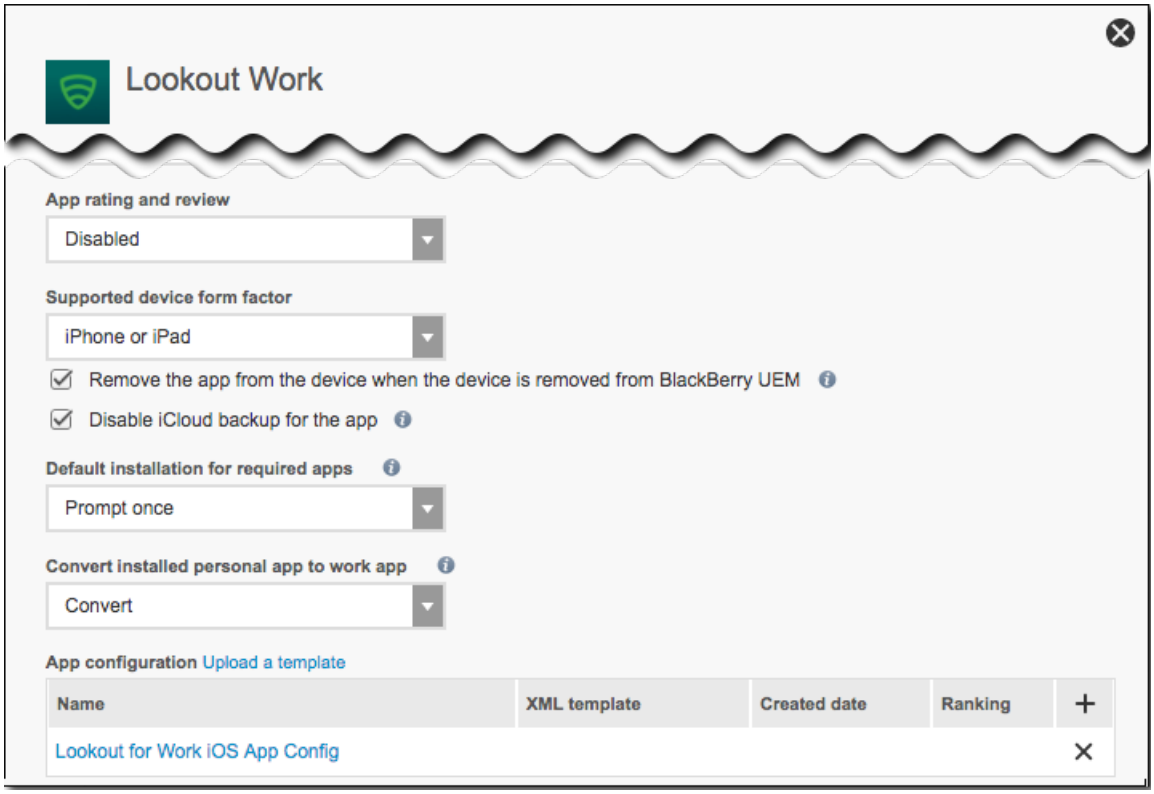
4. In the **App name, vendor, or URL** field enter `Lookout for Work`.

5. Select your country from the drop-down and click **Search**.
6. Locate the Lookout for Work app and click **Add**:



The app information screen appears.

7. Set the following:



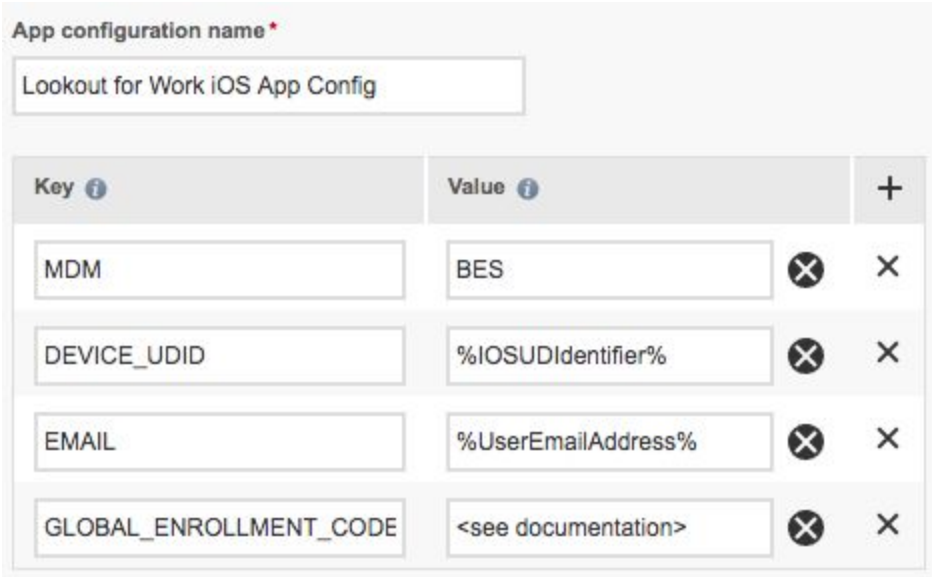
Field	Value
Category	(Optional) Use an existing category or enter the name of a new one. Using categories allows you to filter the Apps list in UEM, and it organizes the Work Apps list by category on end user devices.
App rating and review	**Disabled**
Supported device form factor	**iPhone or iPad**
Remove the app from the device	**Checked**

when the device is removed from BlackBerry UEM	
Disable iCloud backup for the app	**Checked**
Default installation for required apps	**Prompt once**
Convert installed personal apps to work app	**Convert**
App configuration	(See below)

8. To create the App configuration settings, click the **+** icon on the far right of the App configuration table and select **Configure manually**:

9. Click the **+** icon in the header and select **String** to create each new key-value:

10. Name the configuration `Lookout for Work iOS App Config` and create the following key-value pairs:



Key	Value

MDM	BES
DEVICE_UDID	%IOSUDIdentifier%
EMAIL	%UserEmailAddress%
GLOBAL_ENROLLMENT_CODE	Enter the 7 letter Enrollment Code from the **System > Account** screen in your Lookout MES Console. For example: 

IMPORTANT: These values are case-sensitive.

11. Click **Save**.
12. Click **Save**.

Adding the iOS In-House Lookout for Work App

Lookout distributes an In-House edition of the Lookout for Work iOS app outside of the Apple App Store. Before distributing this version of the app, you must sign it using your iOS Enterprise Developer Certificate.

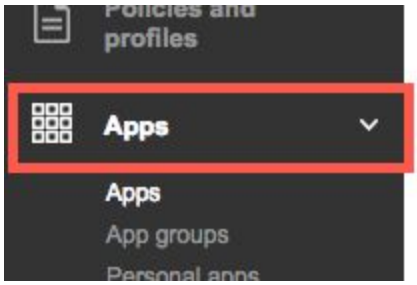
NOTE: You must use a Mac device to complete this task.

For details, see iOS App Re-Signing Process on the Lookout Enterprise Support Portal. Make note of your new Bundle ID (for example, `com.lookout.enterprise.AcmeInc`), as you'll need it to configure the app in UEM.

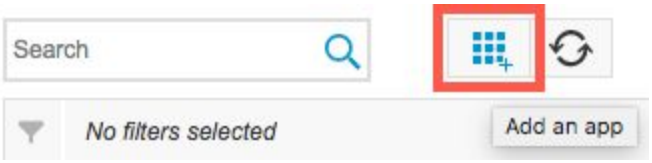
NOTE: It is important to upload the Lookout for Work IPA to the Mobile Endpoint Security Console (Step 6 in the document linked above), even though you are using BlackBerry UEM to distribute the app. This step validates that the app was re-signed correctly and also helps set up your iOS Sideloaded App Whitelist by automatically whitelisting apps that were signed with your iOS Enterprise Developer Certificate. This reduces the number of sideloaded app detections you see when you first roll out Lookout Mobile Endpoint Security (MES) to your test devices.

Once you have re-signed the app, you can add it to UEM:

13. In the BlackBerry UEM menu bar, click **Apps**:



14. Click the Add App icon to the right of the search bar:

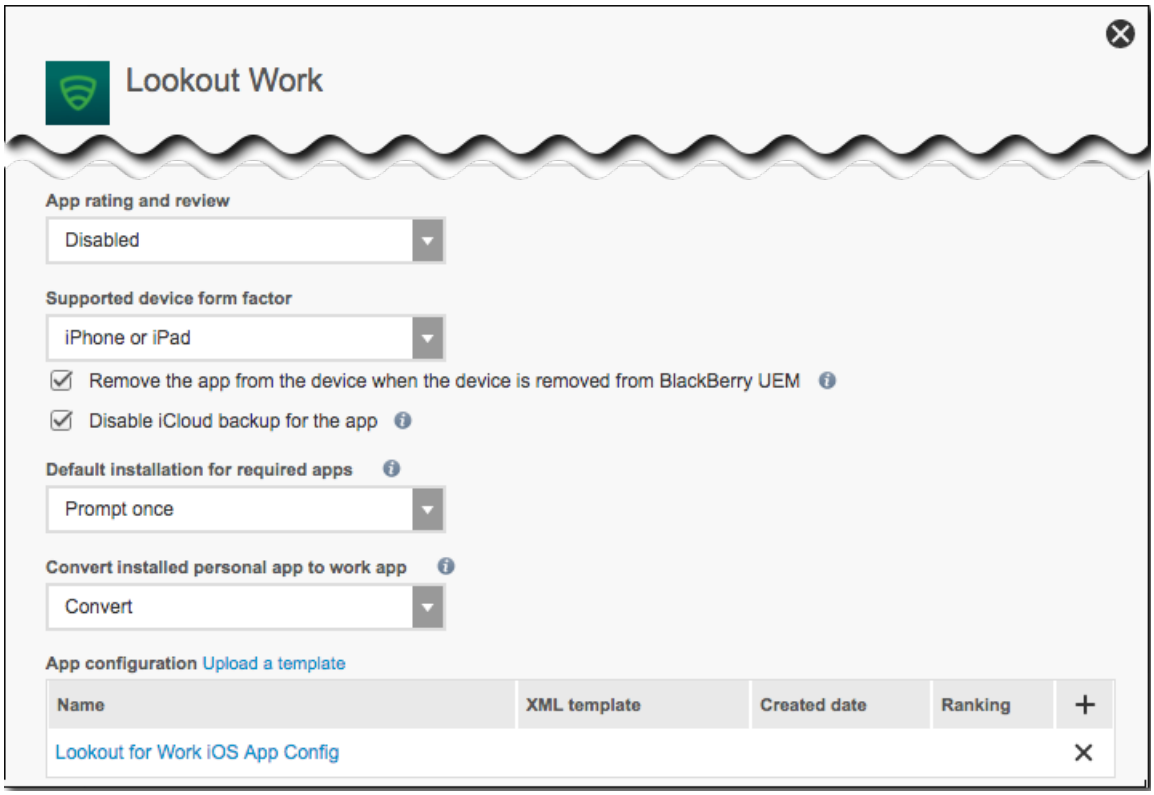


15. Select **Internal apps**:

16. Click **Browse** to upload your resigned Lookout for Work `.ipa` file, then click **Add**:

A loading spinner displays, then the app settings screen appears.

17. Set the following:

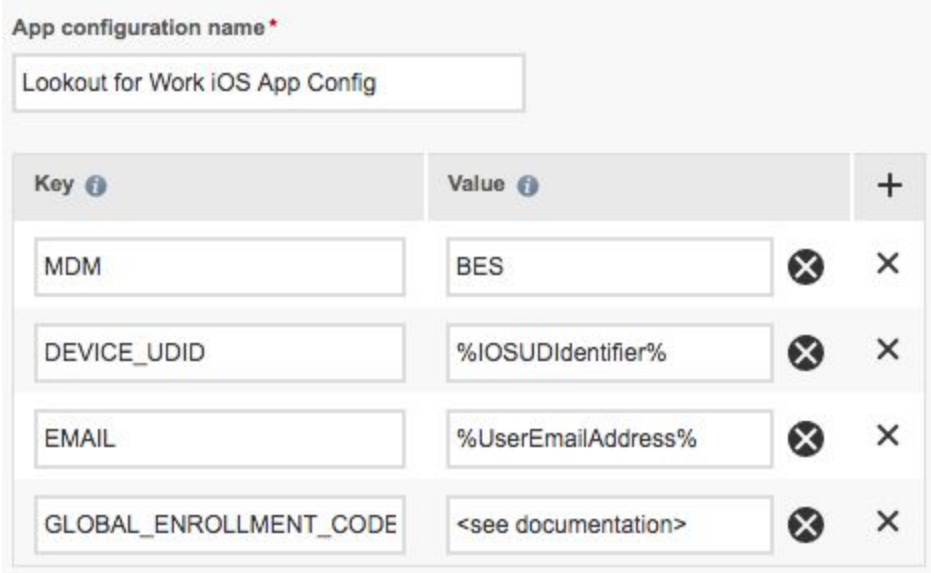


Field	Value
Category	(Optional) Use an existing category or enter the name of a new one. Using categories allows you to filter the Apps list in UEM, and it organizes the Work Apps list by category on end user devices.
App rating and review	**Disabled**
Supported device form factor	**iPhone or iPad**
Remove the app from the device when the device is removed from BlackBerry UEM	**Checked**
Disable iCloud backup for the app	**Checked**
Default installation for required apps	**Prompt once**
Convert installed personal apps to work app	**Convert**
App configuration	(See below)

18. To create the App configuration settings, click the **+** icon on the far right of the App configuration table and select **Configure manually**:

19. Click the **+** icon in the header and select **String** to create each new key-value:

20. Name the configuration `Lookout for Work iOS App Config` and create the following key-value pairs:



Key	Value
`MDM`	`BES`
`DEVICE_UDID`	`%IOSUDIdentifier%`
`EMAIL`	`%UserEmailAddress%`
`GLOBAL_ENROLLMENT_CODE`	Enter the 7 letter Enrollment Code from the **System > Account** screen in your Lookout MES Console. For example: 

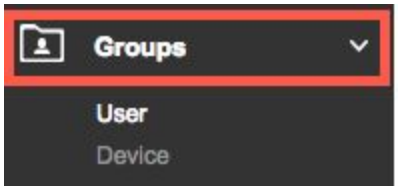
IMPORTANT: These values are case-sensitive.

21. Click **Save**.
22. Click **Save**.

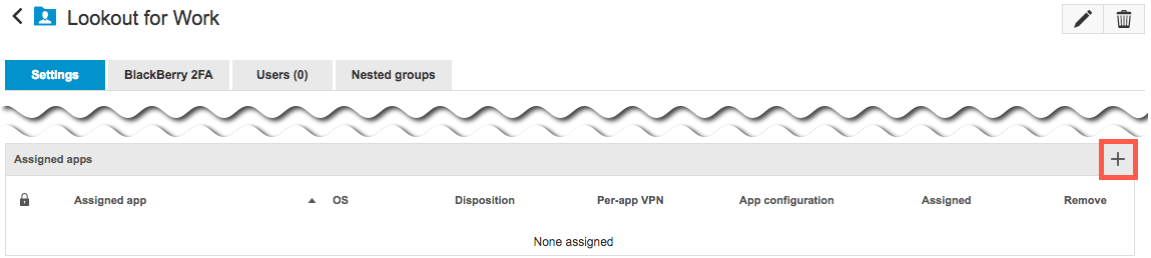
Assigning the App to User Groups

Once you have added the Lookout mobile app(s) to UEM, you can assign them to user groups from the Groups page.

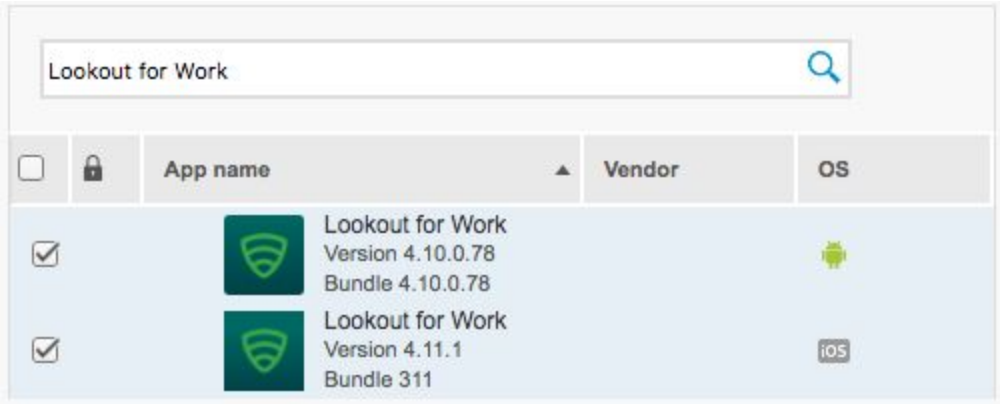
1. In the BlackBerry UEM menu bar, click **Groups**:



2. Select the `Lookout for Work` enrollment group you created in Creating User Groups for Enrollment and Device State Sync.
3. On the group page, click the **+** icon on the far right of the **Assigned Apps** list to assign an app:



4. Search for `Lookout for Work` and select the iOS and Android apps, then click **Next**:



5. Set the Disposition to **Required** for both apps, and select the **Lookout for Work iOS App Config** for the iOS app:

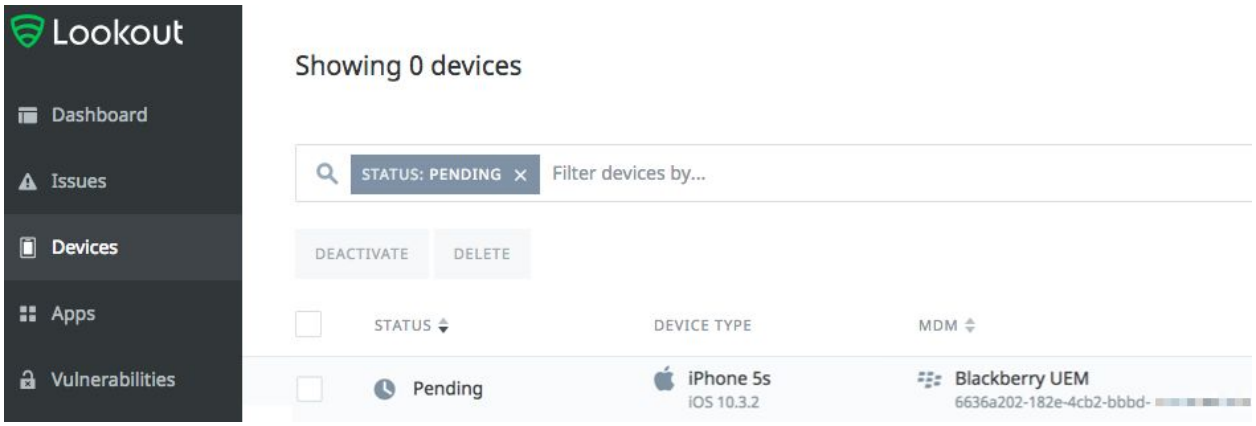
Marking the app as Required allows you to trigger a compliance policy as documented in Requiring the Lookout for Work App.

6. Click **Assign**.
   A success prompt displays and the apps display in the Assigned Apps list for the group.

Monitoring Enrollment and Activation

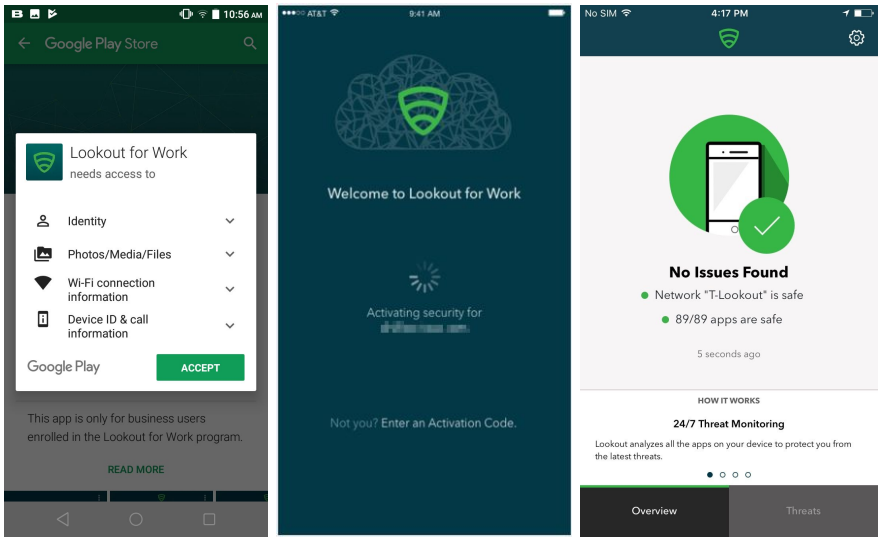
You can review the users and devices in the enrollment group in Blackberry UEM. Navigate to **Groups** and click the `Lookout for Work` enrollment user group, then click the **Users** tab to view included users and devices. Pending devices are listed in the `Lookout MES - Pending` user group.

Lookout MES polls BlackBerry UEM for enrolled devices and displays them on the Devices page of the console. Initially, discovered devices have a Status of “Pending.” As end users open and activate Lookout for Work, the activated devices move out of “Pending” status and change to “Secured.”



End User Device Activation

UEM distributes Lookout for Work to any user groups that have it as an assigned app (as documented in Assigning the App to User Groups). The device user must install the app, and then open it. On opening Lookout for Work, the user must click **Activate** if running a version of the app prior to 4.11 on iOS or 4.13 on Android. On later versions, the app activates automatically when opened and prompts for the required permissions (unless the user is on an Android device and your BES UEM deployment has accepted end user consent for Android Work devices).



NOTE: If the user declines permissions or closes the app, their device is still activated and secured in Lookout and in your MDM. Lookout cannot alert the user of issues without having device permissions, but it continues to report issues to the Lookout MES Console.

Configuring and Enforcing Compliance

In BlackBerry Unified Endpoint Management, you apply policies to User Groups and UEM enforces these policies at the user level. Policies are specific to an operating system (either iOS or Android for devices enrolled in Lookout).

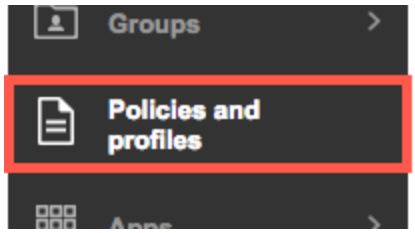
If a single user has multiple devices, and any of those devices is in violation of a policy that applies to a group that includes the user, then the user is considered out of compliance. As long as any of a user's devices has an active threat, they remain in the "Lookout MES - [Low/Medium/High] Risk" User Group.

Requiring the Lookout for Work App

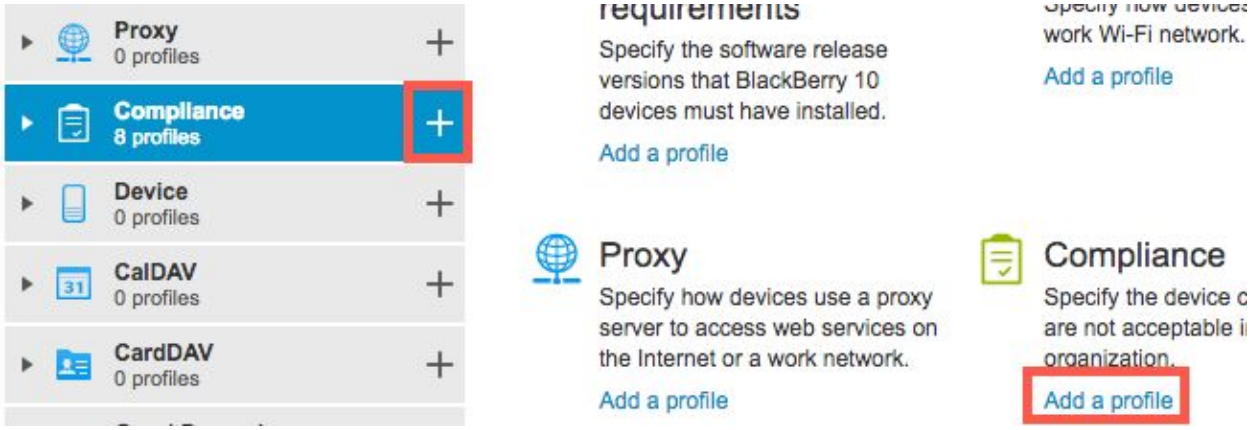
You can create a Compliance policy to require certain apps on mobile devices. Since you set Lookout for Work as Required when assigning groups (see Assigning the App to User Groups), devices without the app are flagged in violation of this policy.

If you already have a compliance policy for required apps, you do not need to follow the steps below. Devices that are missing Lookout for Work are handled in the same way as devices missing any other Required app.

1. In the BlackBerry UEM menu bar, click **Policies and profiles**:

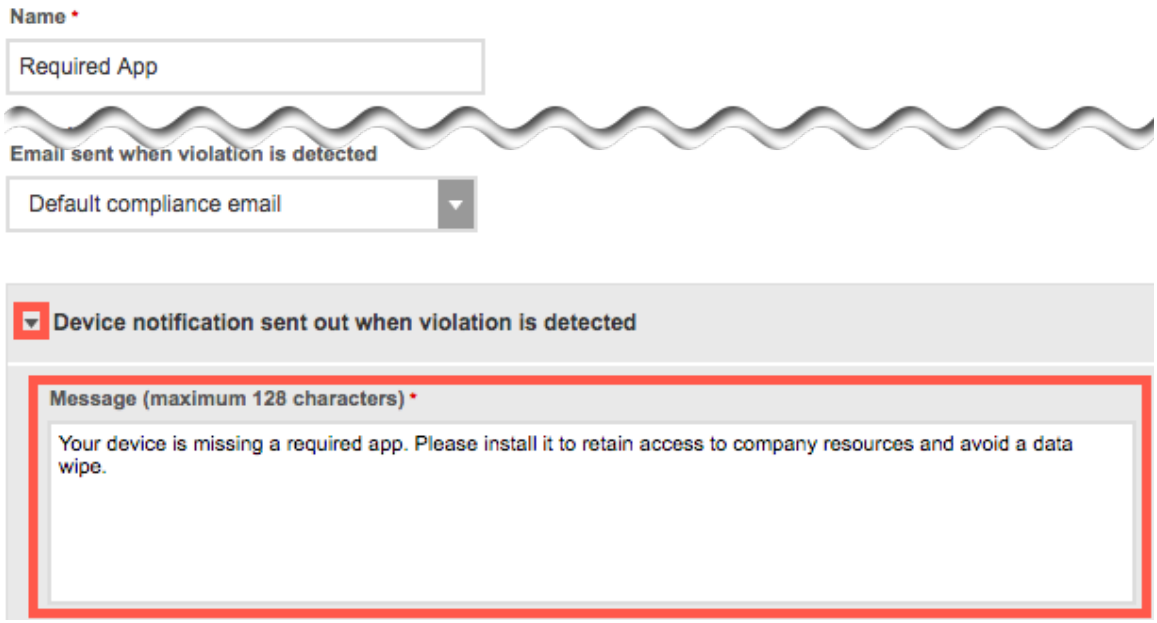


2. Click the **+** icon beside **Compliance** to create a new compliance policy, or click the **Add a profile** link under the **Compliance** description:



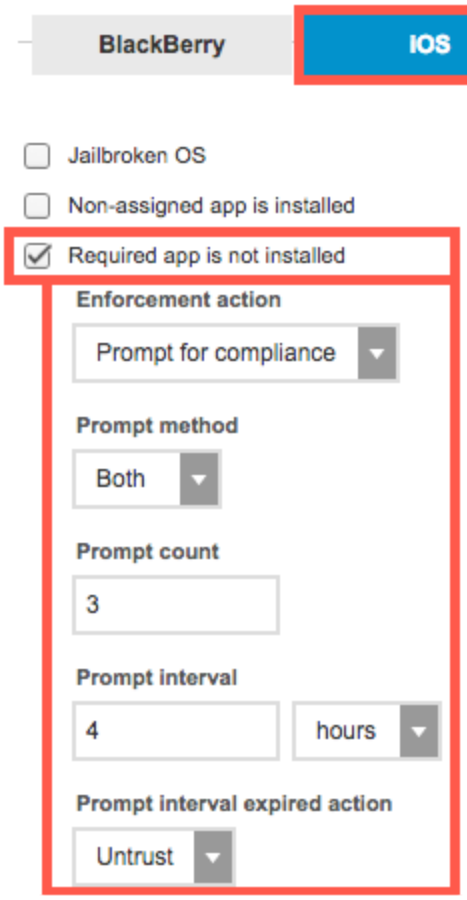
The Add a compliance profile screen displays.

3. Enter the following:



Field	Value
Name	Required App
Email sent when violation is detected	Default compliance email
Device notification sent out when violation is detected	Expand the field by clicking the arrow and input the following: `Your device is missing a required app. Please install it to retain access to company resources and avoid a data wipe.`

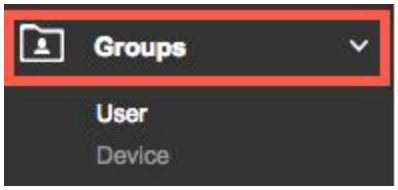
4. Click the **iOS** tab to open the iOS settings for this policy and enter the following:



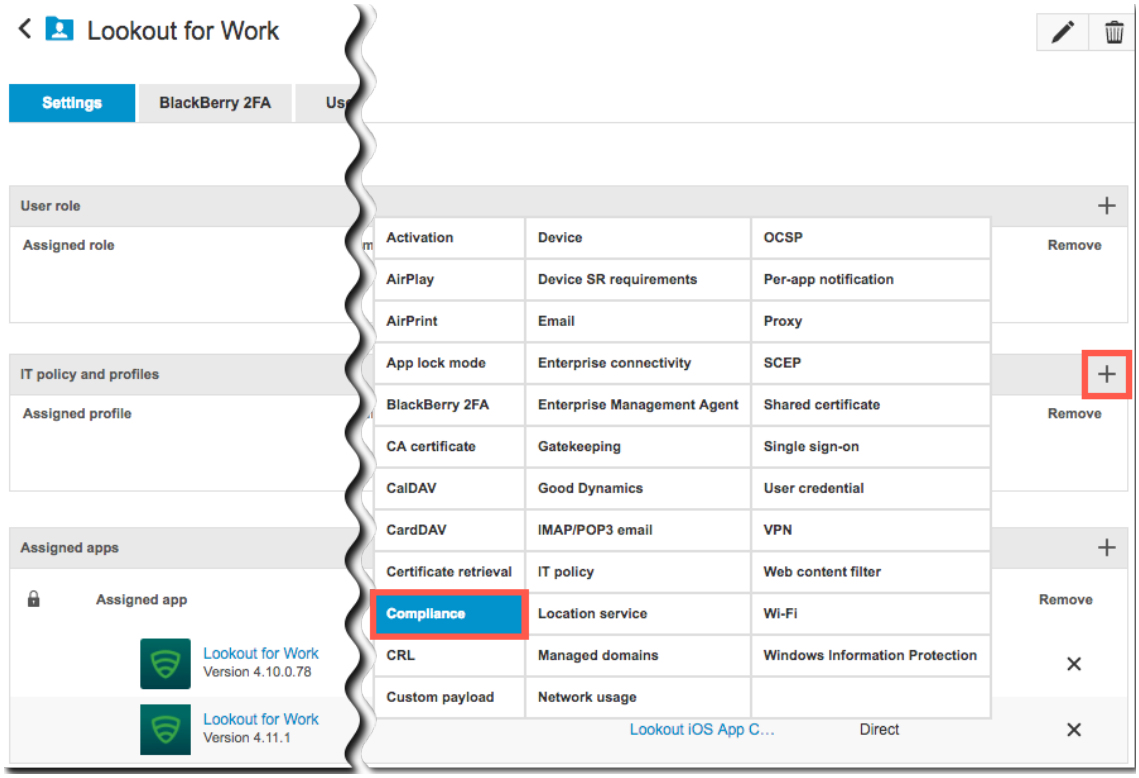
Field	Value
Required app is not installed	Checked. This enables the fields listed below.
Enforcement action	**Prompt for compliance**
Prompt interval expired action	**Untrust**

Configure the prompt method, count, and interval based on your organization's requirements.

5. Click **Android** to open the Android settings for this policy and enter the same settings you used above for iOS.
6. Click **Add**.
7. In the BlackBerry UEM menu bar, click **Groups**:



8. Select the `Lookout for Work` enrollment group you created in Creating User Groups for Enrollment and Device State Sync.
9. On the group page, click the **+** icon on the far right of the **IT policy and profiles** list and select **Compliance**:



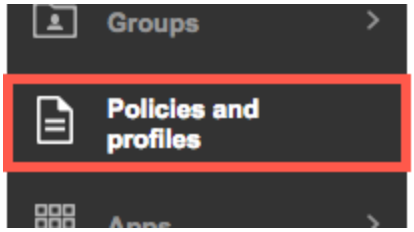
10. Select the **Required App** profile and click **Assign**.

Creating an Always-On Policies for Lookout Low, Medium, and High Risk User Groups in UEM

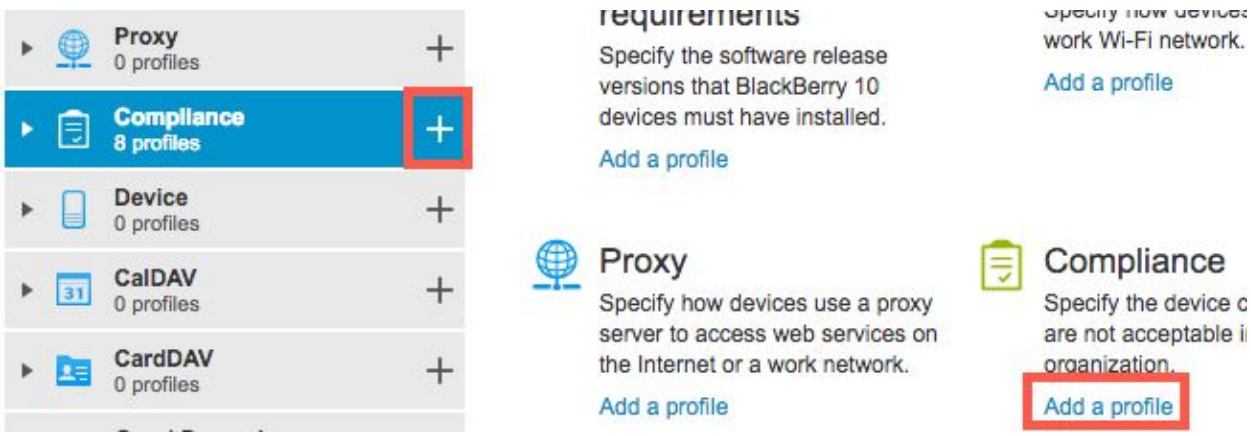
Users are automatically moved into the Low, Medium, or High Risk User Groups you created in Creating User Groups for Enrollment and Device State Sync based on their device threat state in Lookout. In order to apply compliance actions against these groups, you can create Low, Medium, and High Risk policies that use trigger that is always true. By applying an always-on policy to the Low, Medium, or High Risk group, you automatically apply it to any device in that User Group.

The steps below create an always-on policy for High Risk devices that immediately revokes trust:

1. In the BlackBerry UEM menu bar, click **Policies and profiles**:



2. Click the **+** icon beside **Compliance** to create a new compliance policy, or click the **Add a profile** link under the **Compliance** description:

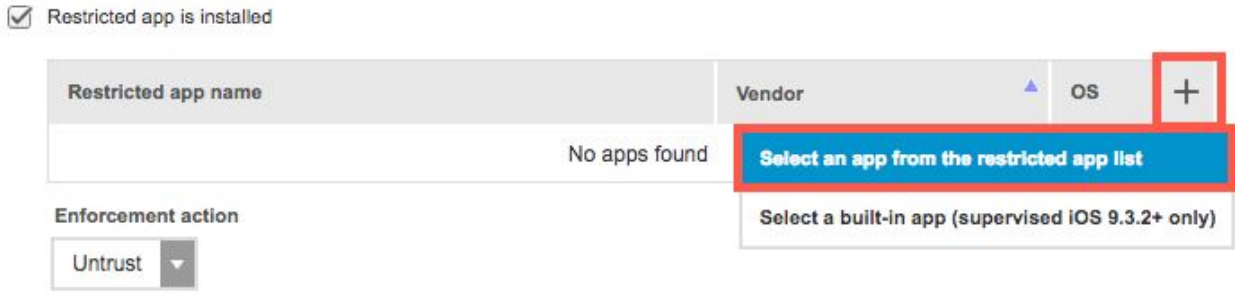


The Add a compliance profile screen displays.

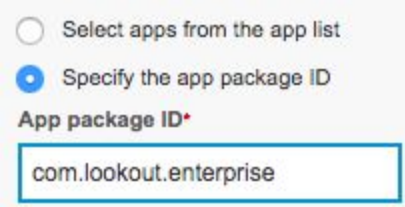
3. Enter the following:

Field	Value
Name	Lookout High Risk (iOS)
Email sent when violation is detected	Default compliance email
Platform	Click the **iOS** tab.
Restricted app is not installed	Checked. This enables the fields listed below.
Restricted App Name	(See below)
Enforcement action	**Untrust**

4. To set the **Restricted App Name**, click the **+** icon on the right of the list header, then click **Select an app from the restricted app list**:



5. Click **Specify the app package ID** and enter the ID.



Default IDs are listed below. If you are using an `.apk` file provided by Lookout Enterprise Support or if you are using the iOS In-House Edition, check the package ID by navigating to the UEM **Apps** list and clicking the Lookout for Work Android app to see details.

App Edition	Package ID
iOS App Store Edition	`com.lookout.work`
iOS In-House Edition	`com.lookout.enterprise.<YourCompanyName>` (for example, `com.lookout.enterprise.AcmeInc`)
Android Edition	`com.lookout.enterprise`

6. Click the **Android** tab and repeat Steps 3-5.
7. Check **Enforce compliance actions in the personal space**.
8. Click **Add**.
9. In the BlackBerry UEM menu bar, click **Groups**.
10. Select the `Lookout (High Risk)` group you created in Creating User Groups for Enrollment and Device State Sync.
11. On the group page, click the **+** icon on the far right of the **IT policy and profiles** list and select **Compliance**.
12. Select the **Lookout High Risk** profile and click **Assign**.

Optionally, repeat these steps to add policies for Medium and Low Risk devices and assign them to the corresponding user groups. Configure the **Enforcement action** based on your company's requirements.

Troubleshooting and Frequently Asked Questions

Enrolling, Activating, and Deactivating Devices

Why isn't auto-activation working for iOS?

Answer: Verify the following:

- Make sure you used the correct global enrollment code in the app config file you created in Adding the iOS App Store Lookout for Work App.
- Make sure you added the managed app config to the iOS app and not the Android App in UEM.
- Make sure you have added the managed app config to the "Lookout for Work" User Group in UEM.

Why aren't devices for deleted users automatically removed from the Lookout MES Console?

Answer: Removing a device from BlackBerry UEM retires it and sends a notification to the device prompting the user to remove Lookout for Work. If they cancel out of this prompt, you must resolve the issue manually.

Either the user must remove the app, or else you must compare active devices in UEM against those in the Lookout MES Console and remove the device via the Lookout MES Console Manage Devices module.