



# **Box for Android for Work with MobileIron Configuration Guide**



<b>Overview of Box for Android for Work with MobileIron .....</b>	<b>3</b>
<b>Feature Summary .....</b>	<b>3</b>
<b>How it Works .....</b>	<b>4</b>
<b>Getting Started .....</b>	<b>7</b>
Creating a MobileIron user account.....	7
Adding Box to the App Distribution Library.....	10
<b>Feature Configurations .....</b>	<b>12</b>
Baseline MobileIron Configurations.....	12
Baseline Box Configurations .....	14
Box use restricted to only MDM managed devices .....	14
OS and Box-provided file encryption.....	16
Force enterprise-only login.....	16
Additional Box Features .....	17
Limit number of devices accessing Box (device pinning).....	17
Remote app logout and data deletion.....	18
Force Box app-level passcode.....	19
Restrict cut, copy, and paste .....	20
Restrict printing.....	21
Disable offline access / saving content to device .....	22
Limit 'Open-in' into other apps (including Document Provider) .....	23
Pre-populate user email address on login screen .....	23
<b>User Experience Based on Box for Android for Work Setup .....</b>	<b>24</b>
<b>Requirements and Considerations.....</b>	<b>25</b>

## Overview of Box for Android for Work with MobileIron

Box for Android for Work is a multi-tenant application that enables customers to restrict the use of Box enterprise accounts to company-managed mobile devices secured by MobileIron.

The Box for Android for Work integration leverages MobileIron Core's APIs to perform a server-to-server validation of EMM credentials. The app is configured using the Android for Work configuration pushed to the app from MobileIron Server.

The Box for Android for Work supports both MobileIron Core and Cloud.

### Solutions for Device OS

<b>iOS</b>	Box for EMM is the recommended solution. Please see the available configuration guides: <ul style="list-style-type: none"><li>• <a href="#">MobileIron Core</a></li><li>• <a href="#">MobileIron Cloud</a></li></ul>
<b>Android</b>	For Lollipop and above (5.0+) please refer to this guide. If you require Ice Cream Sandwich support (4.0), please refer to the <a href="#">Box for EMM MobileIron (Wrapped) Guide</a> .

## Feature Summary

Box for Android for Work enables the following features. Specific configuration details are provided in the rest of the document. (See table of contents)

MobileIron Features
Remote app wipe
Jailbreak detection
Force device-level passcode
App Configuration
Android For Work LockDown Policy

Box Features
Box use restricted to only MDM managed devices
OS and Box-provided file encryption
Force enterprise-only login
Limit number of devices accessing Box (device pinning)*
Remote app logout and data deletion
Force Box app-level passcode*
Restrict cut, copy, and paste*
Restrict printing*
Disable offline access / saving content to device*
Limit 'Open-In' into any other apps (including Document Provider)*

Pre-populate user email address on login screen
---

\* Box administrative console setting

## How it Works

### Provisioning and Accessing Box for Android for Work with MobileIron

Box for Android for Work with MobileIron is currently supported with MobileIron Core and Cloud.

An enterprise admin works with a Box CSM to configure a Box for Android for Work instance. The standard Box app available in Google Play is then loaded into the Core App Distribution Library, and the admin sets up a Android for Work configuration to distribute to users' devices along with the app. This Android for Work Configuration contains unique identifiers that Box uses to authenticate users. MobileIron Core passes the necessary app configuration to the Box app, based on Google's [Android for Work](#) functionality.

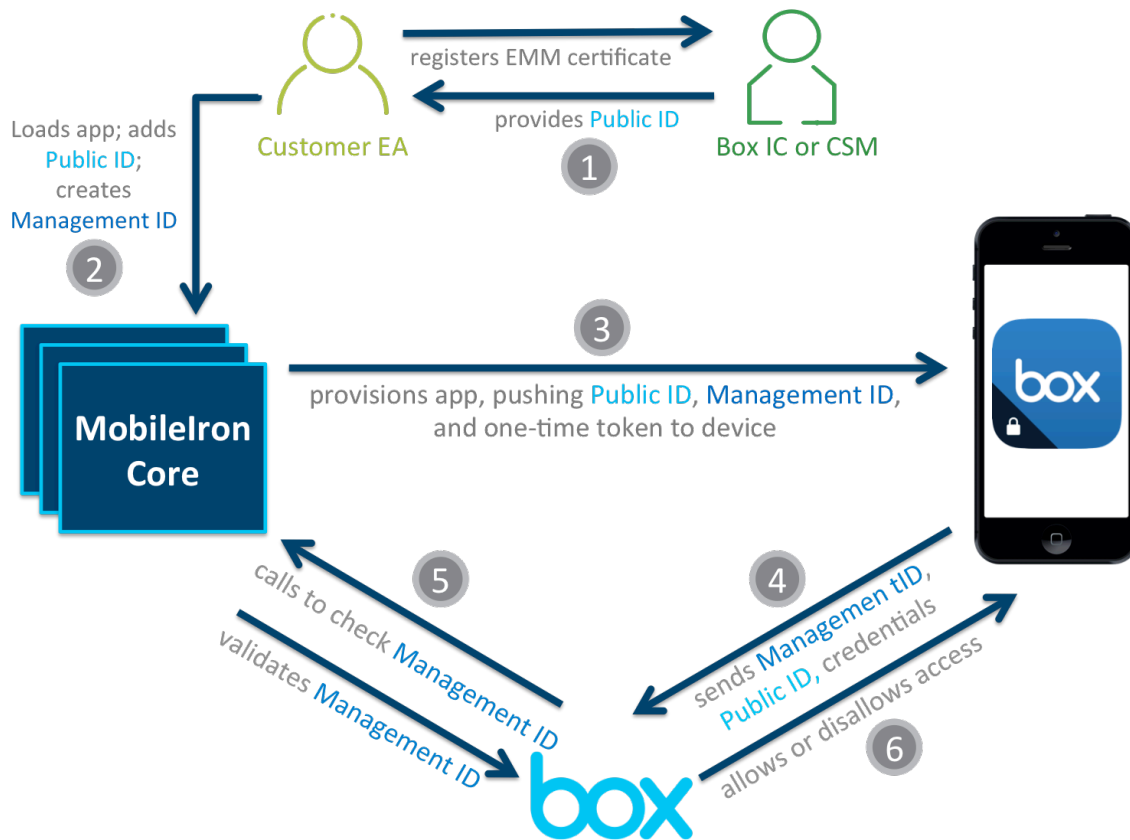
#### **Important Note:**

Customers should review the [MobileIron Core Device Management Guide for Android for Work](#) in detail before doing any of the below configuration steps. This document gives instruction on how to enable your MobileIron Core Server environment to support Android for Work.

### Authentication and Server-to-Server Validation

When a user requests to log in to the Box app, Box validates that the app was provisioned by MobileIron via a one-time token, and sends the customer's unique ID to the Box server, which will then validate if the enterprise and MobileIron combination is valid. Box for Android for Work also checks with the customer's MobileIron server that the user and device are still in compliance. Once MobileIron confirms that the device and user are actively managed by the enterprise, the user will be able to log in.

The following diagram outlines how Box performs server-to-server validation of EMM credentials and checks for managed app configurations.



1. The Box enterprise admin (EA) registers for Box for Android by working with their Box Implementation Consultant (IC) or Customer Success Manager (CSM), who provides a Public ID (in a plist file) to connect with MobileIron Core.
2. The Box app is uploaded into the MobileIron Core App Distribution Library and the admin creates a managed app config that includes the Public ID provided by Box (see instructions below). The MobileIron admin console specifies variables that will generate the values pushed to the application.
3. The Box app, which includes the Public ID, Management ID, and one-time token in the managed app config, is then distributed to user devices via the MobileIron Core enterprise app store. The one-time token is used to validate that the Box app was provisioned by MobileIron Core.

4. When a user requests to log in to Box, the app sends the user's login credentials, Public ID, and Management ID to the Box server. The Box server checks the user's login credentials and uses the Public ID to match the user to a MobileIron Core server.
5. The Box server calls the MobileIron Core server to validate the security posture or status of the device, using the Management ID.
6. If the Box and MobileIron Core servers successfully validate the login credentials, Public ID, and Management ID, the user is able to log in. If any of these checks fail, the user is unable log in.

## Getting Started

### Creating a MobileIron user account

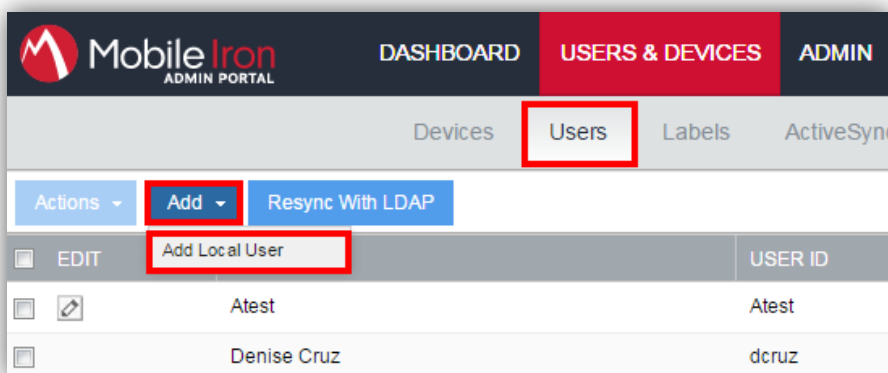
The Box enterprise admin (EA) should notify their Box Implementation Consultant (IC) or Customer Success Manager (CSM) about their interest in deploying Box for Android for Work with MobileIron, and should specify whether or not they are running Core or Cloud versions of the application.

If you are using MobileIron Cloud please skip to step 6.

After engaging Box, steps must be completed within MobileIron Core to provide the following information to the Box IC or CSM (where this information comes from will be covered in subsequent steps):

- API hostname (URL)
- User ID and password for MobileIron account (for Box to access MobileIron APIs)

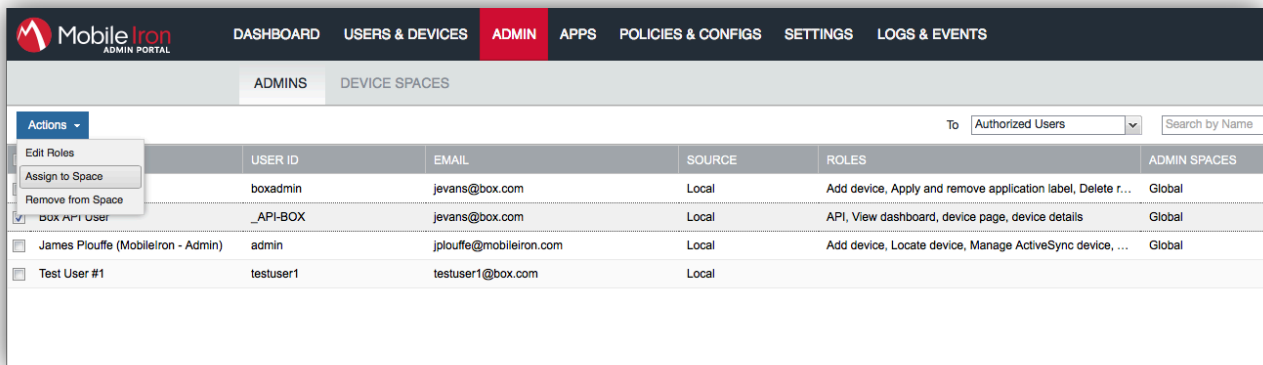
1. To create a MobileIron user account, log in to the MobileIron Core Admin Console and navigate to **USERS & DEVICES > Users > Add > Add Local User**.



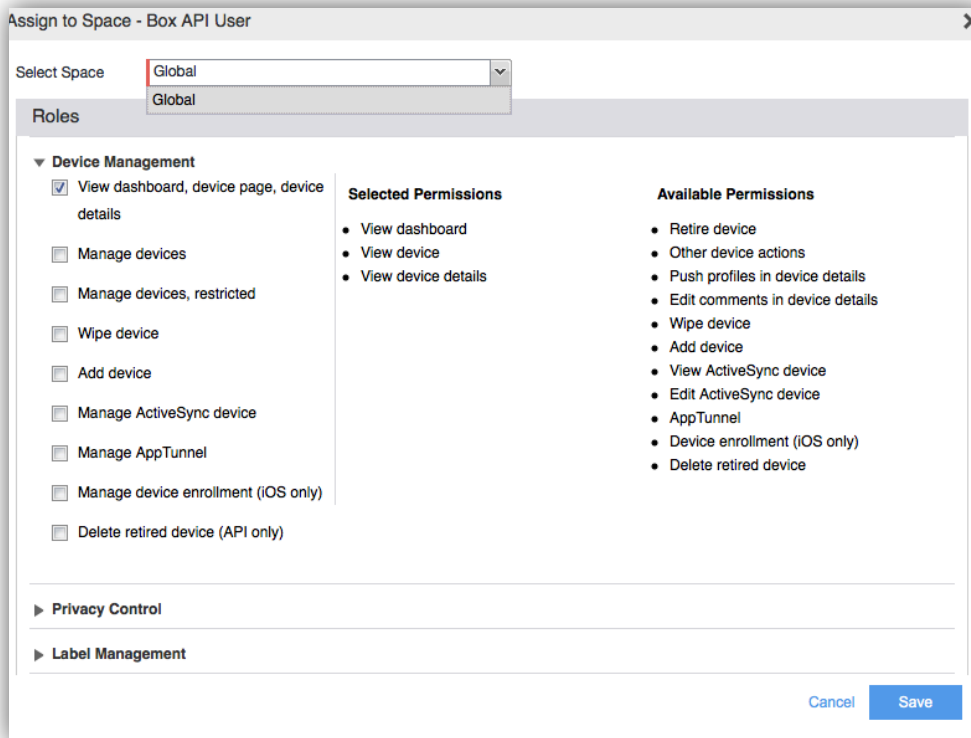
2. Complete the **Add New User** dialog using the appropriate values and click **Save**. The figure below illustrates possible values. It is recommended that display name clearly identify the purpose of the account.

The screenshot shows the 'Add New User' dialog box. It has a title bar with 'Add New User' and a close button. The dialog contains several input fields: 'User ID' with the value '\_API-BOX', 'First Name' with 'Box for', 'Last Name' with 'EMM', 'Display Name' with 'Box for EMM API User', 'Password' with a masked value '\*\*\*\*\*', 'Confirm Password' with a masked value '\*\*\*\*\*', and 'Email' with 'admin@yourdomain.com'.

3. To assign the required role to the user created in the previous step, navigate to **ADMIN > ADMINS**, select the checkbox next to the user created in Step 2, click on **Actions > Assign to Space**.



4. In the **Assign to Space** dialog box, select **Global** from the Select Space drop-down menu.



In the **Device Management** subsection of the **Roles** section, select the checkbox for **View dashboard, device page, device details**.

**Note:** This permission gives Box access to read device details via the MobileIron API. Box for Android for Work only uses this to query the compliance status of a device during the server-to-server validation step of a user log in.



5. Send the Box IC or CSM the User ID and password for the account created in the previous steps, and the Full-Qualified Domain Name (FQDN) for your MobileIron Core server or the URL for your Connected Cloud tenant, as shown in the examples below:

MobileIron Core customers will have a FQDN that looks like this:

**`https://mobileironserver.domain.tld`**

Connected Cloud customers will have a URL that looks like this:

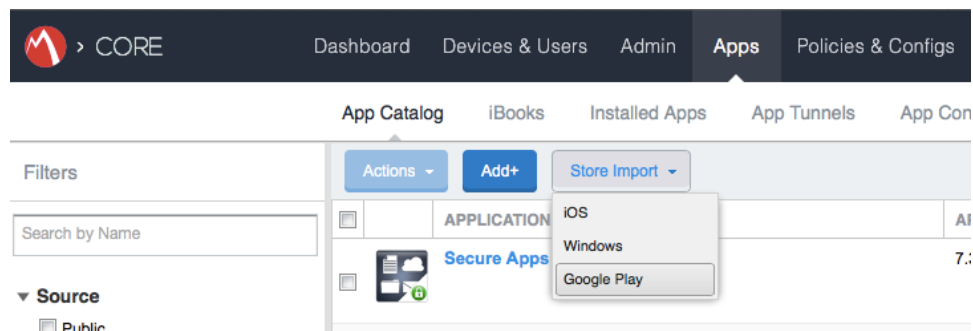
**`https://m.mobileiron.net/tenantname`**

In each case, Box only requires the portion of the URL displayed above.

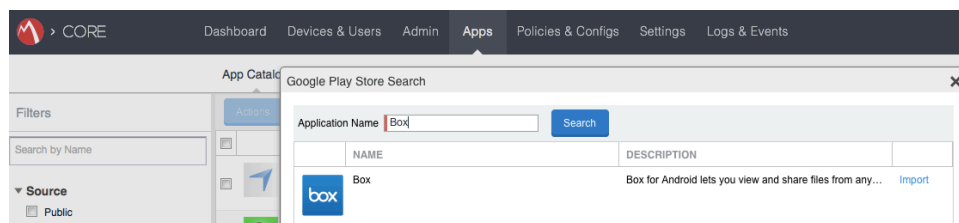
6. The Box IC or CSM registers this information in the customer's Box enterprise account, and provides the Box EA with a Public ID to use in MobileIron Core.

## Adding Box to the App Distribution Library

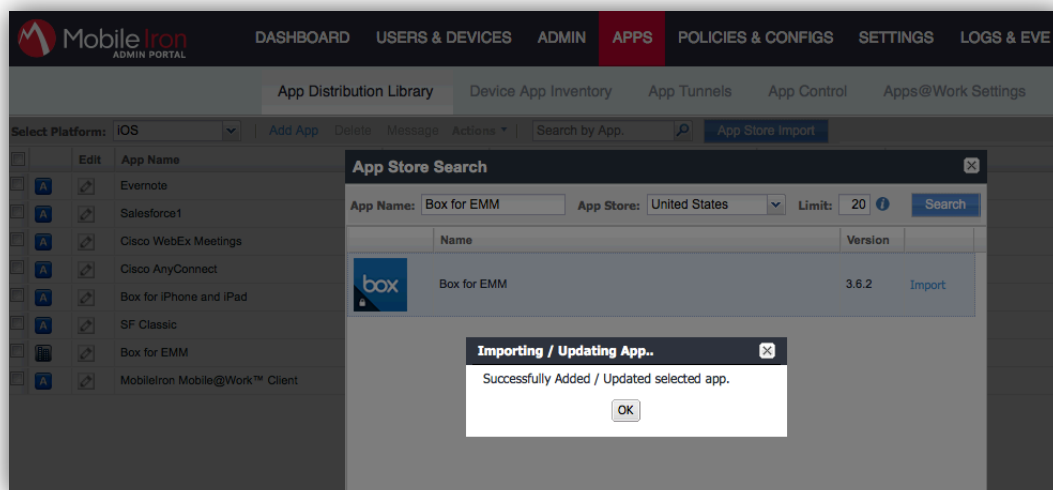
1. Add the Box app to the App distribution library. Navigate to **APPS > App Distribution Library** and select **Android** from the **Select Platform** drop-down menu.
2. Click the **App Store Import** button to the right of the **Search by App** field.



3. Type 'Box' in the **App Name** field of the **App Store Search** dialog and click the **Search** button.



4. Click the **Import/ Re-import** link in the far right column.
5. Click the **OK** button in the **Importing/ Updating App** dialog box.



6. Click the **Close (X)** button in the upper right corner of the **App Store Search** dialog box.
7. Select the min. OS Version (Android for Work native is supported on certain 5.0 devices and on all 6.0 devices)

Dashboard

Devices & Users

Admin

Apps

Policies & Configs

Settings

Logs & Events

App Catalog

iBooks


Installed Apps

App Tunnels

App Control

Apps@Work Settings

App Licenses

 **Box**

Application Name

Box

Min. OS Version

5.0

Display Version

3.7.5

Description

Winner of PC Magazine's Editors' Choice Award:  
"There are plenty of excellent file-syncing storage services, but, on Android, the Box app takes the cake."<p>Securely store, manage and share all your files, photos and documents with 10GB of free cloud storage from Box.</p>

☒ Feature this App in the Apps@Work catalog

Category

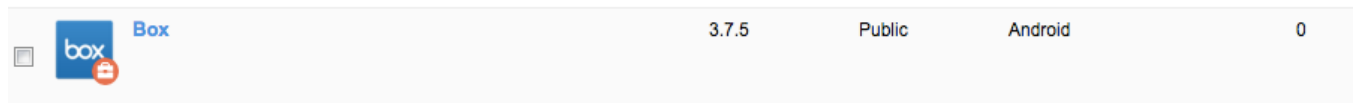
Add New Category

- Click **Next**
- Click **Finish**
- Select** the newly added app. **More Actions** -> **Apply Label**. Apply the label for devices that would like to use the Android for Work enabled Box App

## Feature Configurations

### Baseline MobileIron Configurations

1. Go to Apps -> Apps Catalog. Select Android in the Platform section. Select Box app and click on Box App.



2. Click on the Edit button.  
In the **Apps@Work Catalog** check the below box

#### APPS@WORK CATALOG

☒ Feature this App in the Apps@Work catalog

3. In **Android For Work**  
Check "install this app for Android for Work"  
Check "Silently install"

#### ANDROID FOR WORK

☒ Install this app for Android for Work

☒ Silently Install

☒ Block Uninstall

- **create accounts and set passwords**  
Allows the app to use the account authenticator capabilities of the AccountManager, including creating accounts and getting and setting their passwords.
- **install shortcuts**  
Allows an app to add shortcuts without user intervention.

4. In **Configurations** the following keys are automatically populated in the MobileIron Server. This information is provided by the Box application

#### CONFIGURATIONS ⓘ

User email  ⓘ

Public Id  ⓘ

Management Id  ⓘ

EMM Name  ⓘ

Billing Id  ⓘ

User email: \$EMAIL\$

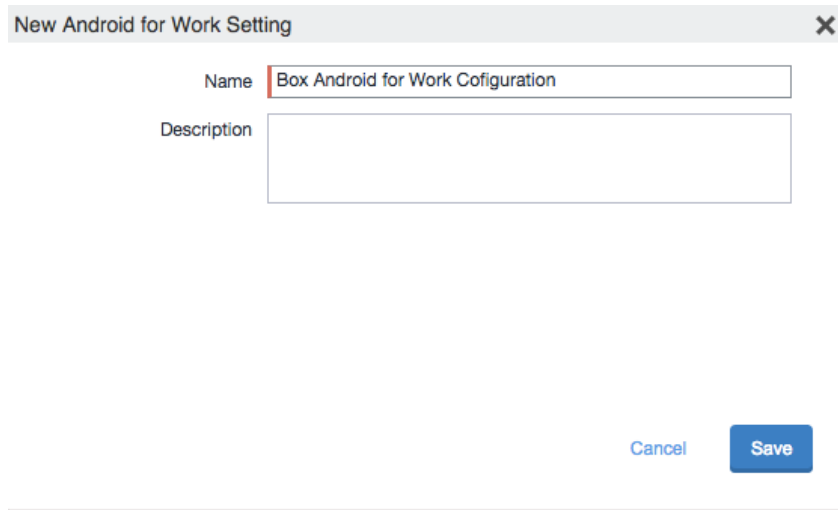
Public id: **Provided by Box**

Management id: \$DEVICE\_UUID\$

EMM Name: **MobileIron**

Billing Id: <**Not applicable for MobileIron**>

5. Policies & Configuration -> Configurations -> Add New -> Android -> Android for Work



New Android for Work Setting

Name: Box Android for Work Configuration

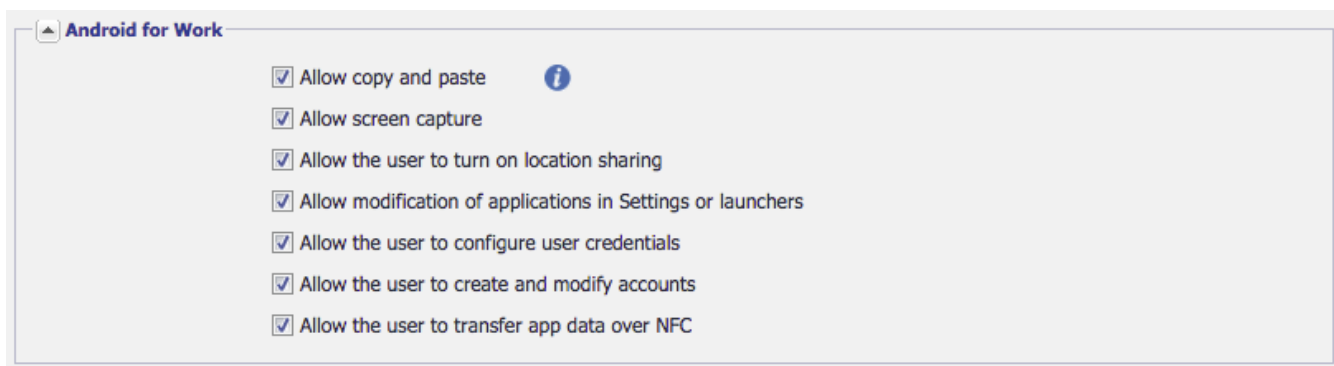
Description:

Cancel Save

6. Click **Save**
7. **Select** the newly created configuration **More Actions -> Apply Label**. Use the same label as applied to the App.

## Additional MobileIron Features

1. Enabling Android for Work Lock Down Policy
  - a) MobileIron Admin Portal: **Policies & Configuration -> Policies -> Default Lockdown Policy**.
  - b) Enable/disable the policies that apply



For additional controls please refer Chapter 2 of [MobileIron Core Device Management Guide for Android for Work](#).

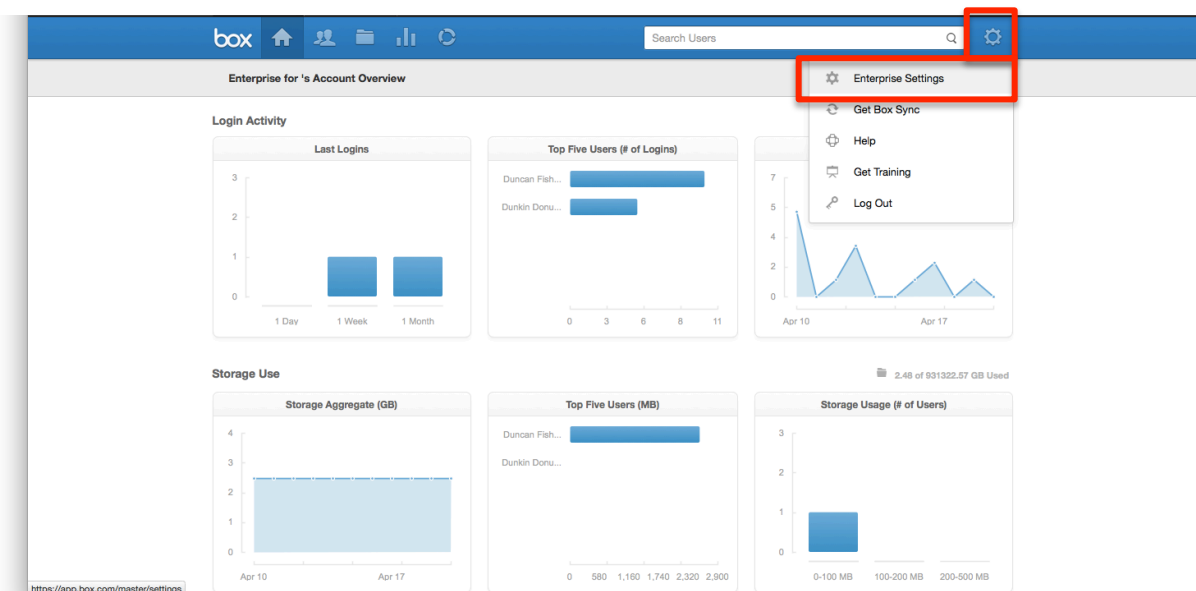
## Baseline Box Configurations

### Box use restricted to only MDM managed devices

This is a default feature of Box for Android for Work– users can't log into Box for Android for Work unless it is provisioned via the MobileIron admin console, using their enterprise credentials.

In order to enforce that users access Box through Box for Android for Work, configure the following settings:

#### 1. Go to Enterprise Settings

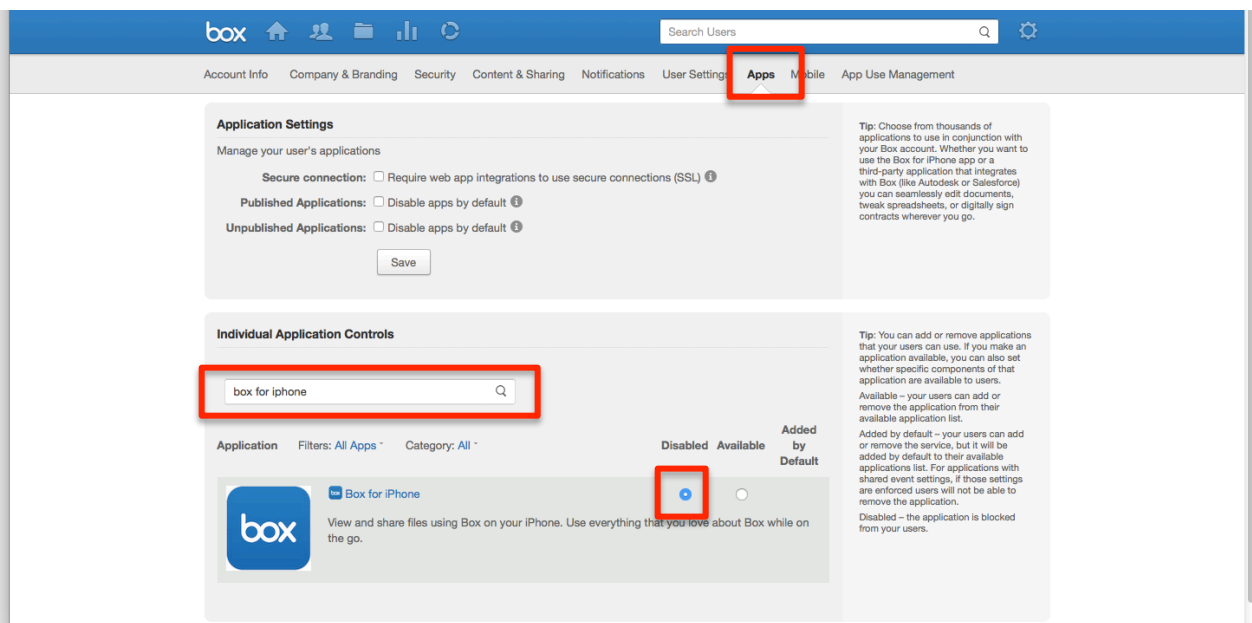


2. Go the **Apps** tab, then search for the following apps and disable them by toggling the radio button to 'Disabled':

- Box for iPhone
- Box for iPad
- Box for Android
- Box.com Mobile Site

Depending on other Box apps you might have deployed, and your Android solution, you may want to disable additional apps.

**Note:** Performing these steps will prevent users belonging to the enterprise's deployments of Box and MobileIron from logging into the regular (unmanaged) Box app and mobile site. **Make sure to notify your Box users before taking this step.**



3. On the same page, search for 'Box for Android EMM (Tablet)' and 'Box for EMM for iPhone' and ensure that the radio button is set to 'Available'.

Individual Application Controls

1 of 3

Search Applications

Application

Filters: All Apps

Category: Official Box

Disabled

Available

Added by Default

Box Capture

☐
☒

Box Edit

☐
☐
☒

Easily edit files on Box using the native applications installed on your computer.
 

Customize Options

Box for Android

☒
☐

The official Box for Android application.

Box for Android EMM (Tablet)

☐
☒

Box for Android EMM Tablet Also enables Android for Work on Lollipop devices.

Box for Android EMM Phone

☐
☒

Box for Android EMM Also enables Android for Work on Lollipop devices.

**Tip:** You can add or remove applications that your users can use. If you make an application available, you can also set whether specific components of that application are available to users.

Available – your users can add or remove the application from their available application list.

Added by default – your users can add or remove the service, but it will be added by default to their available applications list. For applications with shared event settings, if those settings are enforced users will not be able to remove the application.

Disabled – the application is blocked from your users.

## OS and Box-provided file encryption

1. Box automatically encrypts all data in transit to and from the app.
2. When the device has a passcode set, iOS automatically encrypts all device data at rest.
3. For security best practices, MobileIron and Box strongly recommend that customers enforce device passcode to ensure that data on the device is encrypted. See **Enforce device-level passcode** in the MobileIron Configurations section for implementation instructions.

## Force enterprise-only login

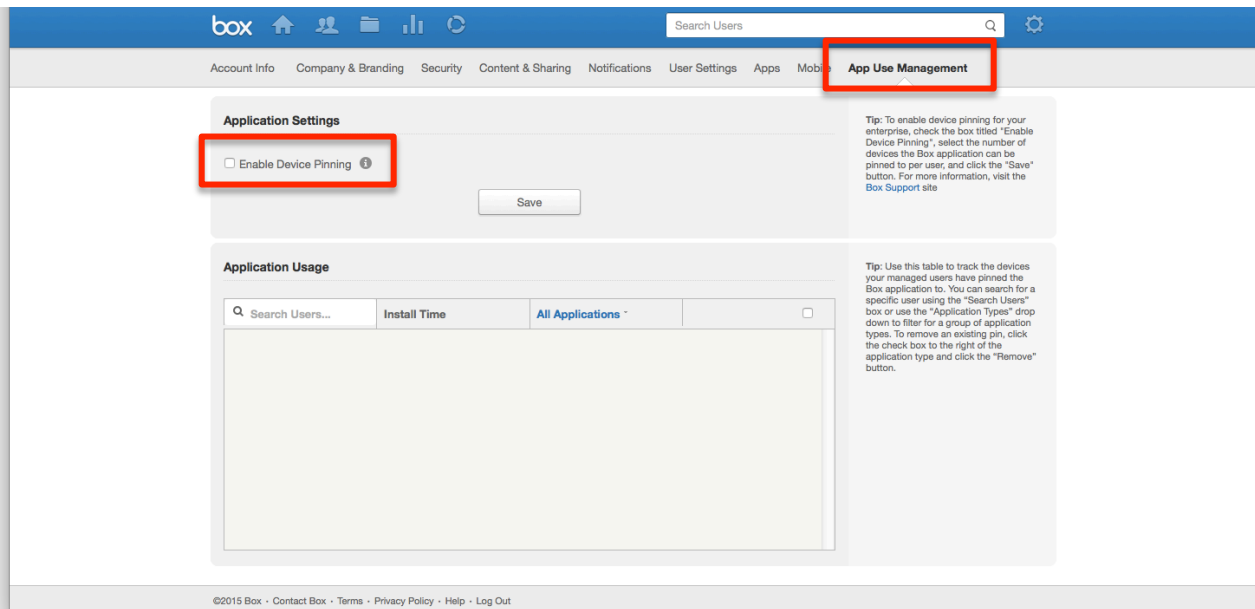
This is a core feature of Box for Android for Work – users can't log into the app except with an account associated with the enterprise that deployed it. This is done by default, with no admin action required.



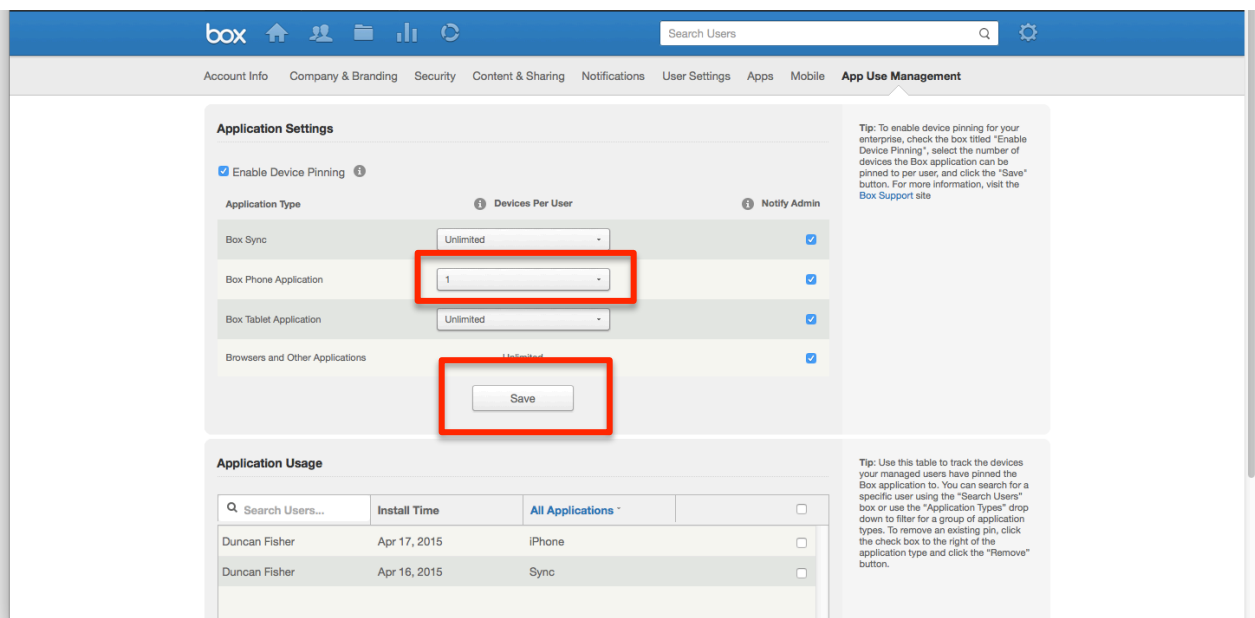
## Additional Box Features

### Limit number of devices accessing Box (device pinning)

1. Go to the **App Use Management** tab under **Enterprise Settings**
2. Check **Enable Device Pinning**.

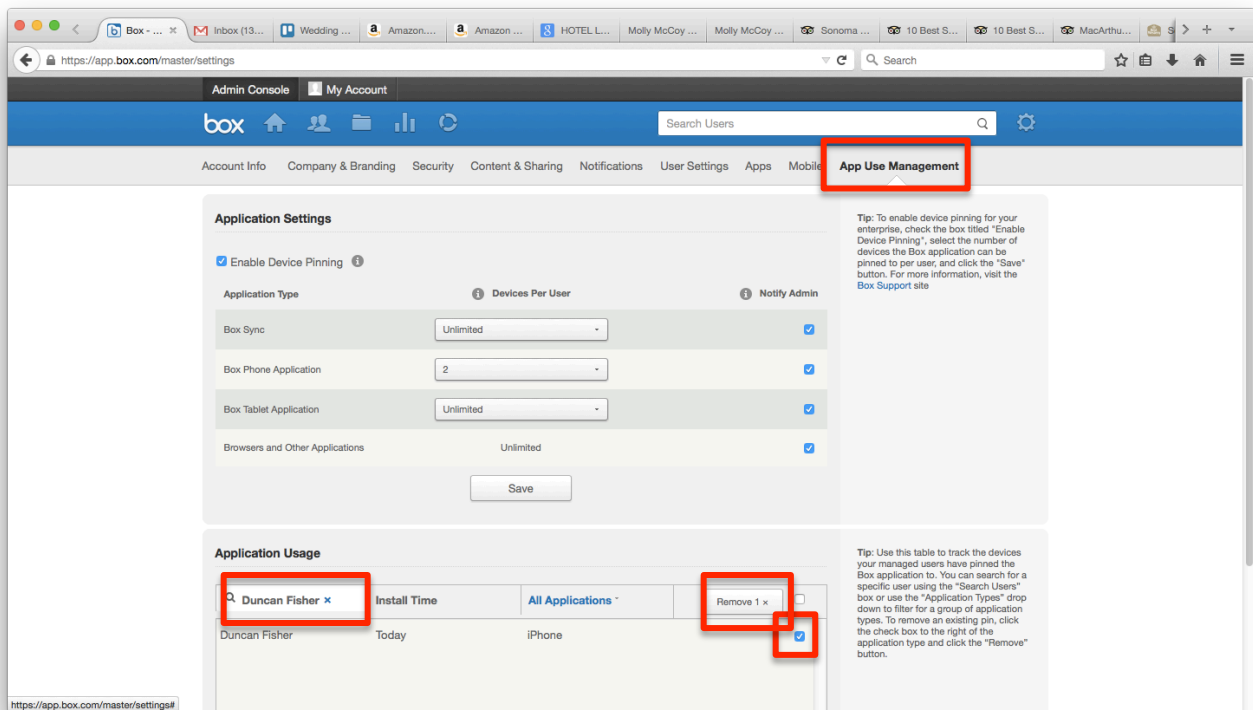


3. Select the **Devices per User** limit for the relevant apps.
4. Click **Save**.



## Remote app logout and data deletion

1. Device pinning must be enabled for this feature to work (see previous feature).
2. Go to the **App Use Management** tab under **Enterprise Settings**.
3. In the Application Usage section, search for the user(s)/application(s) to log out.
4. Check the checkbox next to that user/application.
5. Click the 'Remove 1 x' button to log the user out. If you have more than one user/application selected, the button will display the number you have checked instead.

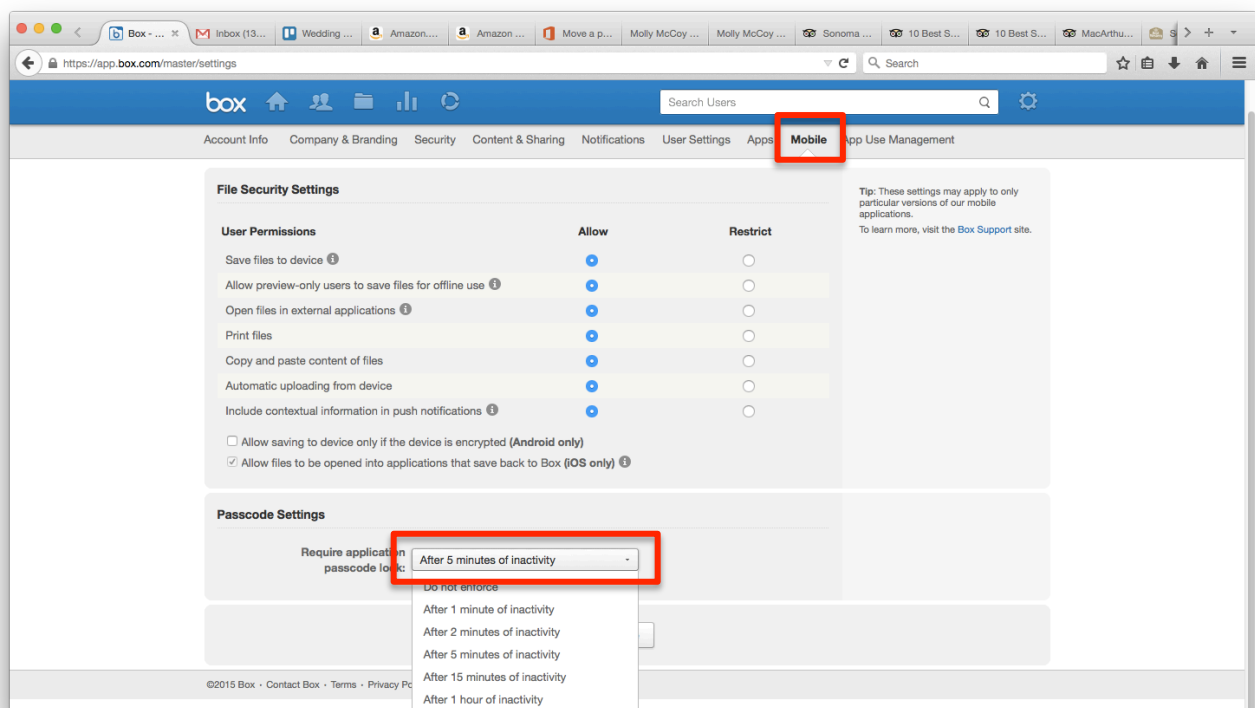


6. The next time Box for Android for Work comes into the foreground, the user will be logged out and all locally saved data will be deleted.

## Force Box app-level passcode

This setting requires users to enter a 4 digit passcode when they open Box for Android for Work at an interval specified by the admin.

1. Go to the **Mobile** tab under **Enterprise Settings**
2. In the Passcode Settings section, choose the desired lockout time from the 'Require application passcode lock' dropdown.
3. Click Save.

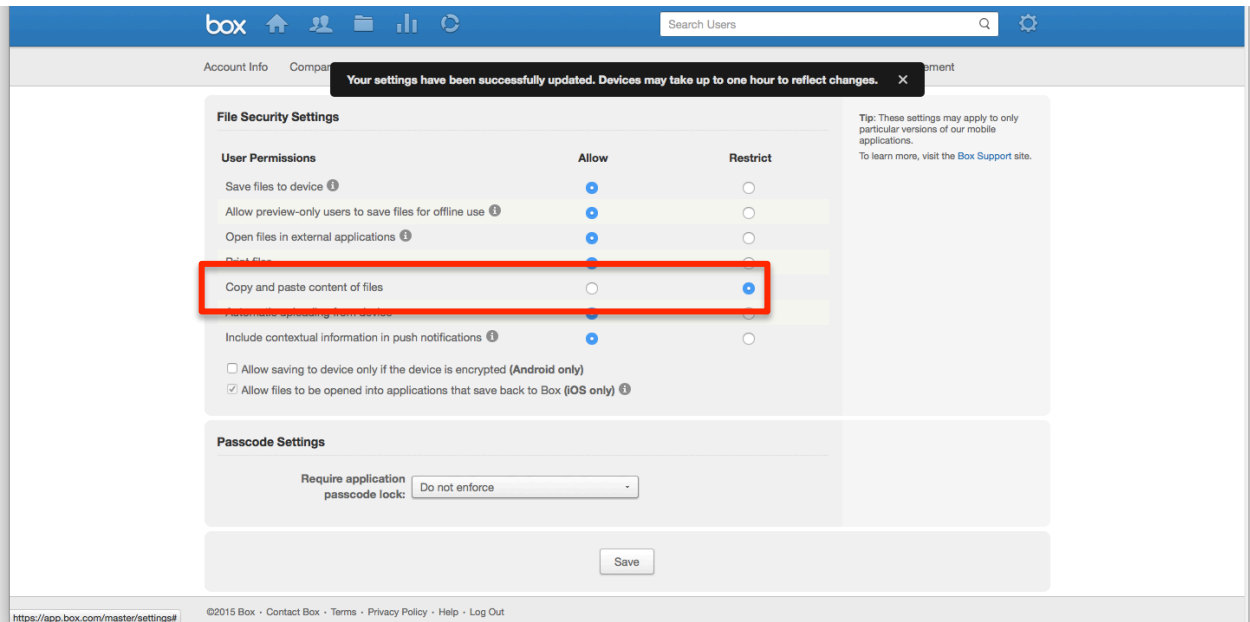


**Note:** For security best practices, MobileIron and Box recommend that customers must enforce device passcode to ensure that data on the device is encrypted. The Box app-level passcode gates the Box for Android for Work app but does not encrypt device data. See **Enforce device-level passcode** in the Additional MobileIron Features section to enforce the device passcode.

## Restrict cut, copy, and paste

This setting prevents users from copying content out of the Box for Android for Work app.

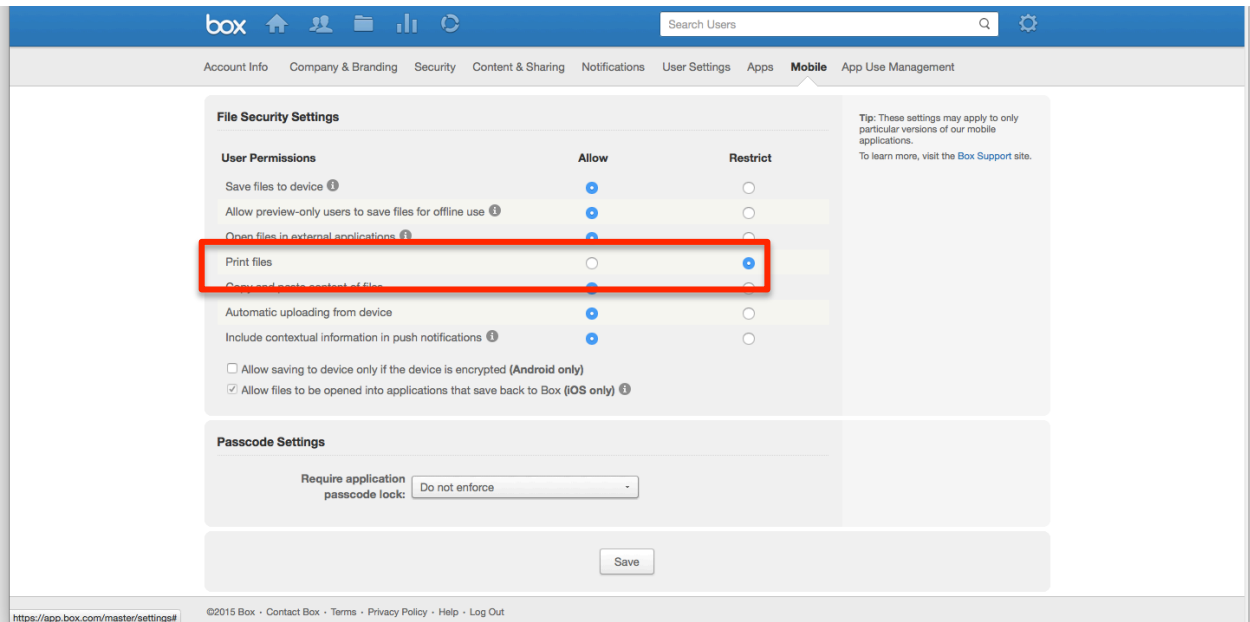
1. Go to the **Mobile** tab under **Enterprise Settings**
2. Set 'Copy and paste content of files' to Restrict.



## Restrict printing

This setting prevents users from printing from the Box for Android for Work app.

1. Go to the **Mobile** tab under **Enterprise Settings**
2. Set 'Print files' to Restrict.

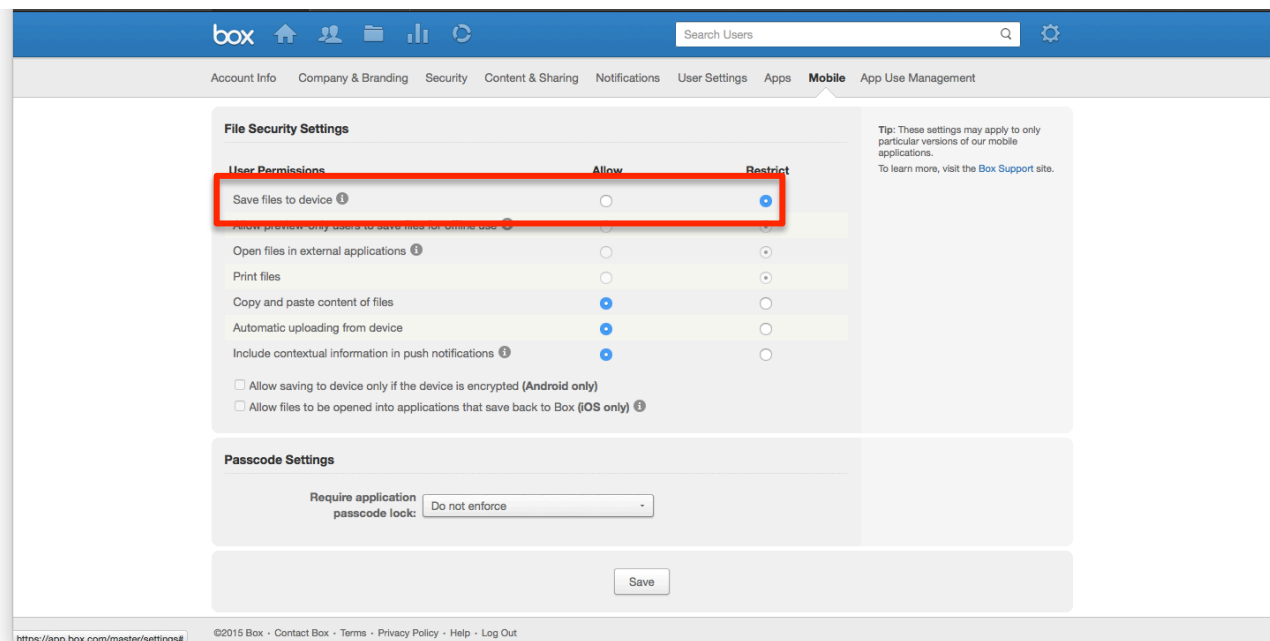


## Disable offline access / saving content to device

This setting prevents users from saving files for offline access within the Box for Android for Work app.

1. Go to the **Mobile** tab under **Enterprise Settings**

2. Set 'Save files to device' to Restrict.

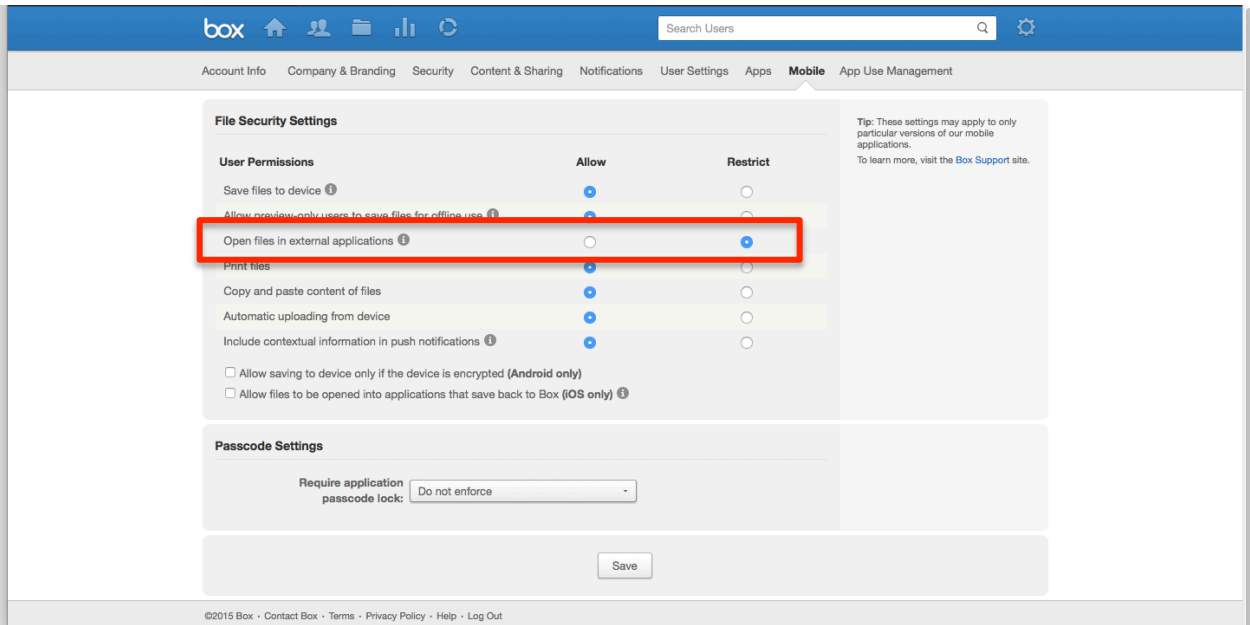


## Limit 'Open-in' into other apps (including Document Provider)

There are different ways for customers to manage 'Open-in' functionality with Box for Android for Work

1. To disable all 'Open-in' and Document Provider functionality, preventing users from opening content from Box for Android for Work in other applications, follow the steps below.

- a. Go the **Mobile** tab under **Enterprise Settings**
- b. Set 'Open files in external applications' to Restrict



## Pre-populate user email address on login screen

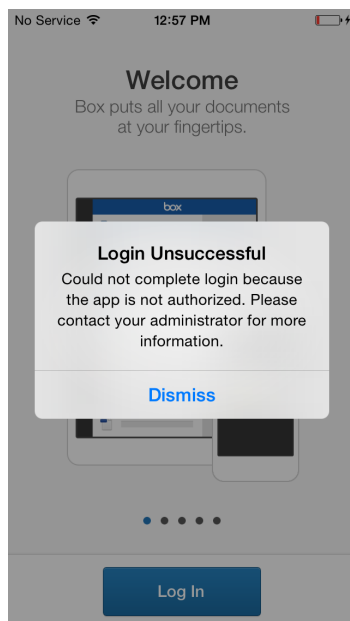
If this feature is enabled, a user's email address (the one associated with their MobileIron account) will be pre-populated when they arrive on the Box for Android for Work login screen. See step 11 in the Baseline MobileIron Configurations section for implementation instructions.

## User Experience Based on Box for Android for Work Setup

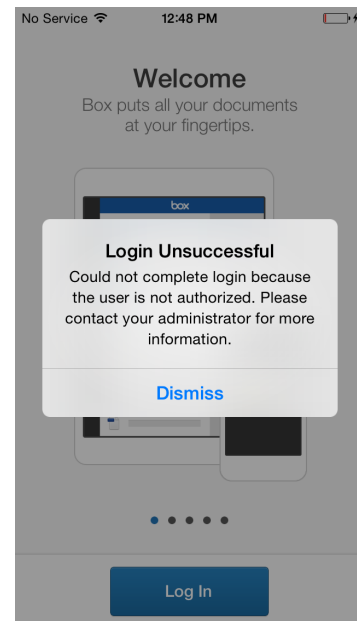
#	Scenario	Behavior
1	A user managed by MobileIron requests to log in to the Box for Android for Work app that has been provisioned via MobileIron.	The user can log in successfully.
2	A user managed by the MobileIron requests to log in to the Box for Android for Work app that they installed directly from an app store.	The Public ID configured in the MobileIron admin console will not have been pushed to the Box for Android for Work app that was installed from an app store, and the user will be unable to log in.
3	A user backs up the app on one device and attempts to restore it on another device	The Box for Android for Work app validates the one time token to determine whether the app was provisioned via MobileIron, and the user will be unable to log in.
4	A Box user not part the enterprise deployment of Box for Android for Work requests to log in to the Box for Android for Work app provisioned via MobileIron.	The user's login info will not match the Public ID on the Box for Android for Work app, and the user will be unable to log in.
5	A user fakes an app installation through the Android for Work provider and pushes dummy managed configurations to the app.	Box checks with the MobileIron server to confirm whether the Management ID is valid and matches that of an authorized user, and the user will be unable to log in.

**Users unable to log in to Box for Android for Work will receive the following messages:**

See the [Box Help article](#) for more details.



App is not authorized (scenarios 2, 3)



User is not authorized (scenarios 4, 5)



## Requirements and Considerations

- All device users in MobileIron Core/Connected Cloud must be managed. A managed user is an enterprise user who has been configured and registered with the company's MobileIron Core/Connected Cloud. The Box for Android for Work solution does not support an enterprise deployment in which users are both managed and unmanaged. This design enables the app to be updated via a typical app upgrade rather than by deleting an older version of an app in order to install a newer version of that app.
- Box for Android for Work allows users to login to with their personal Box credentials while keeping the data separate from their corporate account.
- Box for Android for Work supports devices running Lollipop (5.0) and above.
- Box for Android for Work with MobileIron is supported by MobileIron Core/ Connected Cloud version 7.1 and above.