

Box for Android for Work with MobileIron Configuration Guide

| Overview of Box for Android for Work with MobileIron | |
|---|----|
| Feature Summary | |
| How it Works | |
| Getting Started | 7 |
| Creating a MobileIron user account | 7 |
| Adding Box to the App Distribution Library | |
| Feature Configurations | |
| Baseline MobileIron Configurations | |
| Baseline Box Configurations | |
| Box use restricted to only MDM managed devices | |
| OS and Box-provided file encryption | |
| Force enterprise-only login | |
| Additional Box Features | |
| 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 other apps (including Document Provider) | |
| Pre-populate user email address on login screen | |
| User Experience Based on Box for Android for Work Setup | 24 |
| Requirements and Considerations | 25 |

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

| | Box for EMM is the recommended solution. Please see the available configuration |
|---------|--|
| :05 | guides: |
| 105 | MobileIron Core |
| | MobileIron Cloud |
| | For Lollipop and above (5.0+) please refer to this guide. If you require Ice Cream |
| Android | Sandwich support (4.0), please refer to the Box for EMM MobileIron (Wrapped) |
| | <u>Guide</u> . |

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)* |

* 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 <u>Android for Work</u> functionality.

Important Note:

Customers should review the <u>MobileIron Core Device Management Guide for Android for Work</u> 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)
- To create a MobileIron user account, log in to the MobileIron Core Admin Console and navigate to USERS & DEVICES > Users > Add > Add Local User.

| Mo | bile Iron | DASHBOARD | USERS | ADMIN | |
|-----------|----------------|-----------|-------|--------|------------|
| | | Devices | Users | Labels | ActiveSync |
| Actions + | Add 👻 Resync V | Vith LDAP | | - | |
| EDIT | Add Local User | | | Us | SER ID |
| | Atest | | | Ate | est |
| | Denise Cruz | | | dc | ruz |

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.

| Add New User | | × |
|------------------|----------------------|---|
| User ID | _API-BOX | |
| First Name | Box for | |
| Last Name | EMM | |
| Display Name | Box for EMM API User | |
| Password | ••••• | |
| Confirm Password | ••••• | |
| Email | 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**.

| | DASHBOARD | USERS & DEVICES | ADMIN | APPS | POLICIES & CONFIGS | SETTINGS | LOGS & EVENTS | |
|-----------------------------------|-----------|-----------------|---------------|------|--------------------|----------|---|------------------|
| | ADMINS | DEVICE SPACES | | | | | | |
| Actions - | | | | | | | To Authorized Users | ✓ Search by Name |
| Edit Roles | USER ID | EMAIL | | | SOURCE | ROLES | | ADMIN SPACES |
| Assign to Space | boxadmin | jevans@ | box.com | | Local | Add de | evice, Apply and remove application label, Delete | r Global |
| Dox AM User | _API-BOX | jevans@ | box.com | | Local | API, Vi | iew dashboard, device page, device details | Global |
| James Plouffe (MobileIron - Admir | n) admin | jplouffe@ | mobileiron.co | om | Local | Add de | evice, Locate device, Manage ActiveSync device, | Global |
| Test User #1 | testuser1 | testuser | @box.com | | Local | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

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

| sign to Space - | Box API User | | | |
|---|---|--|---|----|
| elect Space | Global | ~ | | |
| Roles | Global | | | |
| Device Manag | gement | | | |
| View dash details Manage de Manage de Wipe device Add device Manage A Manage A Manage de Manage de Delete reti | board, device page, devic evices evices, restricted ce e ctiveSync device ppTunnel evice enrollment (iOS only red device (API only) | Selected Permissions View dashboard View device View device details | Available Permissions Retire device Other device actions Push profiles in device details Edit comments in device details Wipe device Add device View ActiveSync device Edit ActiveSync device AppTunnel Device enrollment (iOS only) Delete retired device | |
| Privacy Contr | rol | | | |
| Label Manage | ement | | | |
| | | | Cancel Sav | re |

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

- 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.

| 🐴 > CORE | Dashboard | Devices & Us | sers Admin | Apps | Policies a | & Configs |
|----------------|-----------|--------------|----------------|--------|------------|-----------|
| | App Catal | og iBooks | Installed App | os App | o Tunnels | App Con |
| Filters | Actions | - Add+ | Store Import 👻 | | | |
| Search by Name | | APPLICATION | iOS | | | A |
| ▼ Source | | Secure Apps | Google Play | | | 7.: |
| Public | | | | | | |

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

| 🐴 > CORE | Dashboard | Devices & Users Admin | Apps Policies & Configs | Settings Logs & Events | |
|-------------------|------------|--------------------------|-------------------------|--|--------------|
| | App Catalo | Google Play Store Search | | | × |
| Filters | Actions | Application Name Box | Search | | |
| Search by Name | | NAME | | DESCRIPTION | |
| Source Public | - 1 | box | | Box for Android lets you view and share files from | m any Import |

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

| 2 | Mob | ADMIN PORTAL | DASHBOAR | D USERS | 6 & DEVICES | | APPS PC | DLICIES & CC | NFIGS | SETTI | NGS LOO | GS & EVE |
|--|-----------|-------------------------|-----------|-----------|---------------|-------------------|----------------|--------------|--------|---------|---------|----------|
| App Distribution Library Device App Inventory App Tunnels App Control Apps@Work Settings | | | | | | | | | | | | |
| Select | Platform: | ios 👻 | | | | | | App Store Ir | nport | | | |
| | Edit | App Name | | App Stor | e Search | | | | | | × | |
| | | Evernote | | Ann Namer | Box for EMM | Ann C | Linited | States | Limite | 20 0 | Search | |
| | Ø | Salesforce1 | | App Name: | | App St | tore: United | States | Limit: | 20 0 | Search | |
| | Ø | Cisco WebEx Meetings | | | Name | | | | | Version | | |
| | Ø | Cisco AnyConnect | | how | Day for EMM | | | | | 262 | Turnet | |
| | | Box for iPhone and iPad | | | BOX IOF EIVIN | | | | | 3.0.2 | | |
| | Ø | SF Classic | | | | | | | | | | |
| | Ø | Box for EMM | | | Import | ting / Updating | J App | \times | | | | |
| | | MobileIron Mobile@Work | k™ Client | | Succes | sfully Added / Up | pdated selecte | d app. | | | | |
| | | | | | | | ОК | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

- 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 | g iBooks In | stalled Apps App | Tunnels App Contr | ol Apps@ | @Work Settings | App Licenses |
| | Box | | | | | |
| | Application Name | Box | | | | |
| | Min. OS Version | 5.0 | | ~ | | |
| | Display Version | 3.7.5 | | | | |
| | Description | Winner of PC Magazine "There are plenty of ex services, but, on Andro cake."Securely sto files, photos and docur cloud storage from Box | e's Editors' Choice Award: cellent file-syncing storage bid, the Box app takes the re, manage and share all yo nents with 10GB of free | ur | | |
| | | Feature this App in the | he Apps@Work catalog | | | |
| | Category | | v | | | |
| | | Add New Category | | | | |

- 8. Click Next
- 9. Click Finish
- 10. **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.

| | box Box | | 3.7.5 | Public | Android | 0 |
|-----|---|------------------------|------------------|---------------|-------------|---|
| 2. | Click on the Edit button. In the Apps@Work Catalog check | the below box | | | | |
| | | V | Feature this App | in the Apps@W | ork catalog | |
| 3. | In Android For Work Check "install this app for Android Check "Silently install" | for Work" | | | | |
| AND | DROID FOR WORK | | | | | |
| AND | DROID FOR WORK | ✓ Install this app for | Android for Work | | | |

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

| CONFIGURATIONS () | | |
|-------------------|---|---|
| User email | | 0 |
| Public Id | | 0 |
| Management Id | | 0 |
| EMM Name | ~ | 0 |
| Billing Id | | 0 |

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 Sett | ing | × |
|---------------------------|-----------------------------------|---|
| Name | Box Android for Work Cofiguration | |
| Description | | |
| | | |
| | | |
| | | |
| | Cancel Save | |

- 6. Click Save
- 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

| Android for Work | |
|------------------|---|
| | Allow copy and paste |
| | Allow screen capture |
| | Allow the user to turn on location sharing |
| | Allow modification of applications in Settings or launchers |
| | Allow the user to configure user credentials |
| | Allow the user to create and modify accounts |
| | Allow the user to transfer app data over NFC |
| | |

For additional controls please refer Chapter 2 of <u>MobileIron Core Device Management Guide for Android for</u> <u>Work</u>.

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.**

| Account Info Company & Branding Security Content & Sharing Notifica | ations User Setting: Apps Nybile | App Use Management |
|---|--|--|
| Application Settings Manage your user's applications Secure connection: Require web app integrations to use secure of Published Applications: Disable apps by default Unpublished Applications: Disable apps by default Save | onnections (SSL) | Tip: Choose from thousands of applications to use in conjunction with your Box account. Whether you want to use the Box for Phone app or a with Box (like Autodesk or Salestorea) you can samelineasily diff documents, tweak apreadaheets, or digitally sign contracts wherever you go. |
| Individual Application Controls box for iphone Q Application Filters: All Apps* Category: All * Image: Control of the state of the sta | Disabled Available Added by Default | 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 available application is it. Adda db yddaut - your users can add or monyer the service, but it will be applications it. For applications with shared event settings, if those settings are enforced users will not be able to money the application is blocked from your users. |

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'.



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. Box for Android for Work with MobileIron Core/ Cloud – Configuration Guide

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.

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.

| Account Info Company & Branding Security Content & Sharing Notifications User Settings Apps Mob | |
|--|---|
| | |
| Application Settings Tip: To enable dow enterprise, check th Device Prinning Check th Device Pri | nning for your x titled "Enable he number of ion can be slick the "Save" ation, visit the |
| Application Usage Install Time All Applications - Tp: Use this table to your managed users the "Application to a specific user using". Search Users Install Time All Applications - Specific user using - Image: Search Users Install Time All Applications - Specific user using - Image: Search Users Image: Search Users Image: Specific user using - Specific user using - Image: Search Users Image: Specific user using - Image: Specific user using - Specific user using - Image: Specific user using - Image: Specific user using - Image: Specific user using - Specific user using - Image: Specific user using - Image: Specific user using - Image: Specific user using - Specific user using - Image: Specific user using - Image: Specific user using - Image: Specific user using - Specific user using - Image: Specific user using - Image: Specific user using - Image: Specific user using - Specific user using - Image: Specific user using - Image: Specific user using - Image: Specific user using - Specific user using - Image: Specific user using - Image: Specific user using - Image: Specific user using - Specific user using - Image: Spe | :k the devices e pinned the ian search for a Search Users" for ion Types" drop ting pin, click t of the k the "Remove" |
| ©2015 Box + Contact Box + Terma + Privacy Policy + Help + Log Out | |

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

| box 🏦 😃 🗎 | ılı O | | | Search Users | | | ۵ 🔅 |
|---------------------------------|--------------|-------------------|---------------|---------------|--------|---------|--|
| Account Info Company & Brand | ing Security | Content & Sharing | Notifications | User Settings | Apps | Mobile | App Use Management |
| Application Settings | | | | | | | Tip: To enable device pinning for your entermise, check the box titled "Enable |
| Enable Device Pinning | | | | | | | Device Pinning", select the number of devices the Box application can be pinned to per user, and click the "Save" button. For more information, visit the |
| Application Type | | Devices Per User | | | Notify | y Admin | Box Support site |
| Box Sync | Unlin | mited | • | | | | |
| Box Phone Application | 1 | | • | | | | |
| Box Tablet Application | Unli | mited | • | | | | |
| Browsers and Other Applications | | Iloïmited | _ | | | | |
| | | Save | | | | | |
| Application Usage | | | | | | | Tip: Use this table to track the devices your managed users have pinned the Box application to. You can search for a |
| Q Search Users | nstall Time | All Appli | cations * | | | | specific user using the "Search Users" box or use the "Application Types" drop down to filter for a group of application |
| Duncan Fisher | Apr 17, 2015 | iPhone | | | | | types. To remove an existing pin, click the check box to the right of the application type and click the "Bernove" |
| Duncan Fisher | Apr 16, 2015 | Sync | | | | | button. |
| | | | | | | | |

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.

| n/master/settings | | | C Q Search | ☆ |
|---------------------------------|--|---------------------------|--|---|
| Admin Console My Account | | | | |
| 🚽 box 🚓 😃 🗎 🛛 | li O | Search Users | ۵ 🛱 | |
| Account Info Company & Branding | Security Content & Sharing Notifications | User Settings Apps Mobile | App Use Management | |
| Application Settings | | | Tip: To enable device pinning for your | |
| C Enable Device Pinning | | | Device Pinning", select the number of devices the Box application can be pinned to per user and click the "Save" | |
| Application Type | Devices Per User | Notify Admin | button. For more information, visit the Box Support site | |
| Box Sync | Unlimited • | | | |
| Box Phone Application | | 0 | | |
| box Prone Application | | | | |
| Box Tablet Application | Unlimited | U | | |
| Browsers and Other Applications | Unlimited | | | |
| | Save | | | |
| Application Usage | | | Tip: Use this table to track the devices | |
| | | | your managed users have pinned the Box application to. You can search for a specific user using the "Search Users" | |
| Duncan Fisher × Insta | II Time All Applications * | Remove 1 × | down to filter for a group of application types. To remove an existing pin, click | |
| Duncan Fisher Toda | y iPhone | | application type and click the "Remove" button. | |
| | | | | |

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.

| pp.box.com/master/se | ttings | | | | V C Q Search | ☆自↓ |
|----------------------|---|----------------------------------|---------------|----------------------|--|-----|
| l | xx 🛧 보 🖬 네 | 0 | | Search Users | ۹ ا | ¢ |
| A | ccount Info Company & Branding S | ecurity Content & Sharing N | lotifications | User Settings Apps M | App Use Management | |
| | File Security Settings | | | | Tip: These settings may apply to only particular versions of our mobile | |
| | User Permissions | A | low | Restrict | applications. To learn more, visit the Box Support site | 18. |
| | Save files to device (9) | | 0 | 0 | | |
| | Allow preview-only users to save files for | or offline use 🚯 | 0 | 0 | | |
| | Open files in external applications 🚯 | (| 0 | 0 | | |
| | Print files | (| 0 | 0 | | |
| | Copy and paste content of files | | 0 | 0 | | |
| | Automatic uploading from device | | 0 | 0 | | |
| | Include contextual information in push | notifications (1) | 0 | 0 | | |
| | Allow saving to device only if the device | vice is encrypted (Android only) | | | | |
| | Allow files to be opened into application | tions that save back to Box (iOS | only) 🕄 | | | |
| | Passcode Settings | | | | | |
| | Bequire application | | | | | |
| | passcode lock: | After 5 minutes of inactivity | • | | | |
| | _ | Do not enforce | | | | |
| | | After 1 minute of inactivity | | | | |
| | | After 5 minutes of inactivity | | | | |
| | M015 Day Cantact Day Tarma Drivery Da | After 15 minutes of inactivity | | | | |
| G | 2015 Box + Contact Box + Terms + Privacy Pc | After 1 hour of inactivity | | | | |

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.

| Account Info Compar Your settings have been successfully | y updated. Devices may ta | ike up to one hour to refle | ert changes. X |
|---|-------------------------------|-----------------------------|--|
| File Security Settings | | | Tip: These settings may apply to only particular versions of our mobile |
| User Permissions | Allow | Restrict | applications. To learn more, visit the Box Support site. |
| Save files to device 1 | 0 | 0 | |
| Allow preview-only users to save files for offline use ${f 0}$ | 0 | 0 | |
| Open files in external applications (1) | 0 | \bigcirc | |
| Dist files | - | | |
| Copy and paste content of mes | 0 | • | |
| Include contextual information in push notifications | 0 | 0 | |
| ☐ Allow saving to device only if the device is encrypted (Andrc | oid only) Box (iOS only) 🛈 | | |
| Passcode Settings | | | |
| Require application Do not enforce | - | | |
| | Save | | |
| ©2015 Box · Contact Box · Terms · Privacy Policy · Help · Log Out | | | |

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.

| | S | Search Users | ۵ Q |
|--|------------------------------------|--------------------------|--|
| Account Info Company & Branding Security Content & | Sharing Notifications Us | ser Settings Apps Mobile | e App Use Management |
| File Security Settings | | | Tip: These settings may apply to only particular versions of our mobile soulicatione |
| User Permissions | Allow | Restrict | To learn more, visit the Box Support site. |
| Save files to device 🕕 | 0 | 0 | |
| Allow preview-only users to save files for offline use | 0 | 0 | |
| Open files in external applications | • | | |
| Print files | 0 | • | |
| Automatic uploading from device | 0 | 0 | |
| Include contextual information in push notifications $\textcircled{1}$ | 0 | 0 | |
| ☐ Allow saving to device only if the device is encrypted (An | droid only) to Box (iOS only) 🚯 | | |
| Passcode Settings | | | |
| Require application Do not enforce | • | | |
| | Save | | |
| ©2015 Box · Contact Box · Terms · Privacy Policy · Help · Log Out | | | |

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.

| | box 🛧 보 🖬 네 이 | | Search Users | | Q Ø | |
|------------------------------|--|--------------------|----------------------|--------|--|--|
| | Account Info Company & Branding Security Content & Sharing | Notifications | User Settings Apps M | lobile | App Use Management | |
| | File Security Settings | | | | Tip: These settings may apply to only particular versions of our mobile | |
| | User Permissions | Allow | Restrict | | applications. To learn more, visit the Box Support site. | |
| | Save files to device (1) | 0 | 0 | | | |
| | Zerow proview-only abera to save measiful oriented as | Ū | | | | |
| | Open files in external applications (| | ۲ | | | |
| | Print files | | ۲ | | | |
| | Copy and paste content of files | 0 | 0 | | | |
| | Automatic uploading from device | 0 | 0 | | | |
| | Include contextual information in push notifications 🚯 | 0 | 0 | | | |
| | Allow saving to device only if the device is encrypted (Android on | ily) OS only) 🗊 | | | | |
| | Passcode Settings | | | | | |
| | Require application Do not enforce | • | | | | |
| | | Save |] | | | |
| app.box.com/master/settings# | ©2015 Box + Contact Box + Terms + Privacy Policy + Help + Log Out | | | | | |

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

| Account Info Company & Branding Security Content & Sharing | g Notifications | User Settings Apps Mobile | App Use Management | |
|---|-----------------|---------------------------|--|--|
| | | | | |
| File Security Settings | | | Tip: These settings may apply to only particular versions of our mobile | |
| User Permissions | Allow | Restrict | applications. To learn more, visit the Box Support site. | |
| Save files to device 1 | 0 | 0 | | |
| Allow preview-only users to save files for offline use | • | | | |
| Open files in external applications 🚯 | 0 | 0 | | |
| Print files | 0 | 0 | | |
| Automatic uploading from device | 0 | 0 | | |
| Include contextual information in push notifications () | • | 0 | | |
| Allow saving to device only if the device is encrypted (Android of Android | only) | | | |
| Allow files to be opened into applications that save back to Box (iOS only) | | | | |
| Passcode Settings | | | | |
| Require application Do not enforce | | | | |
| passcode lock: | | | | |
| | Save | | | |
| 6/2015 Box + Contact Box + Terms + Privacy Policy + Help + Log Out | | | | |

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 prepopulated 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 <u>Box Help article</u> 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.