

IBM **MaaS360**

# Enterprise Mobile Management (EMM) Policies

## Best Practices Guide

# IBM MaaS360

Copyright © 2016 Fiberlink, an IBM Company. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Fiberlink Communications Corporation.

All brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

Fiberlink

1787 Sentry Parkway West

Blue Bell, PA 19422

May 2016

# IBM MaaS360

## Table of Contents

Introduction .....	4
Best Practice #1: Know Your Industry's Regulations .....	4
Best Practice #2: Require Passcodes .....	5
The Options.....	5
Types of Passcodes .....	5
Minimum Length .....	5
Passcode Expiration.....	5
Passcode Reuse .....	5
Our Recommendations.....	5
How MaaS360 Helps .....	6
Best Practice #3: Enforce Encryption .....	7
Our Recommendations.....	7
How MaaS360 Helps .....	7
Best Practice #4: Restrict Device Features as Necessary.....	8
Our Recommendations.....	8
How MaaS360 Helps .....	8
Best Practice #5: Keep a Watchful Eye on Apps .....	9
Our Recommendations.....	9
How MaaS360 Helps .....	9
Best Practice #6: Use a FIPS-Compliant Container for Email and Content .....	10
Our Recommendations.....	10
How MaaS360 Helps .....	10
Best Practice #7: Distribute Settings Over the Air (OTA).....	11
Our Recommendations.....	11
How MaaS360 Helps .....	12
Best Practice #8: Warn First, Then Remediate Policy Violations .....	12
Our Recommendations.....	12
How MaaS360 Helps .....	13
Best Practice #9: Test Your Policies .....	13
How MaaS360 Helps .....	13
Best Practice #10: Monitor Your Devices .....	14
Our Recommendations.....	14
How MaaS360 Helps .....	14

# IBM MaaS360

## Introduction

This document is designed to provide you with Enterprise Mobility Management (EMM) best practices we've developed while working with our extensive customer base.

It will also demonstrate how MaaS360 can help you secure your mobile environment.

MaaS360 is designed to give you maximum control over mobile devices, so you can reduce risks to your corporate data without jeopardizing employee productivity. It will watch over your devices, both employee-owned and those provided by the corporation, making sure they comply with corporate security policies. You can set it up so that you don't have to do anything if devices fall out of compliance—MaaS360 can take action automatically. Some of these actions include:

- Warning the administrator that there could be a problem
- Sending a message telling the user to do something
- Preventing the user from accessing his corporate email account from his device
- Wiping corporate data, apps and documents from the device while leaving personal data untouched

For example, you can create a policy listing restricted, approved and required apps for your users. If they are out of compliance, the device can be restricted from accessing corporate email accounts, Wi-Fi, and the VPN after 24 hours. You can then assign this policy to all the active Android devices that have reported in to MaaS360 in the last seven days.

## Best Practice #1: Know Your Industry's Regulations

Many of your decisions will be grounded in the regulations for your industry.

For example, if you are in the Healthcare industry, you'll need to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

Armed with this knowledge you can set up your policies. Most companies only have a few policies:

1. Corporate devices
2. Personal devices
3. iOS devices
4. Android devices

Keep it simple. Many of your settings will be the same for each policy, because the requirements of your industry will be the same.

# IBM MaaS360

## Best Practice #2: Require Passcodes

Of all the ways to protect your devices, requiring passcodes probably gets you the greatest results with the least effort. Small devices like tablets and smartphones are easy to lose, so the chances of them ending up in someone else's hands are pretty good. Passcodes also help enforce encryption on a number of devices.

*Note: If you are developing a pure BYOD strategy with a containerized approach, you may forego the device passcode for a container passcode or make a less stringent device passcode to help gain user adoption.*

### The Options

#### Types of Passcodes

Name	Description	Example
Simple	Repeating, ascending or descending values	1111, 2233, 1234, 0987, xyz
Numeric	Requires at least one number	184, 1066, 1490, xyz1
Alphanumeric	Requires at least one letter and one number	itbgc11, g2t, pick1e
Complex, Alphanumeric with Special Characters	Requires at least one letter, one number, and a special character. May also require at least one uppercase and one lowercase letter	T!so4r#, wntg?stio2F, R!h9
Pattern	Android only. The device displays rows of dots, and the user slides his finger across them in a certain order to gain access	

#### Minimum Length

You can have passcodes from one to sixteen characters long. Longer passcodes are more secure, but if you require your users to have very long passcodes your users will have trouble remembering them.

#### Passcode Expiration

You can require your users to enter a new passcode after a specified period of time. When time's up, they'll have to change it.

#### Passcode Reuse

You can prevent your users from using the same two or three passcodes over and over.

### Our Recommendations

1. Require passcodes on all devices that will access corporate resources. Passcodes are your first line of defense.
2. The most secure passcodes are complex. We recommend requiring your users to have alphanumeric passwords with at least one uppercase and one lowercase letter, even though your industry may not require them yet.
3. We recommend that passcodes be at least four or five characters long.

# IBM MaaS360

4. We recommend that you set up passcode expiration.
5. Requiring a different passcode *every* time they change it is probably overkill, but you should set up some reuse restrictions. Use your industry's rules and regulations as your guide.

## How MaaS360 Helps

MaaS360 allows you to set up passcode policies quickly and easily. We've found that most of our customers don't need many. We provide two default policies to help you: one for iOS devices and one for Androids.

To make your changes, just edit one of MaaS360's default policies. There are even more options than we discussed above. These will come in handy if your industry has very stringent passcode requirements.

Configure Passcode Policy <input checked="" type="checkbox"/>	
<b>Passcode</b>	
<b>Enforce Passcode on Mobile Device</b>	<input checked="" type="checkbox"/>
<b>Allow Simple Passcode</b> <small>Passcode values that are ascending, descending or repeating character sequences (e.g. 1111, 123, 654, abc, xyz).</small>	<input type="checkbox"/>
<b>Require Alphanumeric in Passcode (at least one letter)</b>	<input checked="" type="checkbox"/>
<b>Minimum Passcode Length</b>	7
<b>Required Number of Special Characters (1-4)</b>	1
<b>Maximum Passcode Age (1-730 days, or blank)</b>	90
<b>Allowed Idle Time (in minutes) Before Auto-Lock</b>	5
<b>Number of Unique Passcodes Required Before Reuse Allowed (1-50, or blank)</b>	5
<b>Grace Period for Device Lock</b>	5 Minutes
<b>Number of Failed Passcode Attempts Before All Data Is Erased (4-16)</b>	10

With a few clicks you can make your passcode policy a reality.

# IBM MaaS360

## Best Practice #3: Enforce Encryption

Apple's iOS provides block-level encryption on all devices that are 3GS and higher. When a user sets up a passcode, however, it starts using the file-level encryption data protection element. As a result, if you are requiring your users to protect their iOS devices with a passcode, you don't really need to worry about encryption. iOS will handle it automatically.

Google's Android operating system is a different matter. Some devices don't support encryption at all (usually the earlier models and operating system versions). To enforce encryption, you might have to refuse to support some Android devices or use our compliance rules to monitor OS version or encryption.

*Note: If you are developing a pure BYOD strategy with a containerized approach, you may forego the device encryption in favor of the containerized encryption.*

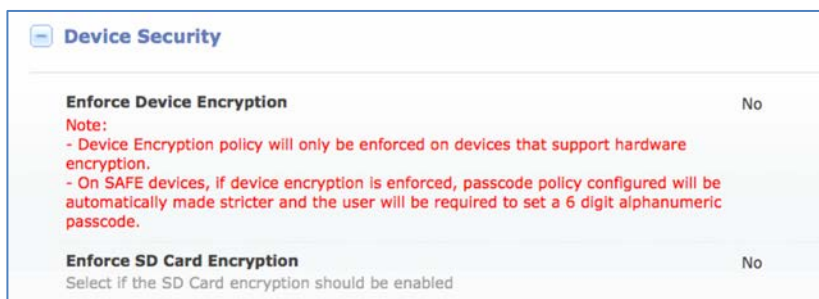
### Our Recommendations

Encryption is a must-have. You may encounter some resistance if you don't support devices that cannot be encrypted, but it's worth it in the end to know that your data is safe.

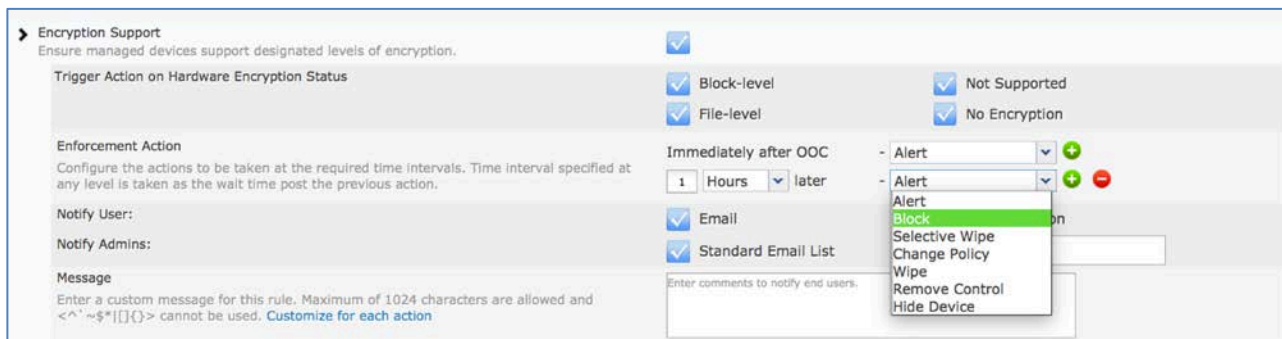
We recommend you prevent any devices that cannot be encrypted from connecting to your corporate resources.

### How MaaS360 Helps

MaaS360 can identify the Android devices that cannot be encrypted.



You can also use MaaS360's Compliance Engine to block devices from accessing corporate resources.



# IBM MaaS360

## Best Practice #4: Restrict Device Features as Necessary

If your industry requires it, you may need to disable certain features on the devices. For example, you might want to disable cameras to protect proprietary information if your users work in a plant.

The operating system and device vendor makes a difference here, too, because device features are different. For example, you may want to prevent iOS users from storing data to iCloud or from accessing Siri when the device is locked.

### Our Recommendations

If these devices are owned by your employees, not given out by the company, you may want to restrict as little as possible. We recommend restricting:

- Accessing Siri when the device is locked
- Bluetooth (or making it non-discoverable)
- Mock locations
- Syncing documents to iCloud (although we don't recommend restricting backing up other things to iCloud or syncing using Photo Stream )
- Camera, screen captures, and YouTube if it is required for your industry
- On iOS devices, we recommend the following settings for Safari:
  - Leave the fraud warnings on
  - Block pop-ups
  - Accept cookies only from visited sites

### How MaaS360 Helps

MaaS360 provides a number of choices for your devices. You can quickly and easily put into place the safeguards to protect devices.

iCloud		
<b>Allow Cloud Backup</b>	Yes	iOS 5.0+
<b>Allow Cloud Keychain Sync</b>	Yes	iOS 7.0+
<b>Allow Documents Sync</b>	Yes	iOS 5.0+
<b>Allow Photo Stream Sync (disallowing can cause data loss)</b>	Yes	iOS 5.0+
<b>Allow Shared Photo Stream</b>	Yes	iOS 6.0+
<b>Allow iCloud Photo Library</b>	Yes	iOS 9.0+
<small>Allow iCloud Photo Library. If disabled, any photos not completely downloaded will be removed from local storage.</small>		

MaaS360 has even more choices than we've discussed, so you can make sure you're in compliance with your industry's requirements.



# IBM MaaS360

## Best Practice #5: Keep a Watchful Eye on Apps

Apps can improve productivity enormously, but they can also open up your organization to risks. Some apps like Dropbox allow your users to store documents outside your span of control. It makes things easier for them, but what happens if the employees leave the company?


It might make sense for you to restrict some apps, depending on what is dictated by your industry or corporate security policies. You might also want to allow other apps. Some of our customers also require employees to have the same collaboration tools so teams can work together.

### Our Recommendations

1. Use your EMM solution to restrict, allow and require apps you need to encourage productivity while keeping your corporate data safe.
2. If your EMM solution has one, use a corporate app catalog to push helpful apps to your users.
3. Use VPP to help ease deployment of public apps on your iOS devices.
4. If you are using Enterprise apps in your environment, we recommend further securing the apps using app wrapping or SDK technology to prevent data leakage or even give access to resources behind the corporate firewall.

### How MaaS360 Helps

Policies allow you to specify restricted, allowed and required apps.

<b>Configure Restricted Applications (App Blacklist)</b> <input checked="" type="checkbox"/>	
Add Name for Apps restricted on managed devices.	
<b>Application Name</b>	Dropbox <a href="#">Change Region</a>
<b>Configure Allowed Applications (App Whitelist)</b> <input type="checkbox"/>	
Add Name for Apps allowed on managed devices. Any other app would be disallowed.	
<b>Configure Required Applications</b> <input checked="" type="checkbox"/>	
Add Name and Bundle ID for the apps required to be installed on managed devices. This policy can be used in conjunction with the Blacklist or Whitelist policy settings. It is recommended that you also use the App Management workflows to distribute this app to the appropriate devices.	
	
<b>Application Name</b>	Box for EMM <a href="#">Change Region</a>
<b>Application Name</b>	MaaS360 for iOS <a href="#">Change Region</a>

# IBM MaaS360



MaaS360 also offers an App Catalog that you can use to push market or enterprise apps directly to your devices.

The App Catalog is set up so it keeps personal apps separate from corporate apps. That way, when an employee leaves the company, you can easily remove all the corporate apps without touching any of the personal ones.

## Best Practice #6: Use a FIPS-Compliant Container for Email and Content

With the right container, you can encrypt emails and attachments, prevent unauthorized backups, prevent copying and pasting contacts or emails, and can block attachments from Android devices. It also gives your users a consistent experience, even if they are on different versions of Android.

### Our Recommendations

1. Block native email capabilities on the device
2. Block Gmail
3. Encrypt emails
4. Encrypt attachments

There's an added bonus, too: it's easier to remove corporate settings when employees leave the company.

### How MaaS360 Helps

MaaS360 Secure Productivity Suite provides a secure container so users can manage all their emails, contacts, calendars, documents, Intranet access and file management suites, like SharePoint, Fileshare and OneDrive. Policies control the movement of data, and you can restrict sharing by users, forwarding of attachments, and copying and pasting. Devices that are lost or stolen can be selectively wiped to remove corporate data.

# IBM MaaS360

Configure Device Security Policies	
<b>Restrict Jailbroken/Rooted Devices</b> Prevent users from accessing secure content if their device is jailbroken or rooted.	No
<b>Restrict Devices with Malware</b> Prevent access to corporate content if malware is detected on the device.	No
<b>Enable Timebomb (days)</b> Delete corporate data from container if not accessed for defined number of days (7 to 365). Leave blank to Ignore.	
Configure Data Protection Policies	
<b>Restrict File Export</b> Restrict export of managed content and email attachments. Ensure that content can not be forwarded using external/personal email clients or opened in unmanaged apps. In Windows Phone devices, if this is enabled, documents and email attachments will not be downloaded.	No
<b>Restrict Clipboard Export</b> Restricts copying of content and pasting it externally to an unmanaged app. Your users would still be able to use copy/paste within the app as well as copy content from outside into the app.	Yes
<b>Restrict Screenshot</b> Restricts user from taking screenshots and disables viewing of app UI in non-secure displays like in the device Task Manager.	No
<b>Restrict Print</b>	No
<b>Restrict Import of Files</b> Users will not be able to import documents from other apps to email or save them locally.	Yes
<b>Allow Widgets</b> Allow user to add Mail, Calendar and Doc widgets.	Yes

Configure Secure Mail	
<b>Mail Server</b> Select the appropriate email server to ensure that the devices get approved automatically. Auto Approval supported for Exchange, Office 365, IBM Traveler and IBM Connections Cloud.	Office 365
<b>Hostname of the ActiveSync Server</b> Enter your Email Server URL.	
<b>Use SSL</b> Configure Secure Connection.	Yes
<b>Domain Name</b> Leave this blank to use the user's domain name. If a username is being entered in the field below and you need a domain name then enter that domain name or %domain% to use user's domain.	
<b>Account Username</b> Leave this blank to use the username in this system. If Account Username is same as Email Address (such as Office365 or IBM Traveler) use %email% as the variable.	
<b>Email Address</b> Leave this blank to use the user's email address.	
<b>Authentication Type</b> Choose from Corporate Credentials or Certificate based authentication.	Password
<b>App Badge Count</b> Select Badge Count to show for new users. Users will be able to change it from App Settings.	
<b>Authenticate using WorkPlace Account</b> Utilizes common WorkPlace credentials for email authentication. Users will not be prompted to enter credentials if WorkPlace credentials have already been entered.	No
<b>Default Signature</b> Users will still be able to add their personal signature ahead of the default signature.	
<b>Organize by Thread</b> This setting will be applied only during initial mail configuration. Users can change this under Email Settings in the App.	No

Secure Mail Security Settings	
<b>Restrict Attachment Forwarding</b> Restrict emails with attachments from being forwarded.	No
<b>Restrict Email to External Domains</b> Prevent email from being sent to non-corporate email domains.	No

## Best Practice #7: Distribute Settings Over the Air (OTA)

Your wireless network, VPN and passcode settings will likely be the same for all your users. Configuring them all individually would be a lot of extra time and trouble for your IT department. Some EMM solutions will let you create settings once and then push them to your users.

### Our Recommendations

Use a policy to push your wireless network, VPN and passcode settings to your users. If you push them OTA, you won't have to touch each device. That can save your IT department a great deal of time and effort. There's an added bonus, too: you don't have to track down all your users and get their devices.

When someone leaves the company, you can remove their access and data the same way. You don't need to try to track down someone's personal device as they're leaving—just remove the settings and information remotely.

# IBM MaaS360

## How MaaS360 Helps

MaaS360 allows you to set up these profiles for your users in minutes. Then you can push them to your users OTA. When someone leaves the company, you can remove the profiles remotely, using the Remote Control action.

The screenshot shows the configuration page for a Wi-Fi profile titled "Wi-Fi : WPA/WPA2 (Enterprise) Profiles". The interface includes several settings:

- Configure for type:** A dropdown menu set to "WPA/WPA2 (Enterprise)".
- Service Set Identifier (SSID):** A text input field with the placeholder text "Identification of the wireless network to be connected."
- Auto Join:** A checkbox that is currently unchecked.
- Hidden Network:** A checkbox that is currently unchecked.
- Encryption Type:** A dropdown menu with "-----Select-----" selected. Below it, a note states: "WPA" corresponds to WPA and WPA2 and applies to both encryption types. Make sure that these values exactly match the capabilities of the network access point. If you're unsure about the encryption type, or would prefer that it applies to all encryption types, use the value "Any".
- Always Prompt User for Password:** A checkbox that is currently unchecked. Below it, a note states: "Supported for Encryption Types Any, WEP or WPA".

## Best Practice #8: Warn First, Then Remediate Policy Violations

When your users do something that puts them out of compliance, it's a good idea to give them some kind of notice. Although you have the ability to take action right away, a better approach is to send them a message and let them remediate the noncompliance on their own before enforcing a more restrictive action.

### Our Recommendations

Set up device management options to automatically handle out of compliance situations. Send users a message explaining the company's policy and why they are out of compliance with it. In most cases, you can give them some time to fix the problem before taking action (although there are exceptions).

Your EMM solution should be able to do all this automatically, without your IT department having to learn of the problem and then take action.

# IBM MaaS360

## How MaaS360 Helps

With MaaS360's Compliance Engine you can set up nested automatic enforcement actions with multiple messages.

The screenshot shows the configuration for a policy titled "Jailbroken (iOS) and Rooted (Android) Devices". The policy description is "Ensure managed devices are not jailbroken or rooted. IOS Application is required for Jailbreak detection." and is currently enabled (checked).

**Enforcement Action:** Configure the actions to be taken at the required time intervals. Time interval specified at any level is taken as the wait time post the previous action.

**Notify User:** (empty field)

**Notify Admins:** (empty field)

**Message:** Enter a custom message for this rule. Maximum of 1024 characters are allowed and <^'~\$\*[]{}> cannot be used. [Same message for all actions](#)

**Actions:**

- #1. Immediately after OOC - Alert (dropdown) [Green Plus]
- #2. 2 Hours later - Block (dropdown) [Green Plus, Red Minus]

**Notification Settings:**

- Email
- Standard Email List
- Device Notification

**Message Content:**

- #1. First notice: Your device is jailbroken. This is against corporate policy. In 2 hours you will be blocked from corporate resources if not remediated.
- #2. Second notice: You have failed to remediate your jailbroken device. Corporate access has been restricted.

You can set up enforcement actions for a number of scenarios. Each one can be handled differently—everything from a sending a simple email to the Administrator to remotely performing a selective wipe. Best of all, this can be done without your IT department's involvement.

## Best Practice #9: Test Your Policies

Before you deploy a policy to any of your users, you should first deploy it to test users. This is especially important if you have a lot of users.

## How MaaS360 Helps

MaaS360 allows you designate a group of users as test users. With a few clicks you can deploy a new policy to those devices so the users can experiment with it. If there's a problem, you can roll back the policy and edit it. If not, you can publish the policy to the actual users.

# IBM MaaS360

## Best Practice #10: Monitor Your Devices

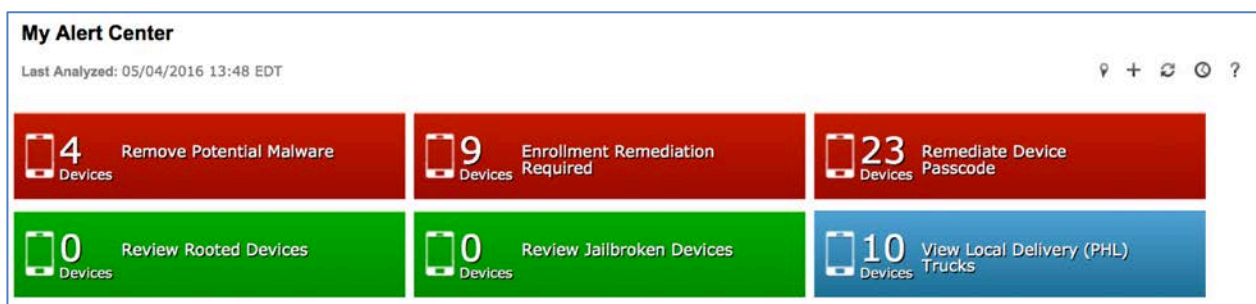
After your policies are in place, you'll want to make sure your users are following them.

### Our Recommendations

Your EMM solution should provide you with statistics on how secure your environment is. You can set up alerts to see how many devices are out of compliance, and which devices they are.

### How MaaS360 Helps

The Home page displays **My Alert Center**, a dashboard of important information that you can customize to meet the needs of your organization.



The alerts are red, green or blue. Security alerts can be red or green, depending on if the situation needs attention. Information alerts are blue.

When you know which devices are out of compliance, you can take the appropriate action, based on your industry's rules and regulations.

Search Results [Show Criteria](#)

Device Name	Username	Model	Operating ...	Last Repor...	Configure...	OS Version	Platform ...	Configurat...	Managed ...
<input type="checkbox"/> bbatey-Venue 8 7840 <a href="#">View</a>   <a href="#">Locate</a>   <a href="#">Message</a>   <a href="#">More...</a>	bbatey	Venue 8 7840	Android 4.4.4 (KTU...	05/04/2016 12:11 ...	Doc Store is enable...	4.4.4	Android	No	Enrolled
<input type="checkbox"/> Cisbrecht iPad 4 <a href="#">View</a>   <a href="#">Locate</a>   <a href="#">Message</a>   <a href="#">More...</a>	cisbrecht	iPad (4th Gen, CDM...	iOS 9	05/04/2016 09:53 ...	WiFi payload config...	9.3.1 (13E238)	iOS	No	Enrolled
<input type="checkbox"/> iPad <a href="#">View</a>   <a href="#">Locate</a>   <a href="#">Message</a>   <a href="#">More...</a>	marketingdemos	iPad mini	iOS 9	05/04/2016 02:54 ...	Email Settings,Rest...	9.2.1 (13D15)	iOS	No	Enrolled
<input type="checkbox"/> rmorris-HTC One X <a href="#">View</a>   <a href="#">Locate</a>   <a href="#">Message</a>   <a href="#">More...</a>	rmorris	HTC One X	Android 4.1.1 (JRO...	05/01/2016 12:26 ...	Wi-Fi configuration ...	4.1.1	Android	No	Enrolled

Jump To Page: \_\_\_\_\_ Displaying 1 - 4 of 4 Records | Show 25 Records | [Customize Columns](#) CSV [Export](#)