MaaS360®
by Fiberlink, an IBM company

Mobile Device Management (MDM) Policies

Best Practices Guide

www.maas360.com

MaaS360®
by Fiberlink, an IBM company

Mobile Device Management (MDM) Policies

MaaS360® by Fiberlink, an IBM company

Introduction

This document is designed to give you Mobile Device Management (MDM) best practices we've developed while working with our extensive customer base.

It will also show you how MaaS360 can help you.

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. Maintenance will be easier if, as much as it is possible, you treat all your users the same way.

MaaS360® by Fiberlink, an IBM company

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.

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	Tlso4r#, 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.

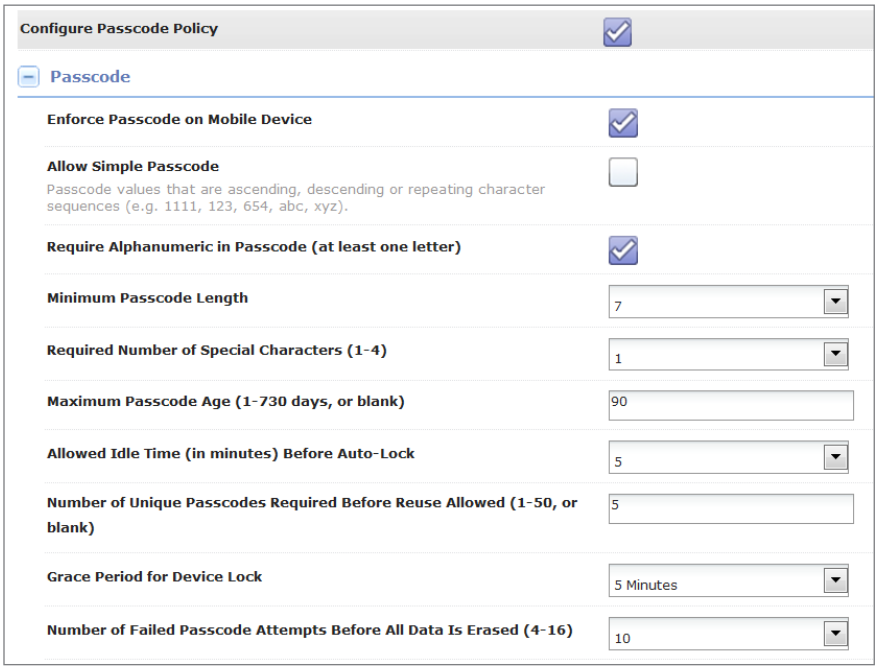
Our Recommendations

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.
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 probably 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.



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

MaaS360® by Fiberlink, an IBM company

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.

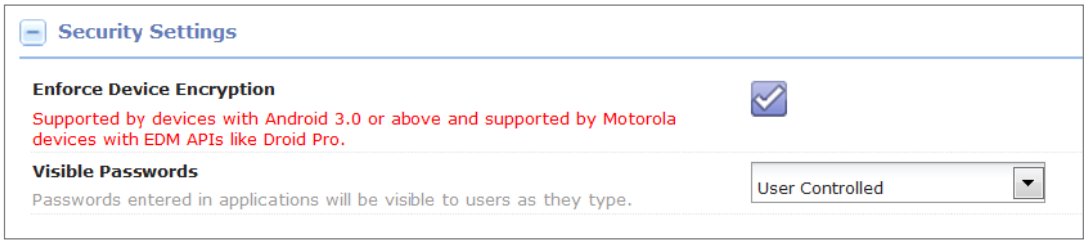
Our Recommendations

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.

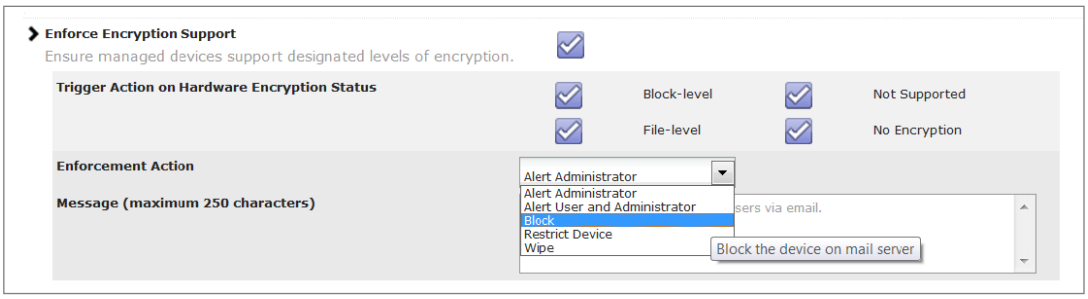
We recommend you prevent any devices that cannot be encrypted from connecting to your corporate resources.

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.



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 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.

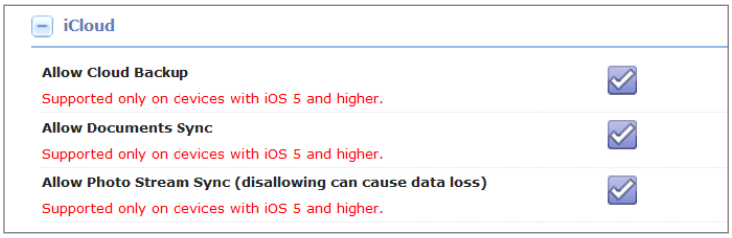
Our Recommendations

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.



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

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?

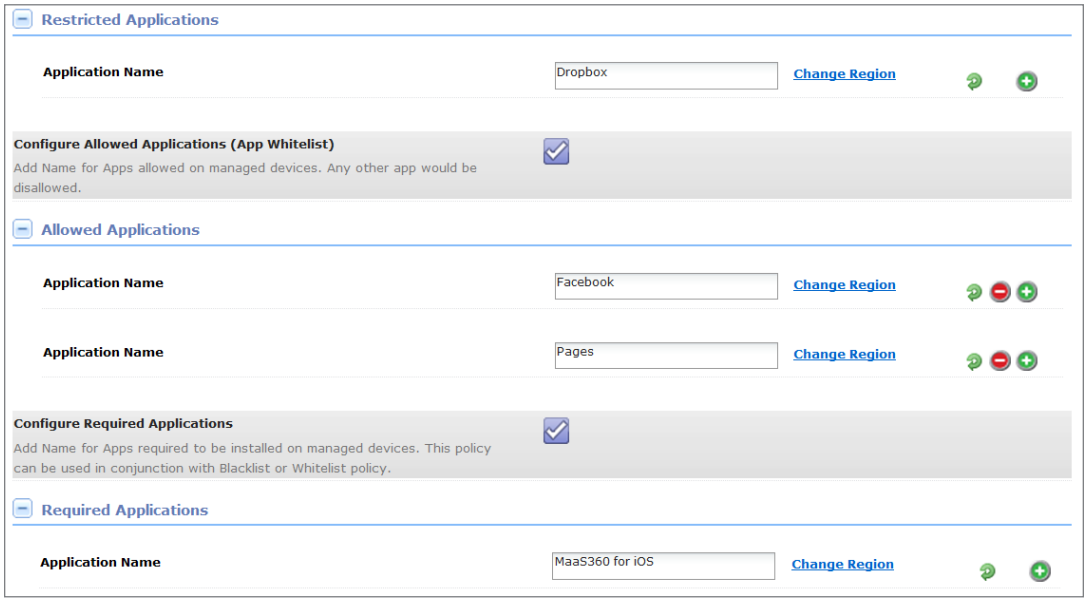
It might make sense for you to restrict some apps, depending on what is dictated by your industry or corporate security policies. You might also want to allow other apps. Some of our customers also require employees to have the same collaboration tools so teams can work together.

Our Recommendations

1. Use your MDM solution to restrict, allow and require apps you need to encourage productivity while keeping your corporate data safe.
2. If your MDM solution has one, use a corporate app catalog to push helpful apps to your users.

How MaaS360 Helps

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



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 TouchDown for Setting up Email (Android Only)

With NitroDesk's TouchDown product, 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.

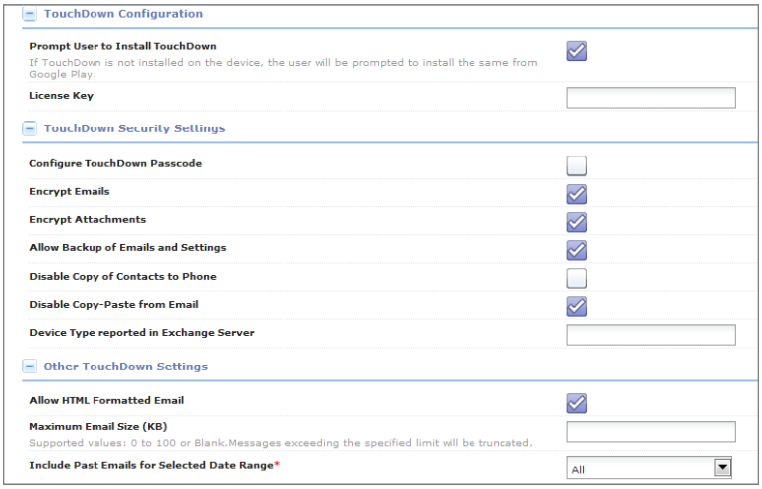
Our Recommendations

1. Block native email capabilities on the device
2. Block Gmail
3. Require users to have TouchDown
4. Encrypt emails
5. Encrypt attachments

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

How MaaS360 Helps

MaaS360 lets you include TouchDown settings in your policy for Android devices.



MaaS360® by Fiberlink, an IBM company

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

Your wireless network, VPN and passcode settings will probably 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 MDM solutions will let you create settings once and then push them to your users.

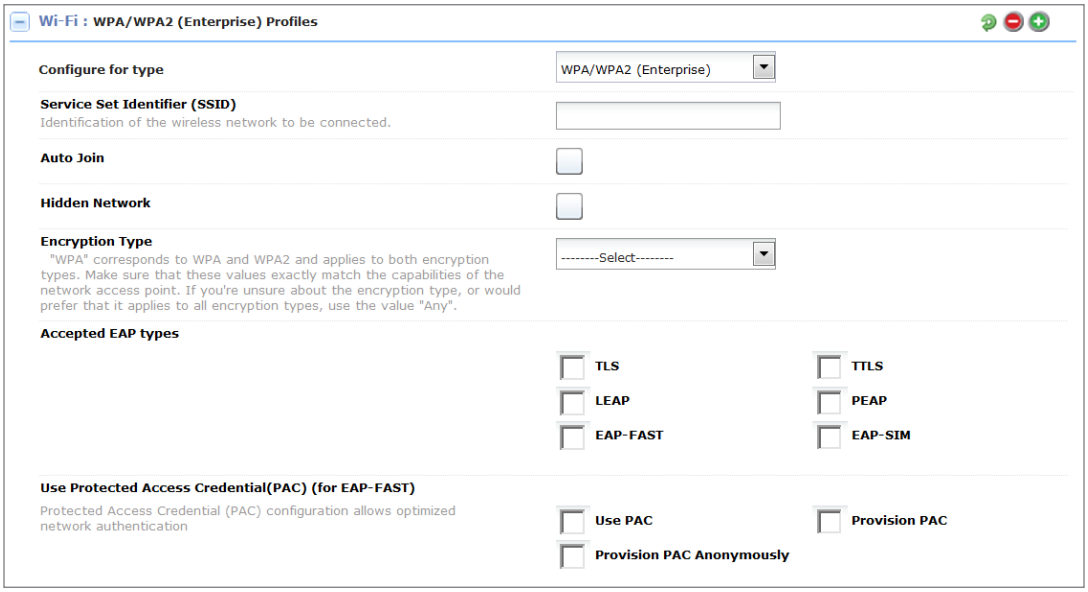
Our Recommendations

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.

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.



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 probably 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.

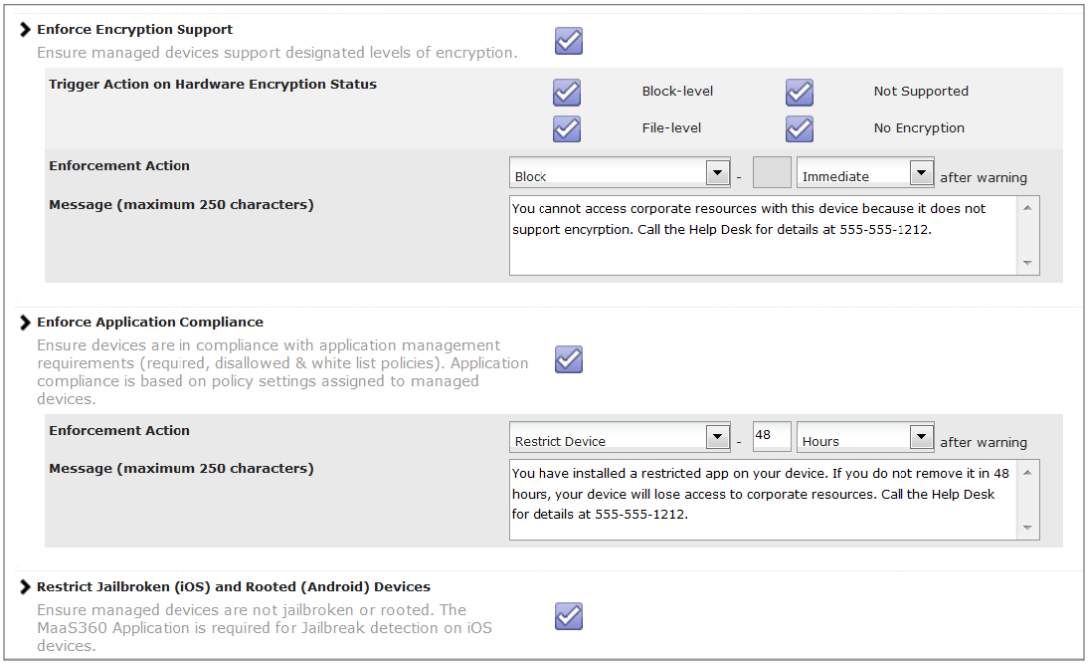
Our Recommendations

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

How MaaS360 Helps

With MaaS360's Compliance Engine you can set up automatic enforcement actions.



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.

MaaS360® by Fiberlink, an IBM company

Best Practice #10: Monitor Your Devices

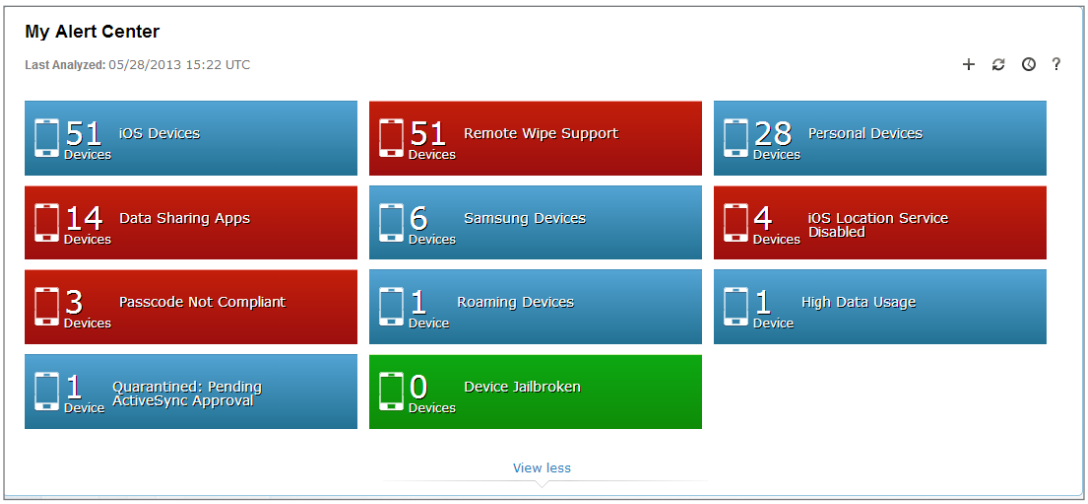
After your policies are in place, you'll want to make sure your users are following them.

Our Recommendations

Your MDM solution should provide you with statistics on how compliant your devices are. You should be able 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.

Device Name	Username	Device Type	Manufacturer	Model	Operating System
Demo Phone	jfran	Smartphone	Apple	iPhone 3GS	iOS 5
jl-Galaxy Nexus	jlert	Smartphone	samsung	Galaxy Nexus	Android 4.0.2 (ICL53F)
jpano-DROIDX	jpano	Smartphone	motorola	DROIDX	Android 2.3.4 (4.5.1_57_DX8-51)
jbert-ADR6300	jbert	Smartphone	HTC	ADR6300	Android 2.2 (FRF91)

For More Information

To learn more about our technology and services visit www.maaS360.com.
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Phone 215.664.1600 | **Fax** 215.664.1601 | sales@fiberlink.com

WP_201402_0017