Getting Started - MDM Setup

Thank you for acquiring the Talon Mobile app. The Talon Mobile app allows you to request sensitive justice information. To use the Talon Mobile app, your agency's mobile device management (MDM) software must meet certain Criminal Justice Information Security (CJIS) mobile device management requirements. Please verify your MDM meets the following requirements set forth in the Mobile Device Management section (5.13.2) of the CJIS Security Policy (version 5.3):

- Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device
- MDM with centralized administration configured and implemented to perform at least:
  - Remote locking of device
  - Remote wiping of device
  - Setting and locking device configuration
  - Detection of "rooted" and "jailbroken" devices
  - Enforce folder or disk level encryption
  - Application of mandatory policy settings on the device
  - Detection of unauthorized configurations or software/applications

MaaS360 MDM

You have chosen the MaaS360 MDM. Below are the basic steps to create the MDM network and distribute the Talon Mobile app. **For more detailed information on MaaS360 MDM setup and management, please contact your MaaS360 representative Michael Gordon at 215-664-1835 or at mgordon@fiberlink.com**. Michael Gordon will register your account and you will be provided with a login link that may be used in Step 2 of the following instructions.

Initial Setup (Steps 1-12)

Important: For all steps, use a Google Chrome or Mozilla Firefox browser. Internet Explorer will not work properly.

Configure the MDM

1. If using iOS devices on the MDM network, you will need to request and upload an Apple Push Notification Service certificate (push certificate), which Apple requires before the MDM software may be used on iOS devices. Before you request a push certificate (in step 2 or 3), you must have a valid AppleID. An Apple ID (also called iTunes ID) should be linked with a public-facing email address instead of a personal email address. Your certificate must be renewed every year, so if the user associated with the push certificate is not available, you will not be able to renew the push certificate.

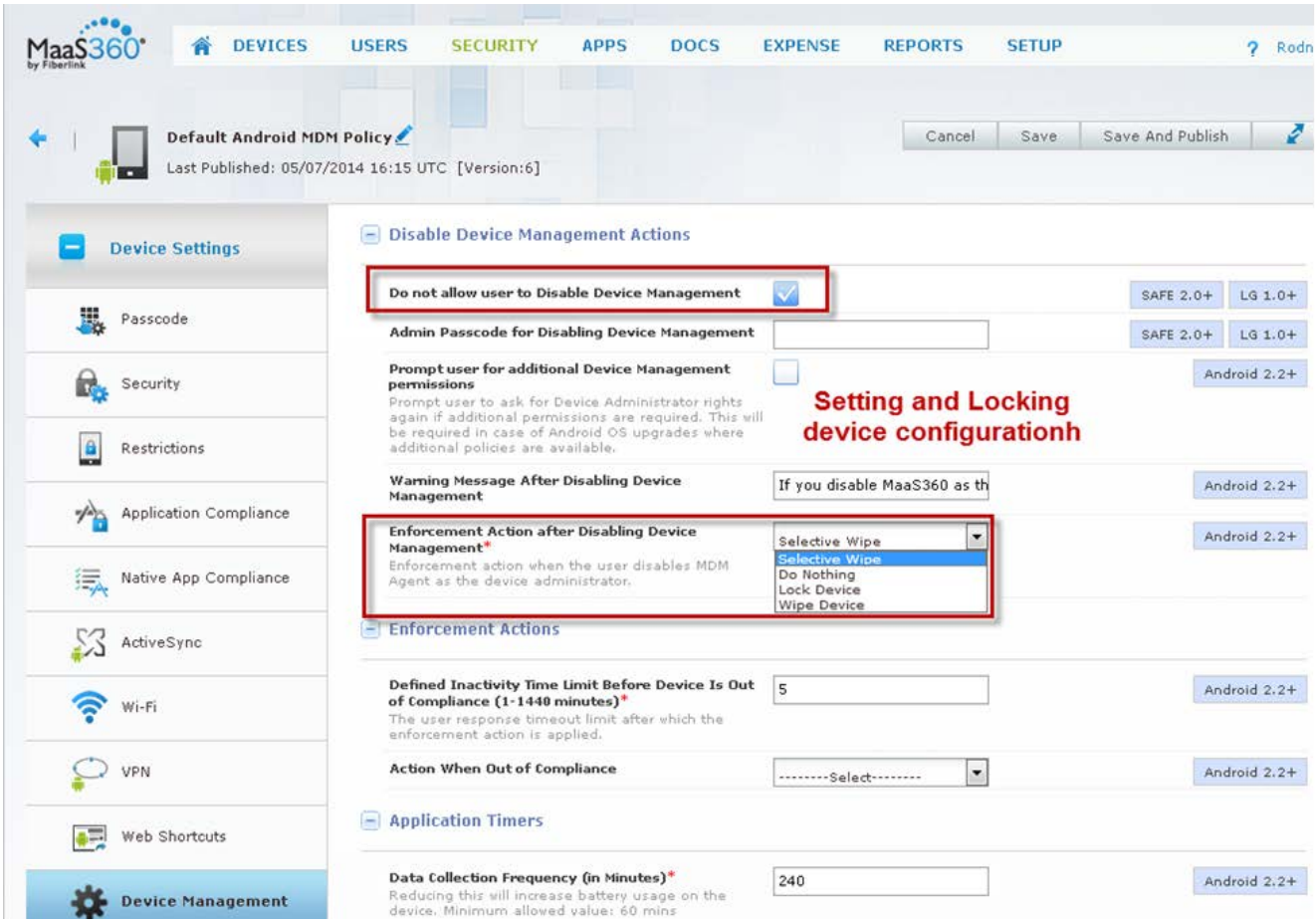
   Please create or have handy your Apple ID and password. If you do not have an AppleID or you would like to create a new AppleID, you may use the following link to do so:

   https://appleid.apple.com/cgi-bin/WebObjects/MyAppleId.woa/

2. Use the link you were provided by your Maas360 representative Michael Gordon (215-664-1835 / mgordon@fiberlink.com) to create an MDM account for your organization. The Quick Start wizard leads you through the steps needed to define your MDM. If applicable, follow the instructions to request and upload the required Apple push certificate necessary to run the MDM software on iOS devices. Android devices do not require a push certificate.

3. If using iOS devices on the MDM network, a push certificate should have been created in step 2. If that was skipped during the Quick Start process in step 2, it may be defined now. Under the **Setup** tab, select the **Services** option. Click on **Mobile Device Management** and see the **Apple MDM Certificate** section.

4. Configure the MDM to meet the "setting and locking device configuration" requirements of the CJIS policy. Click on the **Security** tab and **Policies** option. Then click on the **Add Policy** button. Under the **Device Settings** category, select **Device Management**.



NOTE: The Talon Mobile app encrypts data in transit from the Talon Mobile server to the mobile device for immediate viewing within the Talon Mobile app. No data is stored on the mobile device. The query results are stored only on the Talon Mobile server. However, if you still wish to enforce folder or disk level encryption, **please see the MaaS360 website for more detailed information on MaaS360 MDM setup and management.**

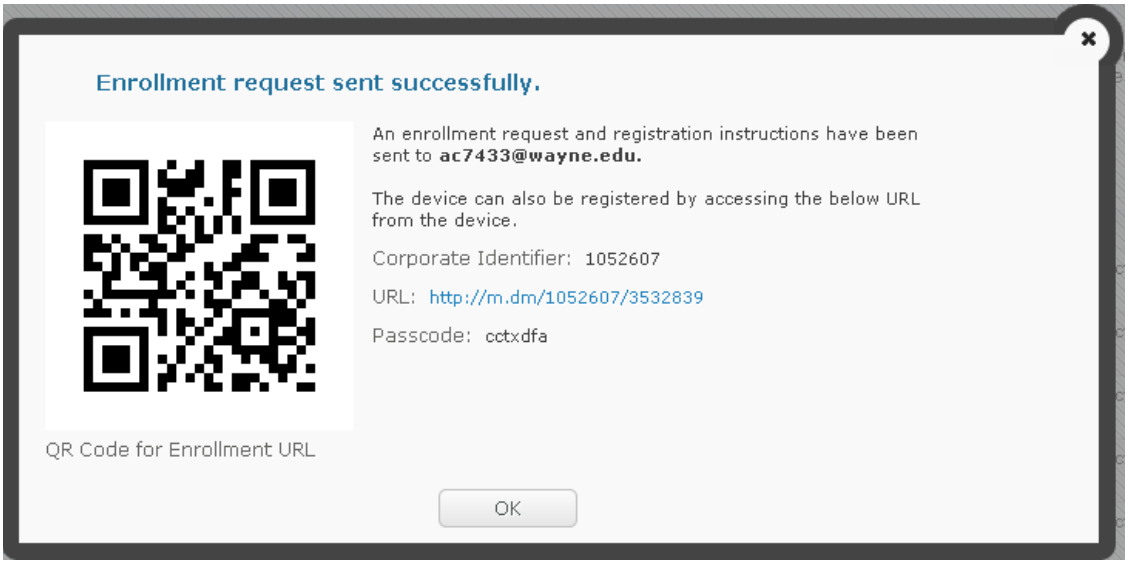
5. **To set and apply policies on devices and to detect unauthorized configurations or software/applications on devices**, search those topics in the Fiberlink MaaS360 support documentation using the following link.

http://www.maas360.com/support/visibility-and-control/maas360-services-user-guide/

Distribute the MDM and Talon Mobile App

6. Add a user to the MDM network. Click on the **Users** tab and click the **Add User** button. Here you are required to enter the **Username**, **Domain,** and **Email** of the user. However, the **User Name** and **Domain** fields are notation only fields. They are not used to distribute the MDM or apps. For the **Domain** name, you may use Core-Technology if you do not have another domain. While defining the user you may also add the user's device if desired (see the following step for details on adding a device).

7. If the user's device was not added in the last step, add the user's device by clicking on the **Add Device** link below the user line. When adding the device, an email/text is sent to the user with a link and passcode allowing the user to download and enroll in the MaaS360 MDM. Additionally, the enrollment information is displayed on your screen.



NOTE: If you are installing the MDM/Talon Mobile app on a device that does not have a dedicated telephone number or email address, you will need to provide the information displayed on the screen to the user manually (either verbally or by printing the screen and giving it to the user).

8. Repeat steps 6 and 7 for each user that you would like added to the MDM network. If for some reason a user was not enrolled, you may repeat step 7 again.

9. Obtain the Talon Mobile app file(s). In a separate browser (Google Chrome or Firefox), use the links below to access and save the file(s) to your desktop or other location.

   IOS: https://csb9.coretechcorp.com:2306/manager/TMA_IOS.ipa

   Android: https://csb9.coretechcorp.com:2306/manager/TMA_Android.apk

10. Upload the Talon Mobile app files you obtained in the last step to the MDM network for distribution. Under the **Apps** tab, click the **Add** button. Select to add an "**Enterprise App for Android**" or "**Enterprise App for iOS**" depending on the device's operating system. To upload the Talon Mobile app file(s), browse to the location where you saved the app file(s) in the last step. You may also choose to distribute the app in this dialog box. If so, select the appropriate distribution option (e.g., distribute to all, a group, or a specific user). Place a mark in the **Instant Install** checkbox. Depending on the distribution method used (e.g., distribute to a specific user, etc.), this step may need to be repeated. Repeat this step for each operating system type (e.g., Android, iOS) allowed on your network.

11. If the app was not distributed in the last step, distribute the app by clicking on the **Distribute** link below each Talon Mobile app line and distribute to all, a group, or a specific user. Place a mark in the **Instant Install** checkbox. Depending on the distribution method used (e.g., distribute to all, a group, or a specific user), this step may need to be repeated. The Talon Mobile app will then be delivered to the device through the MDM. If the **Instant Install** checkbox was marked, the app should install automatically. Otherwise, the user of the device will have to install the Talon Mobile app from within the MaaS360 MDM app on his or her device.

    NOTE: Some Android devices may require the user to allow the device to install apps from sources other than the Play store. In the client device **Settings**, check the **Security** section to allow the installation of apps from **Unknown Sources.**

12. Provide the **IP** and **Port** of the Talon Mobile server to your users. Once the Talon Mobile app is installed on the mobile devices, each user will need to verify that the appropriate values are entered into the Talon Mobile app. If you are unsure of these values, the Core Technology representative who performed the installation of the Talon Mobile product on your server can provide this information.

    NOTE: For those customers with a subscription to the Core Service Bureau's (CSB) hosted Talon Mobile product, the **IP** and **Port** values will be automatically populated in the users' Talon Mobile app with the following information:

    Host: csb5.coretechcorp.com (CSB hosted)
    Port: 2246 (CSB hosted)

Maintain the MDM

1. To configure setup information, see the **Setup** tab.

2. To define others as administrative users for the MDM if desired, click on **Administrators** under the **Setup** tab.

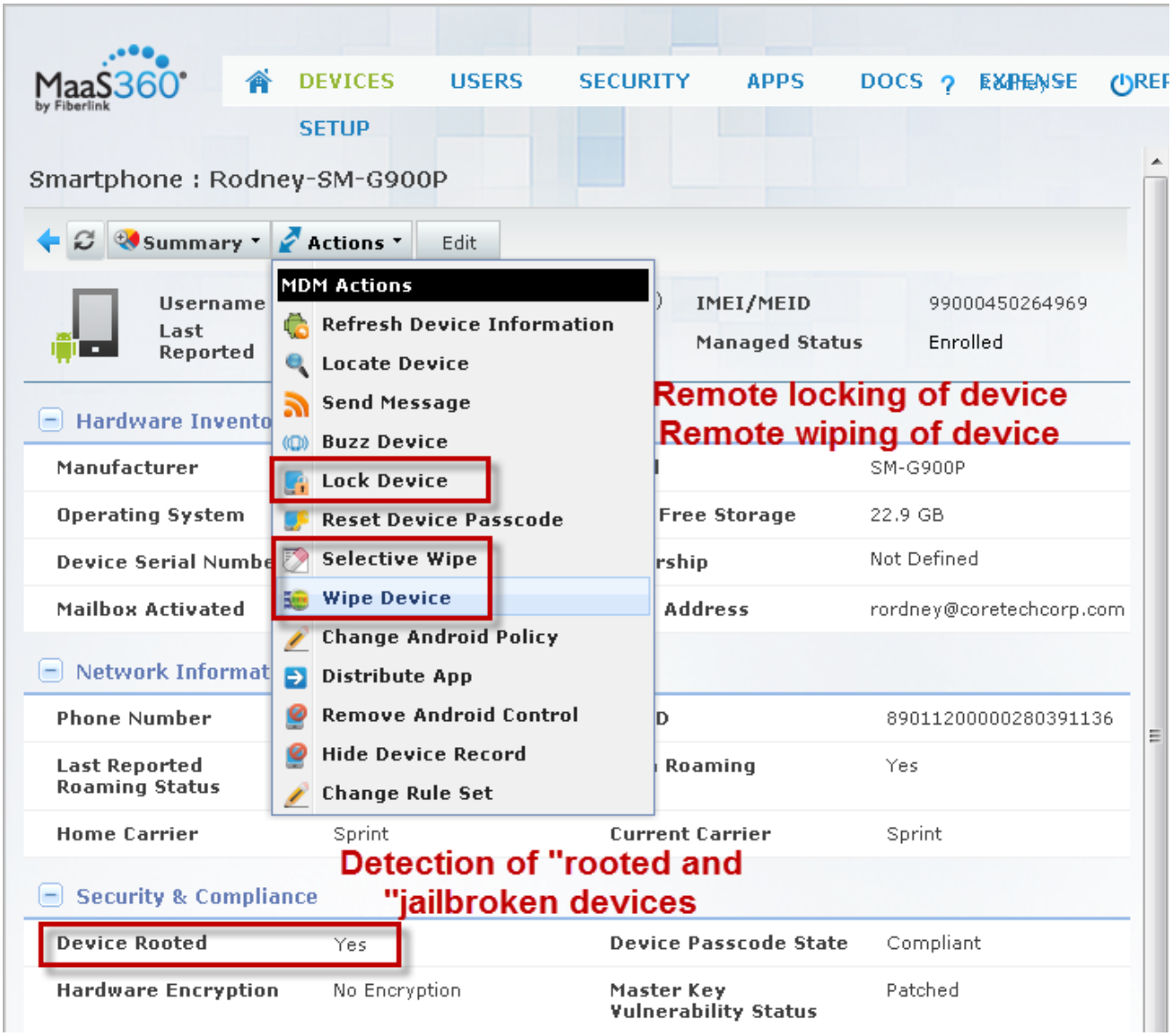
3. To monitor users, see your **My Alert Center** (home screen), or for other informational views, see the **Users**, **Devices**, or **Reports** tabs.

4. To add a new user/device to the MDM network and distribute the app, perform steps 6, 7, and 11 of the **Initial Setup** section.

Noncompliance Actions

1. View the **My Alert Center** (home page) for alerts of jailbroken or rooted devices.

2. Remote lock and wipe mobile device. Within the device view, click the **Actions** button and select the appropriate **Lock device, Wipe device,** or **Selective Wipe** options.



Please see the MaaS360 website for more information on MaaS360 MDM setup and management.