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

Meraki MDM

You have chosen the Meraki MDM (Dashboard/Systems Manager). Below are the basic steps to create the MDM network and distribute the Talon Mobile app. **Please see the Meraki website for more detailed information on Meraki MDM setup and management.**

Meraki Dashboard Login Page:
https://account.meraki.com/secure/login/dashboard_login

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 3), you must have a valid AppleID. An AppleID (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:

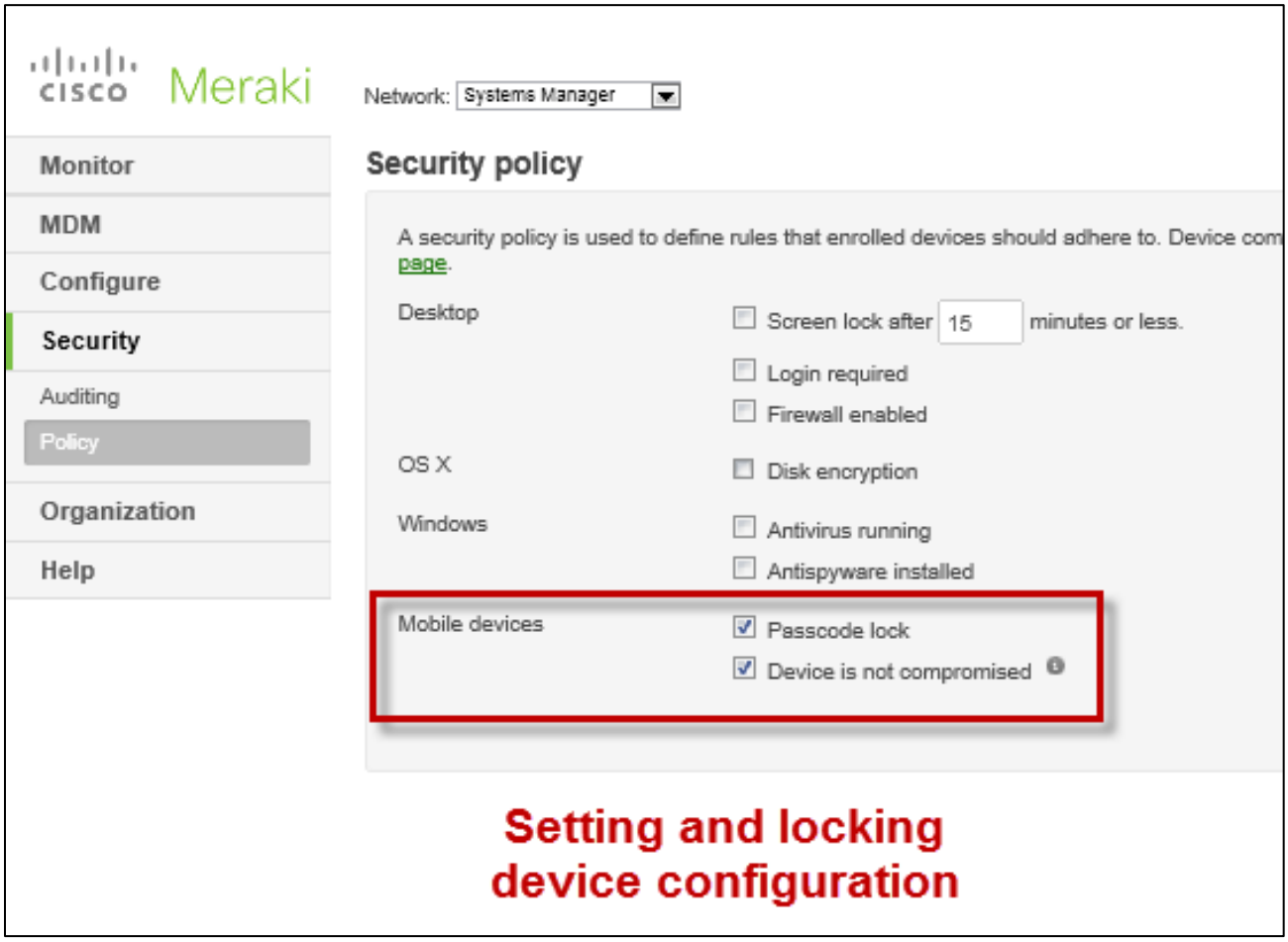
   https://appleid.apple.com/cgi-bin/WebObjects/MyAppleId.woa/

2. Use the link on the previous page to create a Meraki MDM **Dashboard** account for your organization.

3. If supporting iOS devices on the MDM network, follow the instructions to request and upload an Apple push certificate, which is required to run the Meraki MDM app (**System Manager**) on iOS devices. Under the **Organization** category, select **Settings** and follow the instructions listed there to obtain the request form signed by Meraki, upload the signed request form to Apple, and ultimately upload the Apple push certificate to the Meraki MDM **Dashboard**.

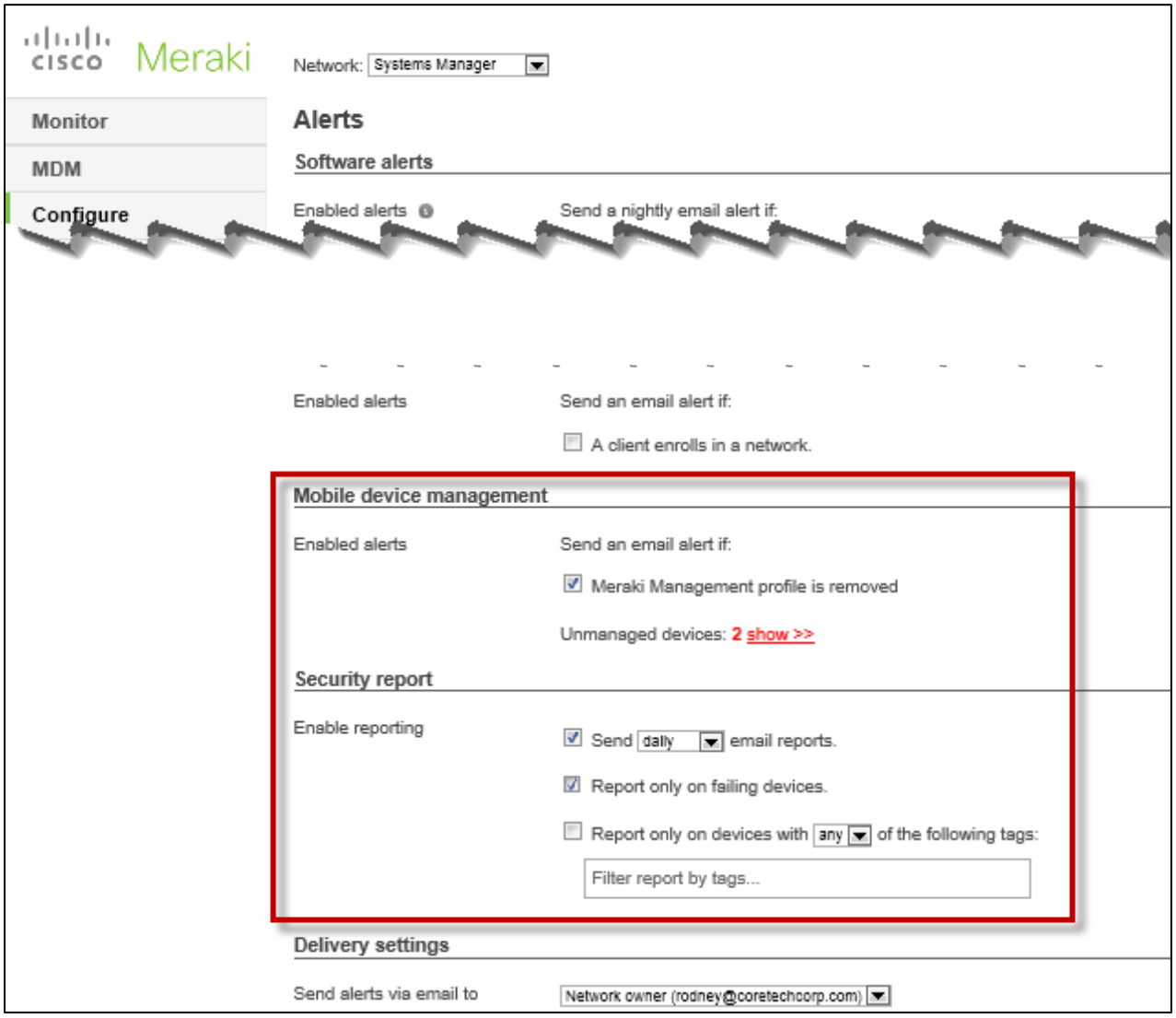
4. Create an MDM network. Under the **Organization** category, select **Create network**. You do not need to add devices here. That will be done in a later step.

5. Configure the MDM to meet the "setting and locking device configuration" requirements of the CJIS policy. Under the **Security** category, select **Policy** and define the **Mobile devices** security policy.



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 Meraki website for more detailed information on Meraki MDM setup and management.**

6. Configure alert notification of device noncompliance. Under the **Configure** category, select **Alerts** and define the type of alerts to be generated.

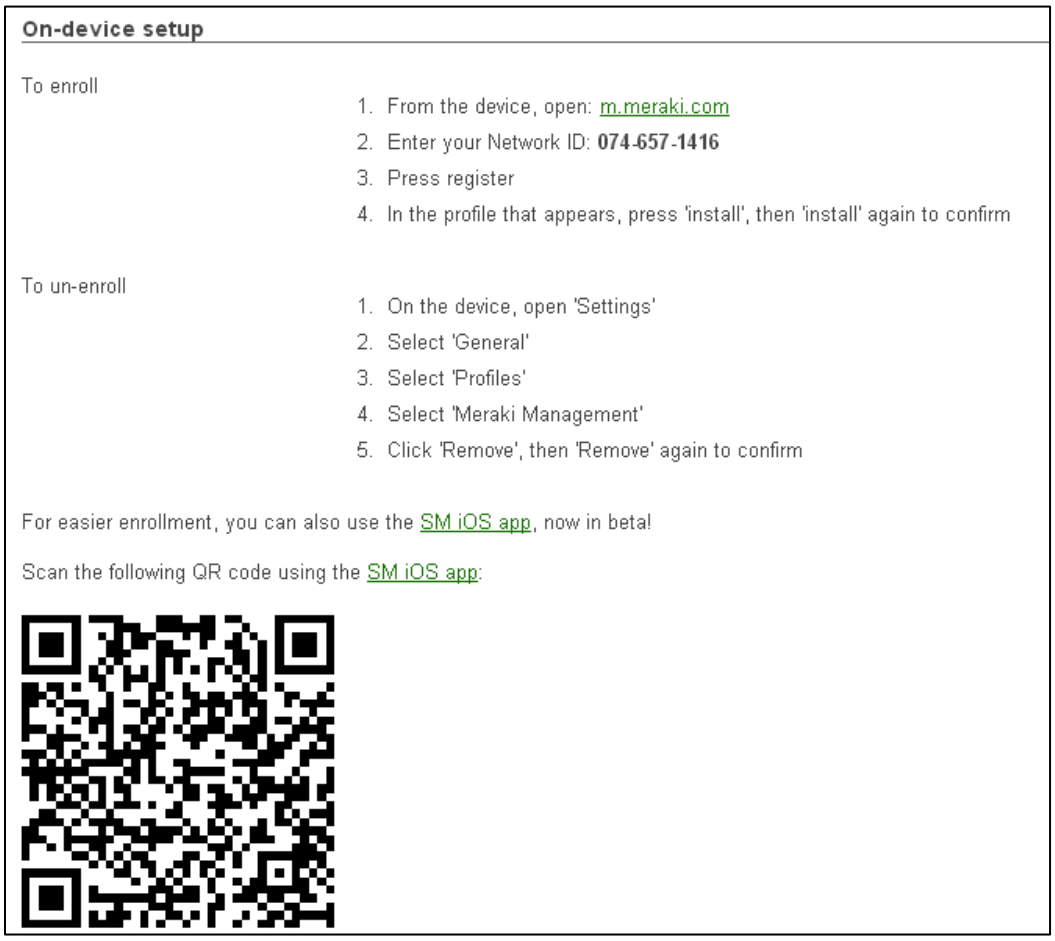


7. **To set and apply policies on devices and to detect unauthorized configurations or software/applications on devices**, search those topics in the Cisco Meraki support documentation using the following link.

   https://docs.meraki.com/display/SM/Systems+Manager+MDM

Distribute the MDM and Talon Mobile App

8. Distribute the MDM. Under the **MDM** category, select **Add devices,** and click on the ***type of device*** (e.g., Android, iOS) desired. Follow the instructions given. Once selected, several enrollment delivery options will display. Use the distribution enrollment option that works best for your agency to deliver the Meraki MDM app (**Systems Manager**). Repeat this step for each user's device you wish to add to the MDM network. Once the user enrolls in the Meraki MDM **Systems Manager** on the device, it may take several minutes (about 10 minutes or so) before the synchronization process is complete and the user can see the Meraki MDM **Systems Manager** app on the device. This step may be used at any time to deliver the **Systems Manager** as well as any already defined apps to a new client device.



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).

9. If using Android devices on the MDM network, you are required to create a "backpack" for the delivery of applications. Under the **MDM** category, select **Settings**. Click on the **Backpack** tab. Click on the **Create a Backpack Definition** link. If the Backpack is already defined, click on the **Add a new file to this backpack** link at the bottom of the screen. To add the app file, enter the URL where the Talon Mobile app file is located (see location below). Once defined, the Talon Mobile app will automatically be delivered to the device through the MDM. The user of the device will then need to install the Talon Mobile app from within the Meraki MDM **Systems Manager** app.

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

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

10. If using iOS devices on the MDM network, obtain the Talon Mobile app file for iOS. In a separate browser (Google Chrome or Firefox), use the link below to access and save the file to your desktop or other location.

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

11. If using iOS devices on the MDM network, add the Talon Mobile app file to the MDM network for distribution. Under the **MDM** category, select **Apps**. Click the **Add new** button and select the "**iOS enterprise app**" option. To add the app file, upload the Talon Mobile app file that was saved in the previous step. Once defined, the Talon Mobile app will automatically be delivered to the device through the Meraki MDM **Systems Manager** app. The user of the device will then need to install the Talon Mobile app from within the Meraki MDM **Systems Manager** app.

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 may 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 settings such as time zone, select **General** from the **Configure** category.

2. To define others as administrative users for the MDM, select **Administrators** under the **Organization** category.

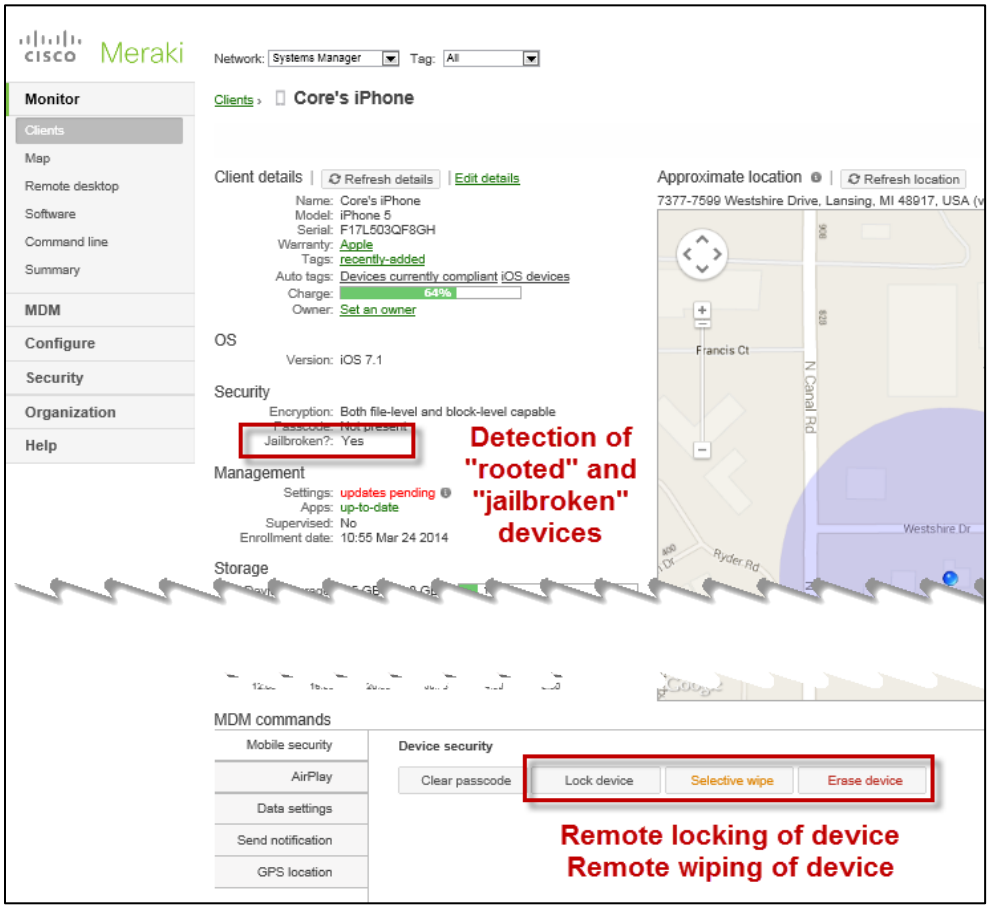
3. To monitor the Client devices, select **Clients** under the **Monitor** Category.

4. To distribute the Meraki MDM Systems Manager app and Talon Mobile App to new devices on the network, perform step 8 in the **Distribute the MDM and Talon Mobile App** section above.

Noncompliance Actions

1. Audit the Client devices. Select **Auditing** under the **Security** Category.

2. Remote lock and wipe of Client device. Within the Client view, click the appropriate **Lock device** and **Selective wipe** or **Erase device** buttons.



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

