



MaaS360® for Mobile Devices: Generating an APNs Certificate



Copyright © 2012 Fiberlink® Corporation. 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 Corporation.

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

Fiberlink Corporation
1787 Sentry Parkway West
Blue Bell, PA 19422

February 2012

Table of Contents

Overview	4
What is an APNs Certificate?	4
Generating an APNs Certificate for MaaS360 for Mobile Devices	4
Generating an APNs Certificate from a Mac	5
Create a Certificate Signing Request (CSR)	5
Upload the CSR to the MaaS360	7
Upload prepared CSR to Apple	9
Complete the CSR Request	10
Export the APNs Certificate	12
Generating an APNs Certificate from a Windows Server	14
Create a Certificate Signing Request (CSR)	14
Upload the CSR to the MaaS360	19
Upload prepared CSR to Apple	21
Complete the CSR Request	23
Export the APNs Certificate	25
Uploading the APNs Certificate to MaaS360 for Mobile Devices	27

Overview

In order to set up MaaS360 for Mobile Device to work effectively with iOS devices, you will need to generate an Apple Push Notification service (APNs) certificate that is unique to MaaS360. Fiberlink does not provide this certificate, but provides information on how you can obtain one from Apple.

What is an APNs Certificate?

The Apple Push Notification service (APNs) is used to allow MaaS360 for Mobile Devices to securely communicate with your iOS devices over the air (OTA).

MaaS360 for Mobile Devices uses your APNs certificate to send notifications to your devices when the administrator requests information, or during a defined monitoring schedule. No data is sent through the APNs service, only the notification.

Generating an APNs Certificate for MaaS360 for Mobile Devices

The following section will walk you through the steps to obtain an APNs certificate from Apple. There are two sets of instructions for creating a certificate from either a Mac or from a Windows server.

Before starting, regardless of which operating system you have, be sure you have the following:

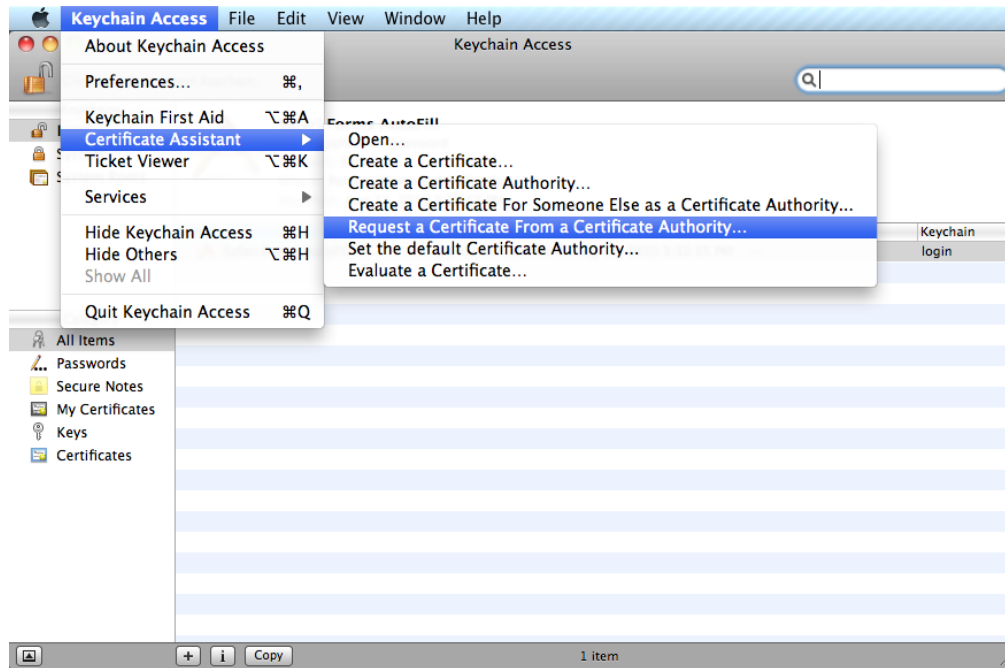
- An Apple ID. (Can be created at <https://appleid.apple.com>)
- Mac OS X workstation or Windows Server with Administrative permissions.
- Web browser (Safari or Chrome are required to work with Apple's website).

Generating an APNs Certificate from a Mac

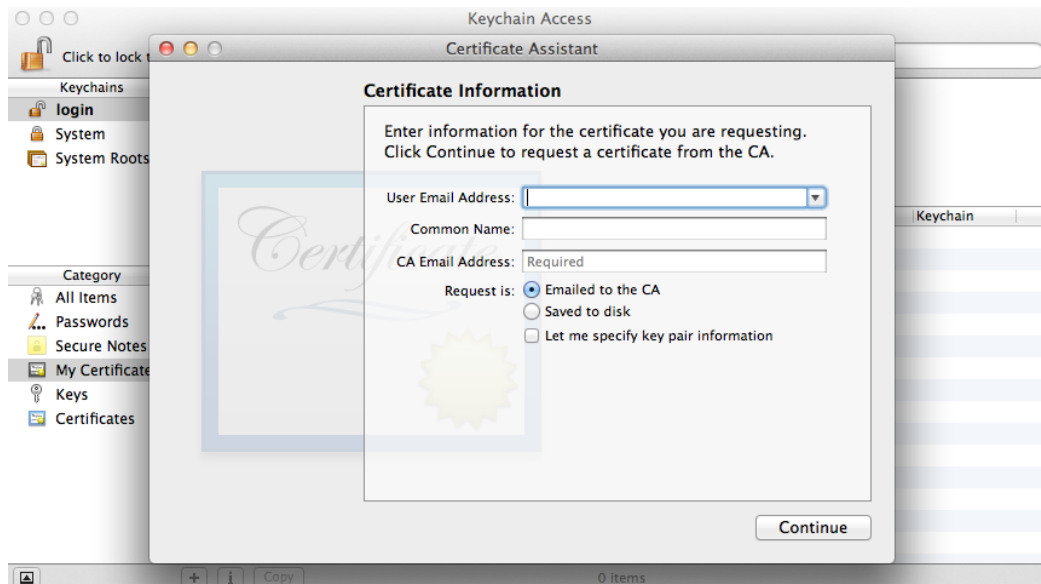
The following instructions are valid for creating an APNs certificate from a Mac device.

Create a Certificate Signing Request (CSR)

1. Click **Applications > Utilities > Keychain Access**.
2. In the sidebar, select **login** under **Keychain**. Select **Certificates** under **Category**.
3. Select **Keychain Access > Certificate Assistant > Request a Certificate From a Certificate Authority**.



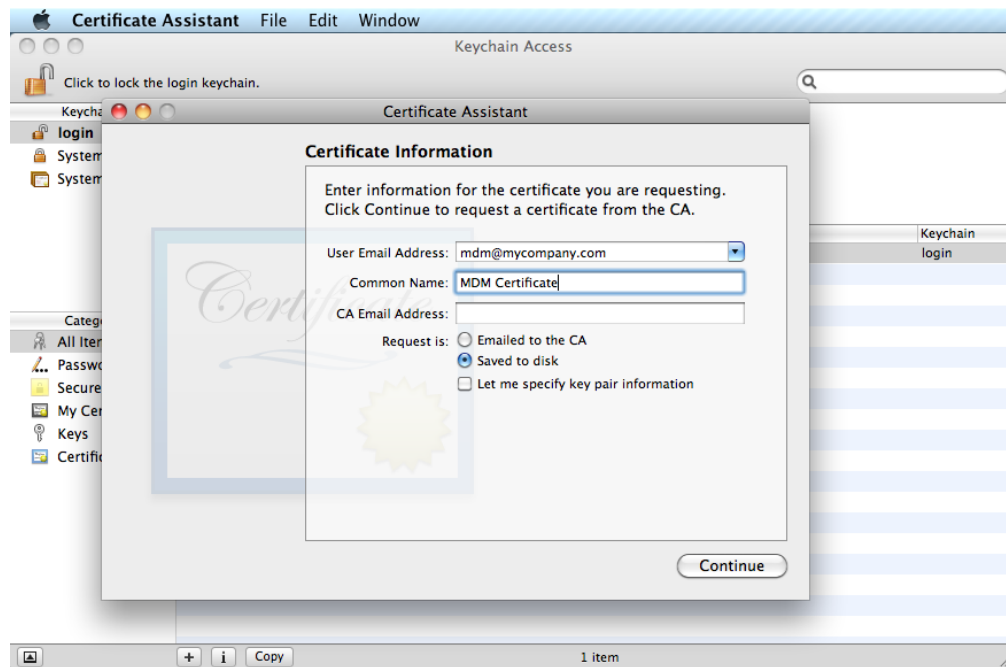
4. This launches the Certificate Assistant wizard.



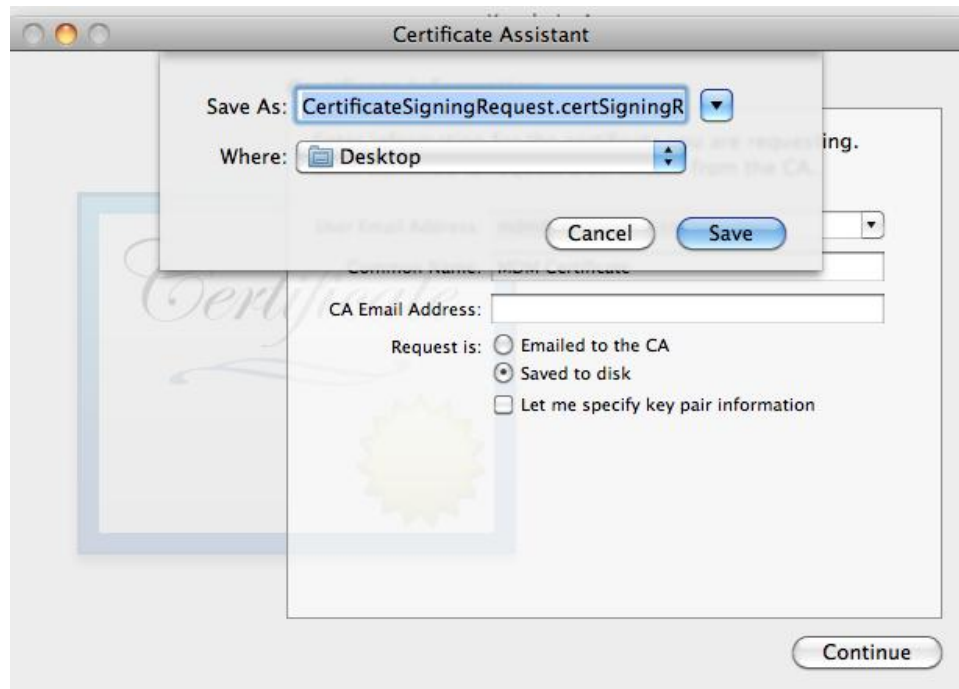
5. Enter the **User Email Address** or select it from the drop-down list, and enter the **Common Name** of the person registered as the Apple account holder.

Note: You must use an email address that has not been used before to generate a certificate.

6. The **CA Email Address** can be left blank if you do not select **Emailed to the CA**.



7. Click to select **Saved to disk**. Click **Continue**. A dialog opens.



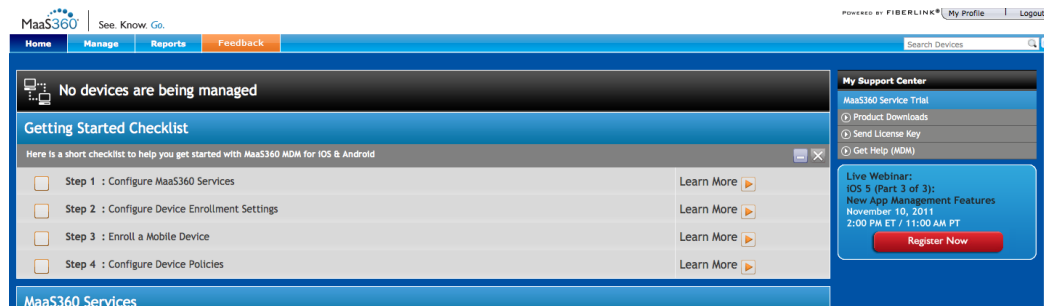
8. Enter a file name and path to save the CSR and click **Save**. Remember that location. The file name has no restrictions. You are now ready to upload the CSR file.

Upload the CSR to the MaaS360

1. In your browser, navigate to MaaS360, <https://portal.fiberlink.com>.

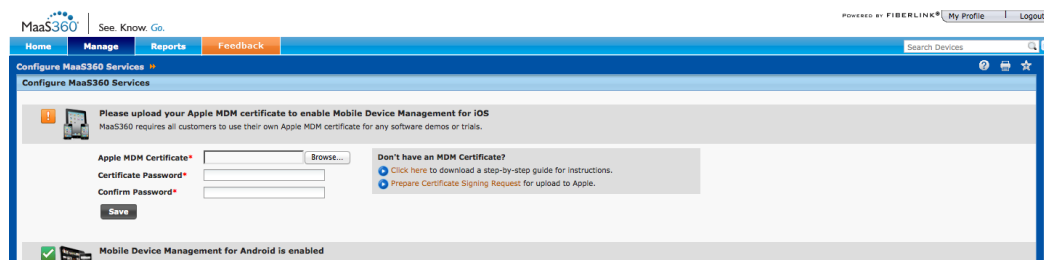


2. Enter your MaaS360 username and password, then click **Log In**.

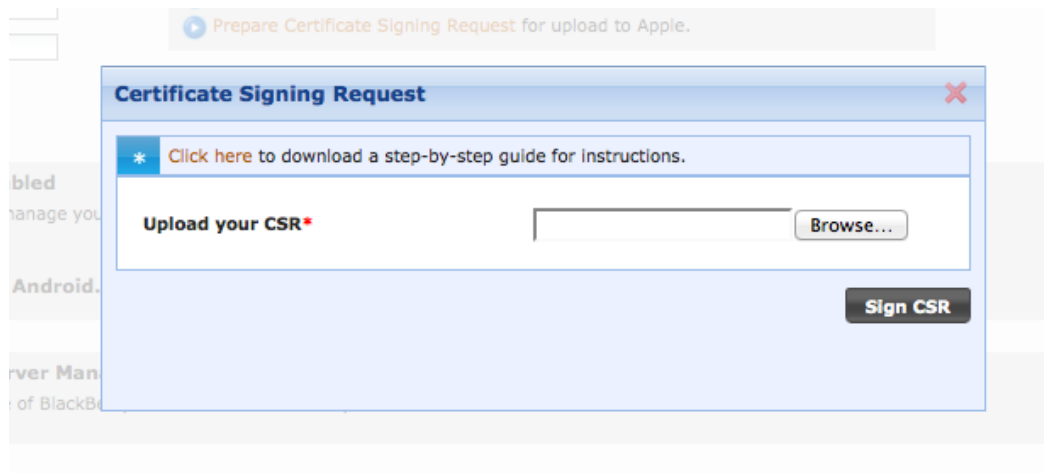


3. Click on **Step 1: Configure MaaS360 Services**.

Note: If you do not see this, go to the **Manage** menu, and click **Configure MaaS360 Services**, under **MDM Services Administration** heading.



4. On the right hand side of the iOS section, under *Don't have an MDM Certificate?*, click **Prepare Certificate Signing Request**.



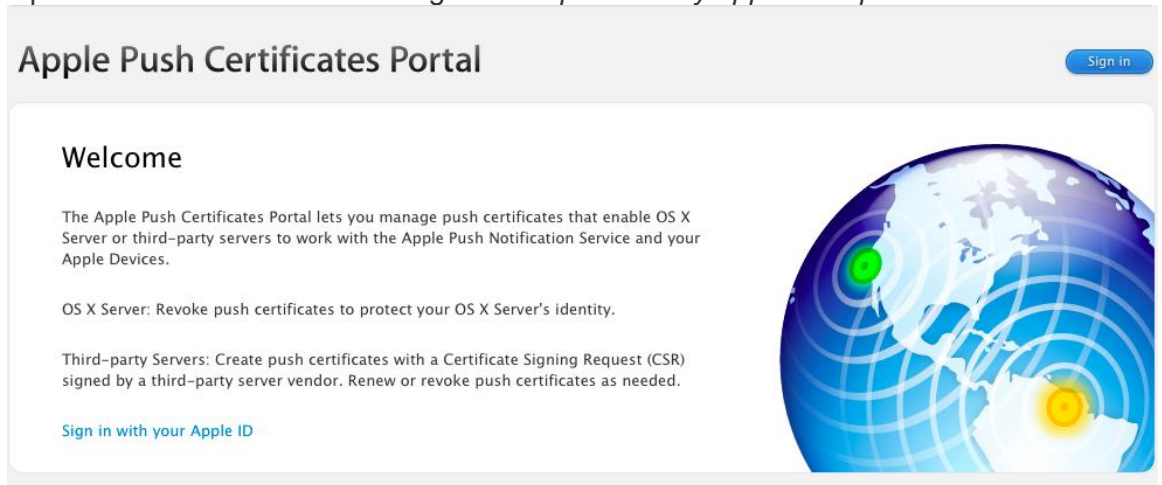
5. Click on the **Browse** button, and select the CSR you created earlier. Then click **Sign CSR**.



6. Click on **Click Here** to download the prepare Certificate Signing Request that is ready to be uploaded to Apple.

Upload prepared CSR to Apple

1. Open Safari or Chrome and navigate to <https://identity.apple.com/pushcert/>.



2. Click **Sign in with your Apple ID**, then enter in your Apple ID and password, and click **Sign in**.

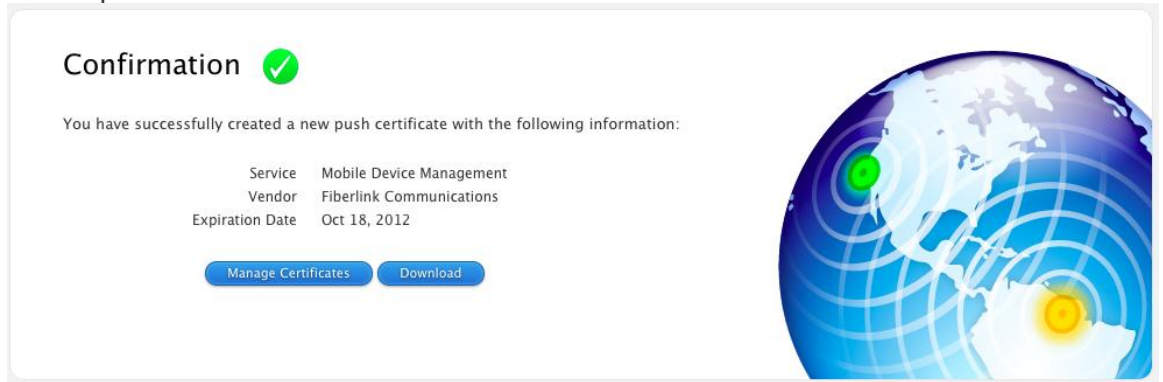


3. Click **Create a Certificate**. You will now need to accept the terms and conditions. If you agree, check the box and click "Accept".



4. Now you will be prompted to upload the file that you downloaded earlier from MaaS360. By default it is named "FiberlinkCSR.txt".
5. Click Choose File and locate the file

6. Click Upload.



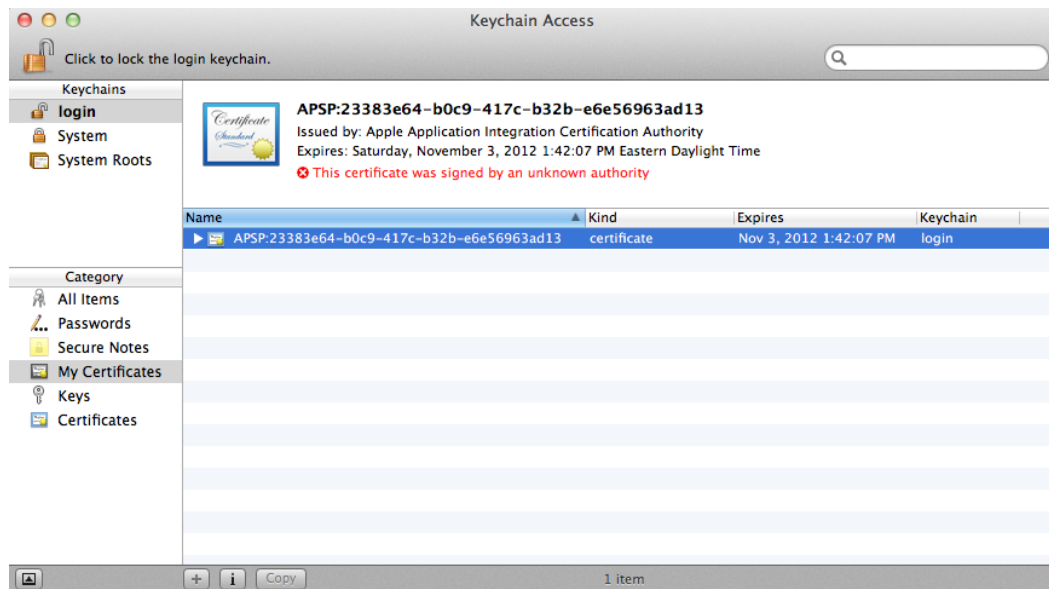
7. After a few seconds, you should see the screen above.
8. Click "Download". You should now have a file named "MDM_Fiberlink Communications_Certificate.pem".

Complete the CSR Request

1. On your local drive, open the file in the Finder.



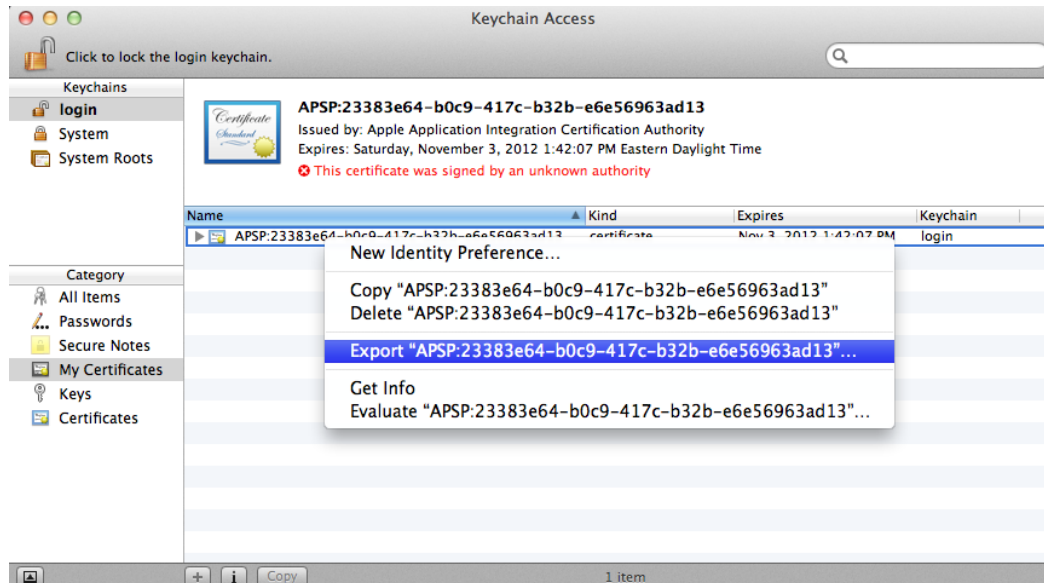
2. Open it with Keychain Access, and complete the CSR process by adding the file to a keychain. If you see a prompt to select a keychain, pick **login** and then click **Add**.
3. In the sidebar, select **login** under **Keychain**. Select **Certificates** under **Category**, and click to expand Apple Production Push Services to verify that you see the private key for your common name.



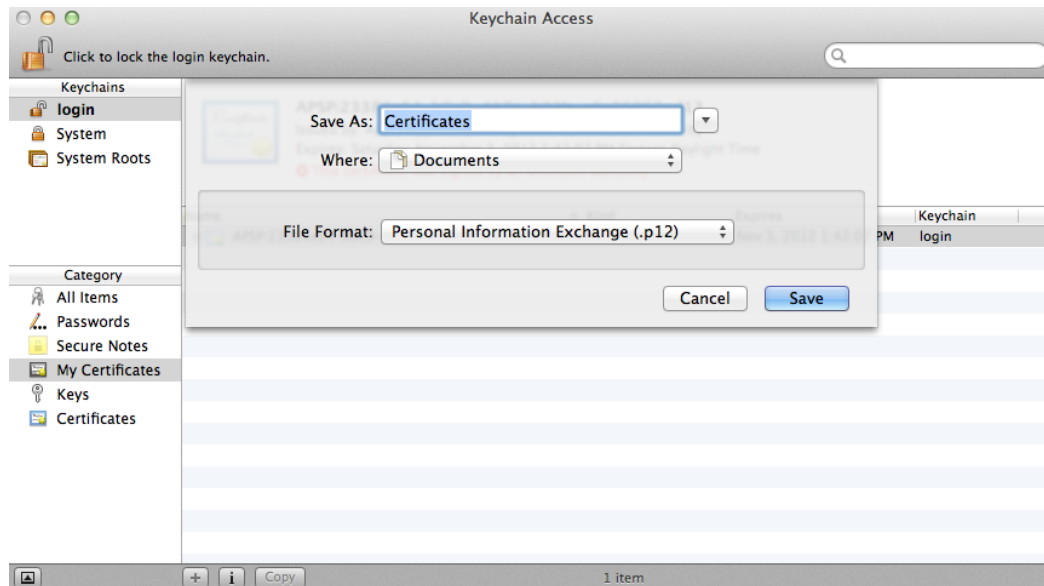
Note: If you do not see the private key, a reboot will generally cause it to appear.

Export the APNs Certificate

1. While viewing the listing of the private key on the Certificates page, right-click (CTRL-click) the private key name and select **Export**.

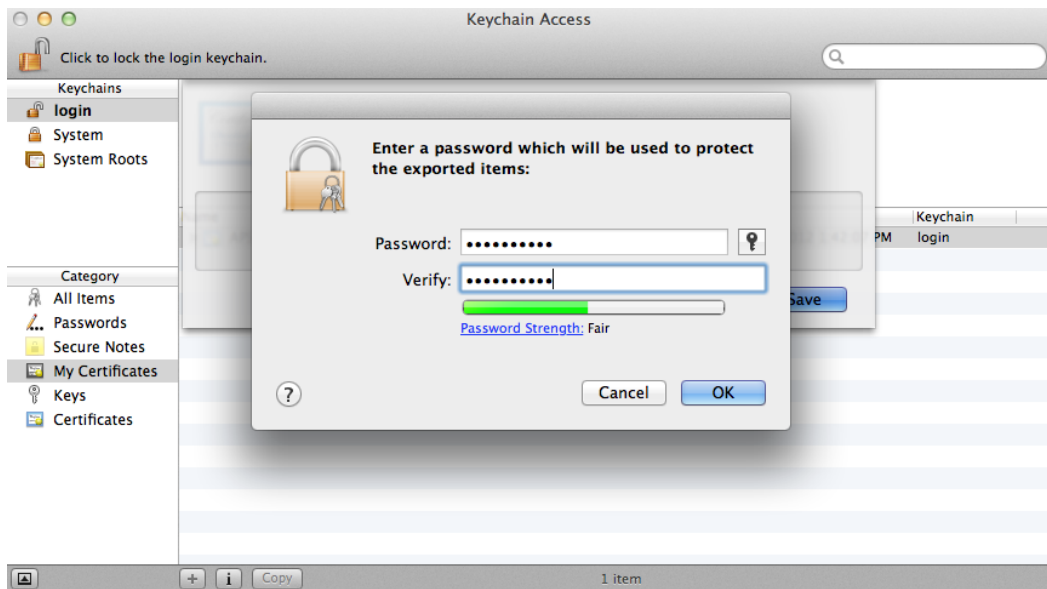


2. Click **Save** to save the private key file to your desktop in .p12 format.

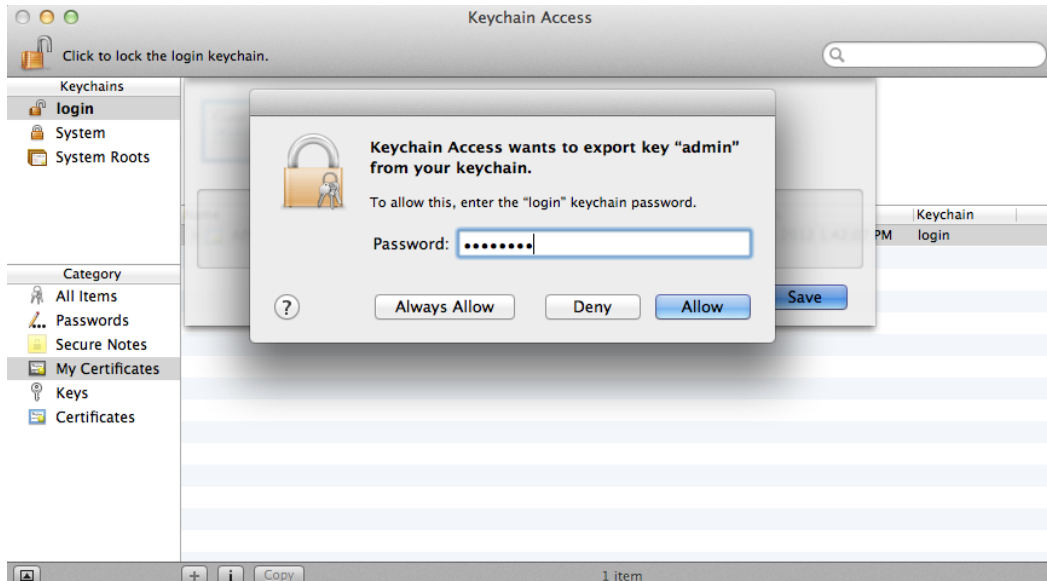


Note: If .p12 is not available as a File Format, then you are not exporting the certificate correctly.

3. Enter a new password, and enter again to verify. Note that the bar just below the **Password** and **Verify** fields indicates the strength of the password you just created. It is suggested that you create a strong password. Click **OK**.



4. When prompted enter the login keychain password. Click **Allow**.



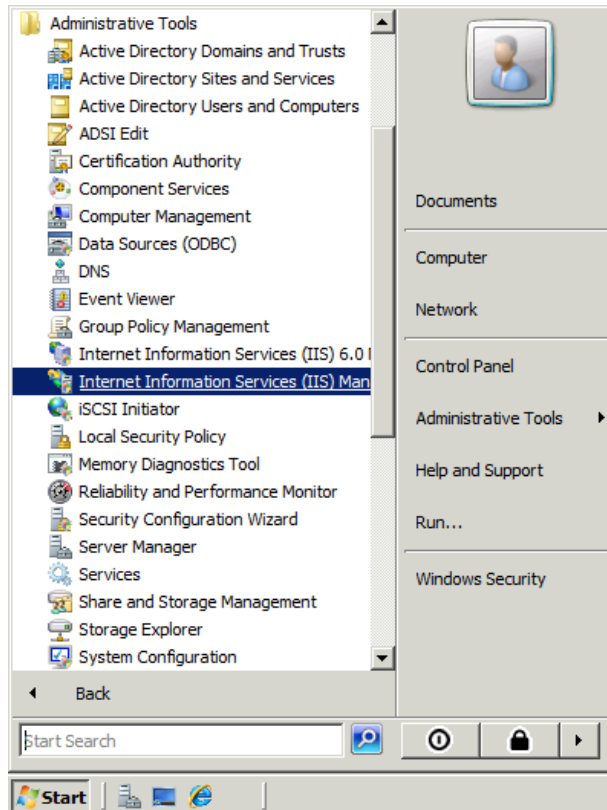
You are now ready to use the APNs certificate (*.p12) and password that you used to export the certificate. Refer to *Uploading the APNs Certificate to MaaS360 for Mobile Devices*.

Generating an APNs Certificate from a Windows Server

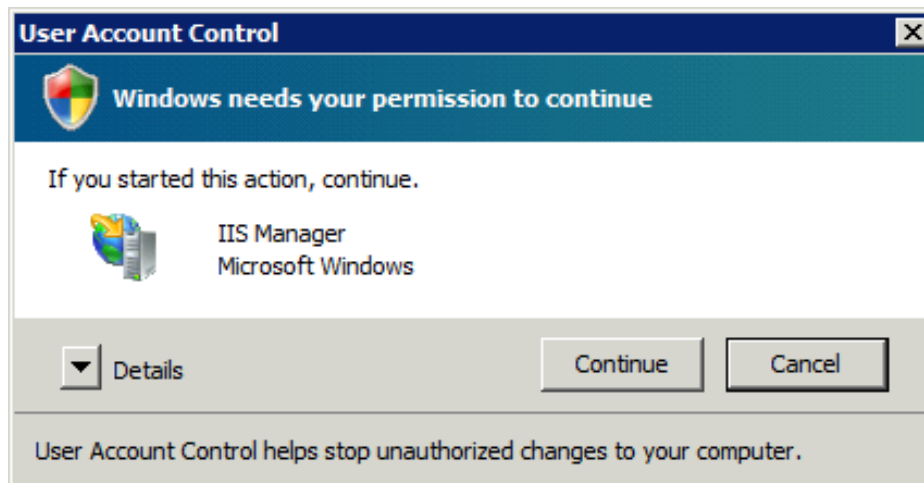
The following instructions are valid for any Windows server, and do not have to be performed on the MaaS360 for Mobile Devices server.

Create a Certificate Signing Request (CSR)

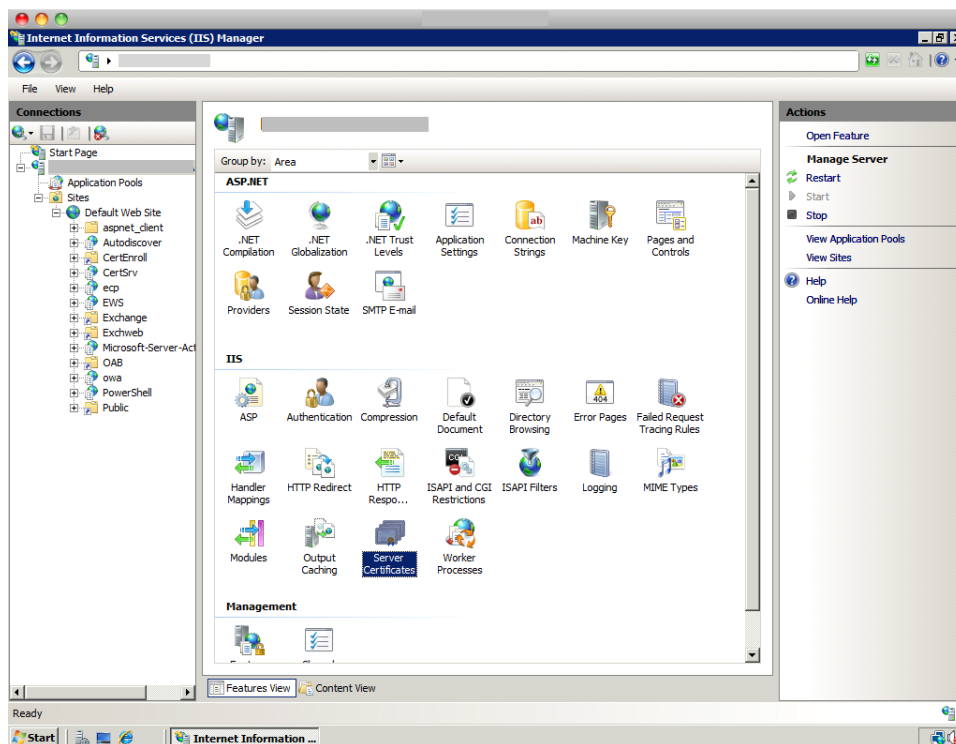
1. From the Windows server, click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.



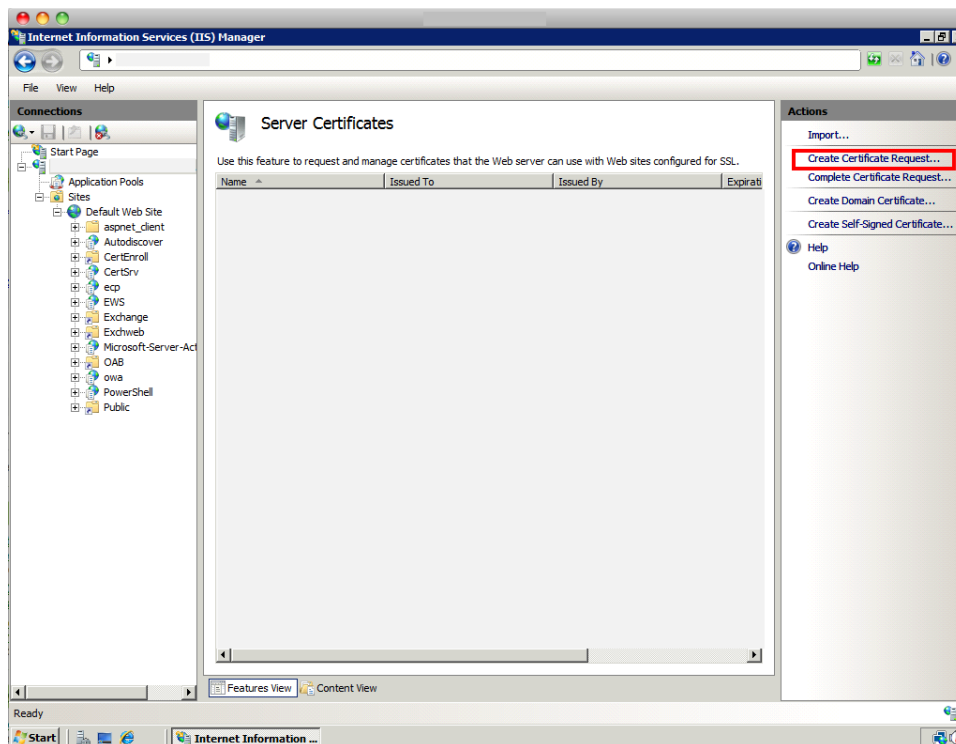
2. The User Account Control dialog prompts you to confirm that you wish to continue.



3. Click **Continue**. The IIS Manager displays.



4. Click on your server name to display its contents. Double-click **Server Certificates**. The Server Certificates page displays with a list of Actions.



5. In the Actions menu, click **Create Certificate Request**. The Distinguished Name Properties page displays. Enter the required information for your company:
 - a. Common Name – this is the name associated with your Apple Development account, for example, My Company MDM Certificate.

- b. Organization – your legal company name.
- c. Organizational unit – your department in the organization.
- d. City/locality – the city where your company is located.
- e. State/province- the state/province where your company is located.
- f. Country/region – select a country/region from the drop-down list.

Request Certificate [?] [X]

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

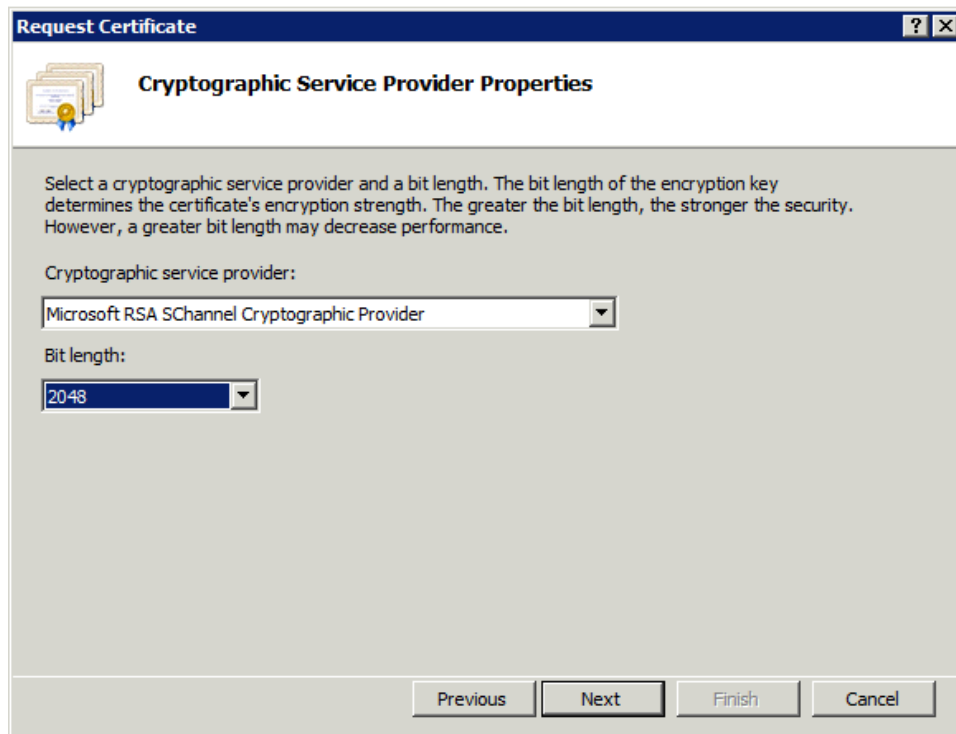
Organizational unit:

City/locality:

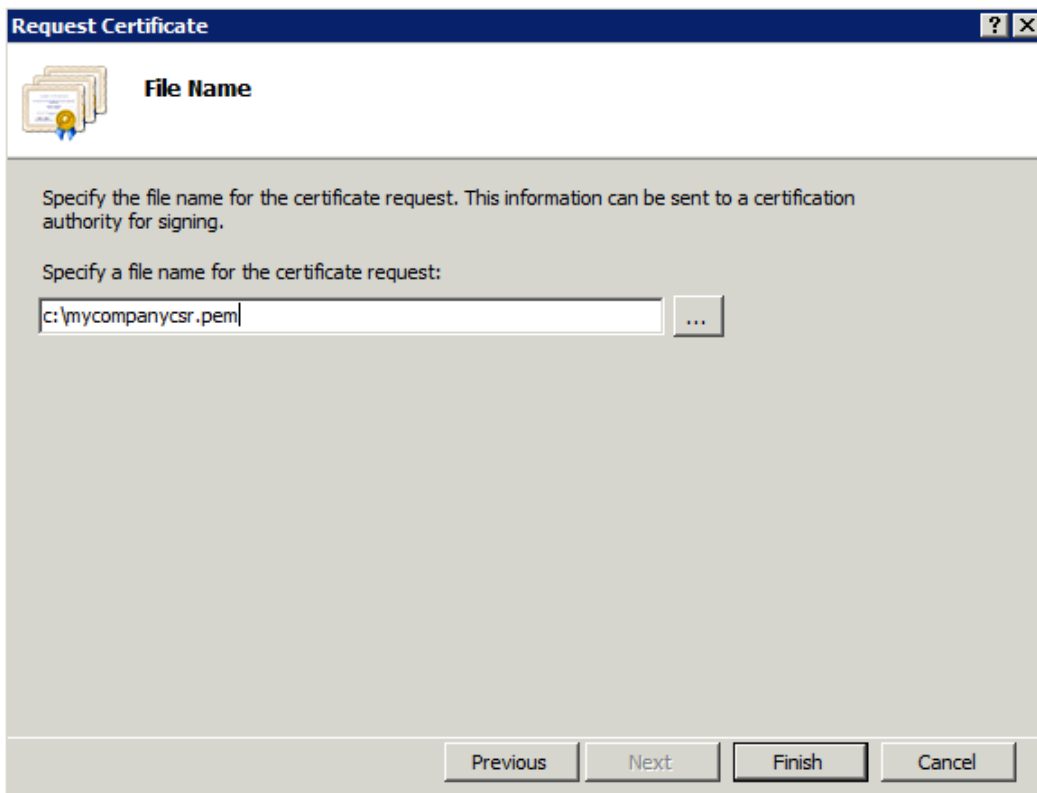
State/province:

Country/region:

6. Click **Next**. The Cryptographic Service Provider Properties page displays.



7. Accept the defaults, and click **Next**. The File Name page opens.



8. Enter a file name and path for the certificate request. You will need to know the file name and location when you upload the certificate request.
9. Click **Finish**. You are now ready to upload the certificate request.

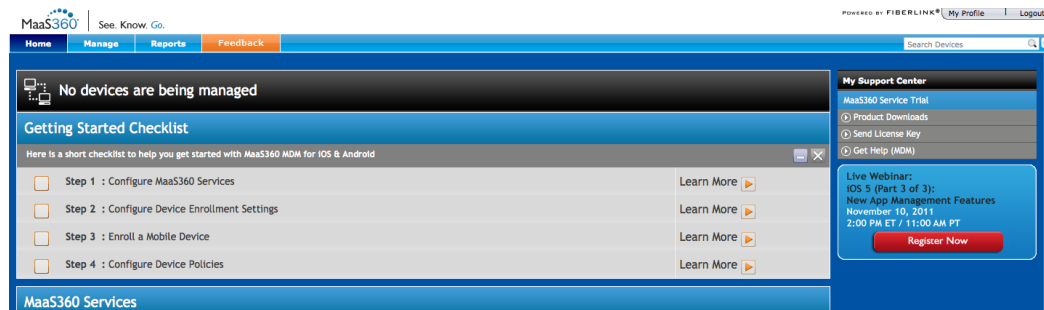
Upload the CSR to the MaaS360

1. In your browser, navigate to MaaS360, <https://portal.fiberlink.com>.



The screenshot shows the MaaS360 login page. At the top is the FIBERLINK logo and a navigation bar with links: ABOUT, PRODUCTS & SERVICES, SOLUTIONS, NEWS & EVENTS, and KNOWLEDGE CENTER. Below this is a banner with the MaaS360 logo and the tagline "See. Know. Go.". A disclaimer states: "You are accessing a privately owned and operated system. Access and use are limited to authorized persons only. Anyone accessing or using this system improperly or without proper authorization is subject to civil, criminal or injunctive action." The main section is titled "Log in to MaaS360 - Fiberlink Communications" and contains a login form with fields for Username and Password, a "Forgot your Password" link, a "Remember Me" checkbox, and a "Log In" button. To the right of the form is a "Quick Help" section with links: "Why is this secure?", "Email this page", and "Bookmark this page". At the bottom, it says "Best viewed with a screen resolution of 1024 x 768" and "© 2011 Fiberlink Communications Corp. All Rights Reserved. | PRIVACY AND LEGAL".

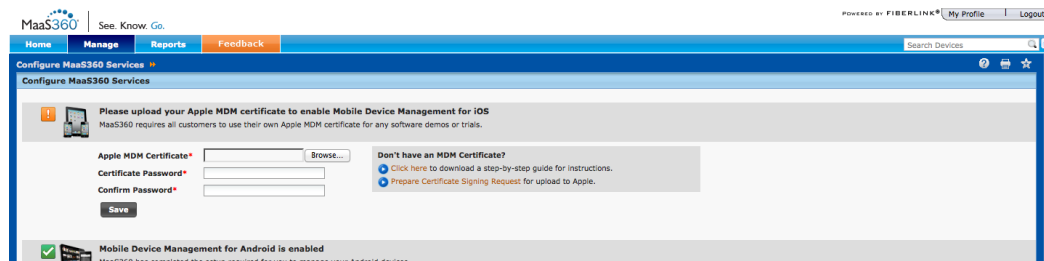
2. Enter your MaaS360 username and password, then click **Log In**.



The screenshot shows the MaaS360 dashboard after a successful login. The top navigation bar includes "Home", "Manage", "Reports", and "Feedback". A search bar is on the right. The main content area shows "No devices are being managed" and a "Getting Started Checklist" with four steps: "Step 1: Configure MaaS360 Services", "Step 2: Configure Device Enrollment Settings", "Step 3: Enroll a Mobile Device", and "Step 4: Configure Device Policies". Each step has a "Learn More" link. On the right, there is a "My Support Center" section with links for "MaaS360 Service Trial", "Product Downloads", "Send License Key", and "Get Help (MDM)". A "Live Webinar" announcement for iOS 5 is also present.

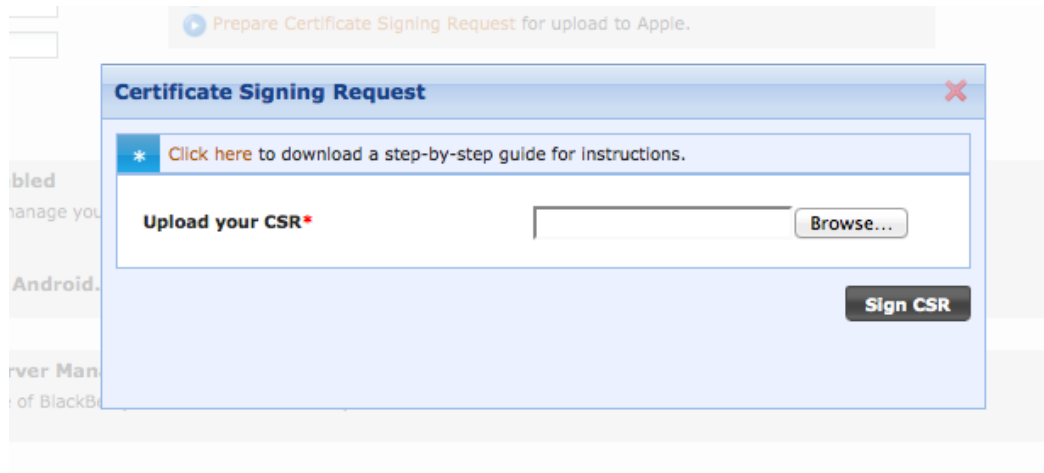
3. Click on **Step 1: Configure MaaS360 Services**.

Note: If you do not see this, go to the **Manage** menu, and click **Configure MaaS360 Services**, under **MDM Services Administration** heading.



The screenshot shows the "Configure MaaS360 Services" page. It has a sub-header "Configure MaaS360 Services" and a message: "Please upload your Apple MDM certificate to enable Mobile Device Management for iOS. MaaS360 requires all customers to use their own Apple MDM certificate for any software demos or trials." There are input fields for "Apple MDM Certificate*", "Certificate Password*", and "Confirm Password*", each with a "Browse..." button. A "Save" button is at the bottom. To the right, there is a section titled "Don't have an MDM Certificate?" with links to "Click here to download a step-by-step guide for instructions." and "Prepare Certificate Signing Request for upload to Apple." At the bottom, a green checkmark indicates "Mobile Device Management for Android is enabled" with a note: "MaaS360 has pre-installed the status required for you to manage your Android devices."

4. On the right hand side of the iOS section, under *Don't have an MDM Certificate?*, click **Prepare Certificate Signing Request**.



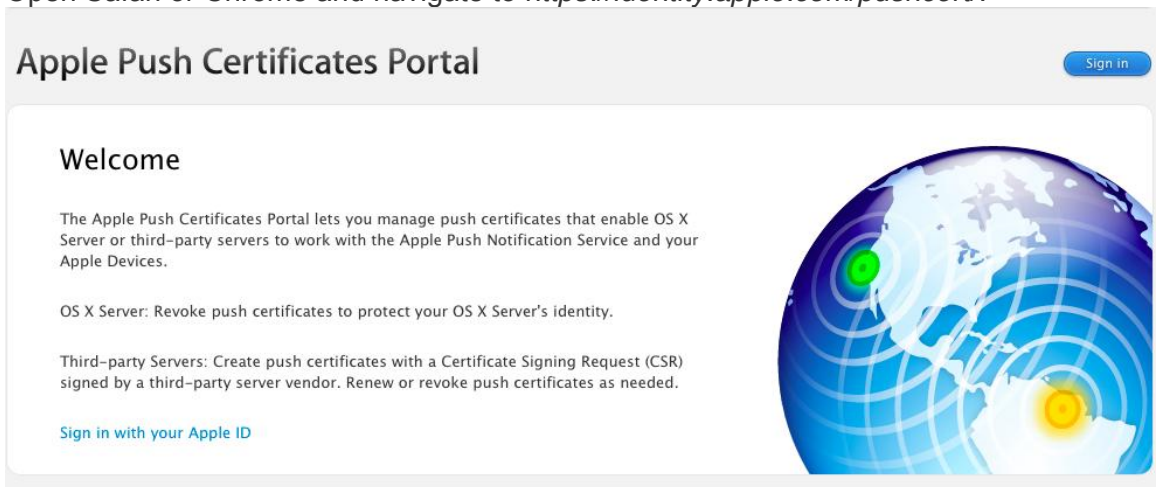
5. Click on the **Browse** button, and select the CSR you created earlier. Then click **Sign CSR**.



6. Click on **Click Here** to download the prepare Certificate Signing Request that is ready to be uploaded to Apple.

Upload prepared CSR to Apple

9. Open Safari or Chrome and navigate to <https://identity.apple.com/pushcert/>.



10. Click **Sign in with your Apple ID**, then enter in your Apple ID and password, and click **Sign in**.

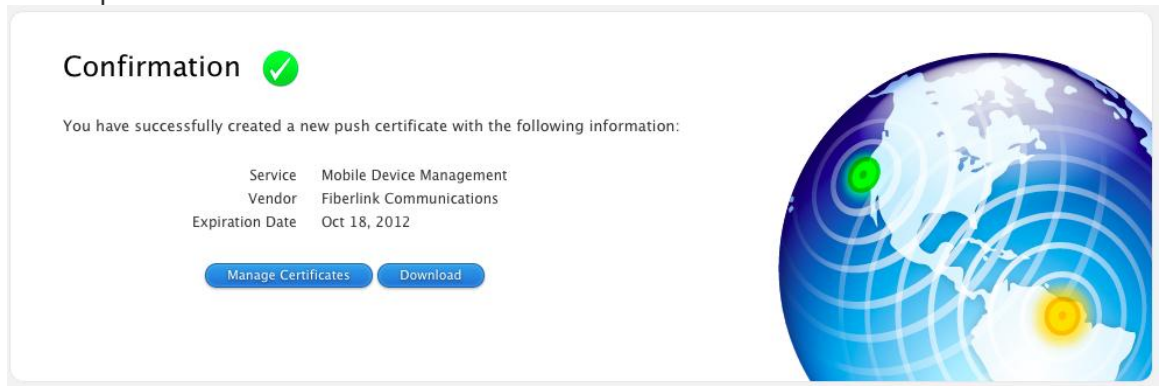


11. Click **Create a Certificate**. You will now need to accept the terms and conditions. If you agree, check the box and click "Accept".



12. Now you will be prompted to upload the file that you downloaded earlier from MaaS360. By default it is named "FiberlinkCSR.txt".
13. Click Choose File and locate the file

14. Click Upload.

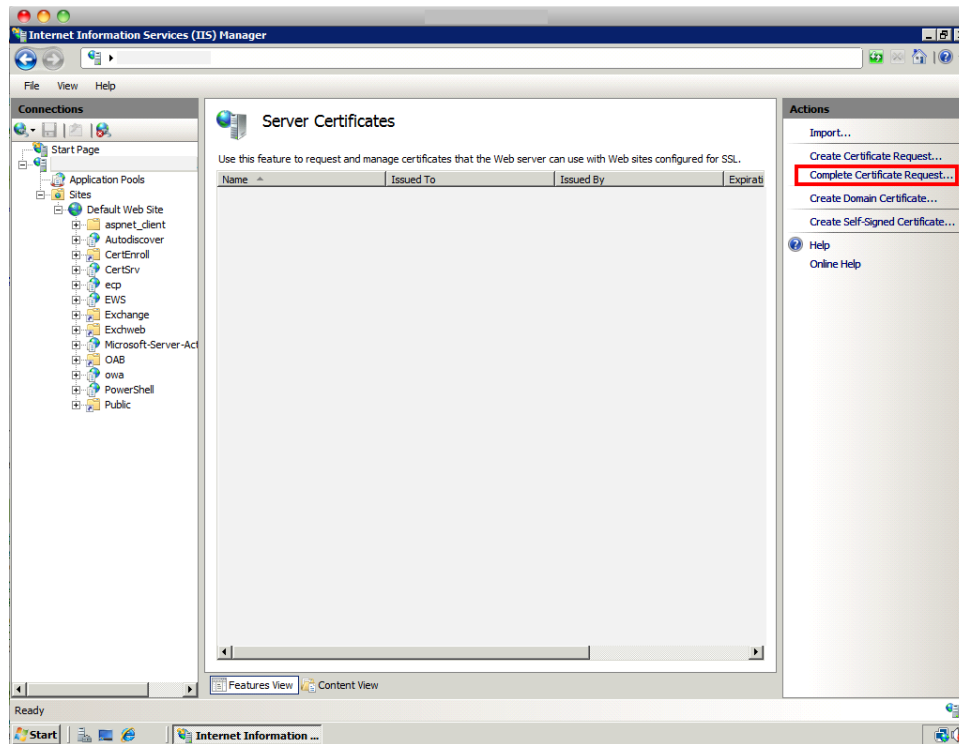


15. After a few seconds, you should see the screen above.

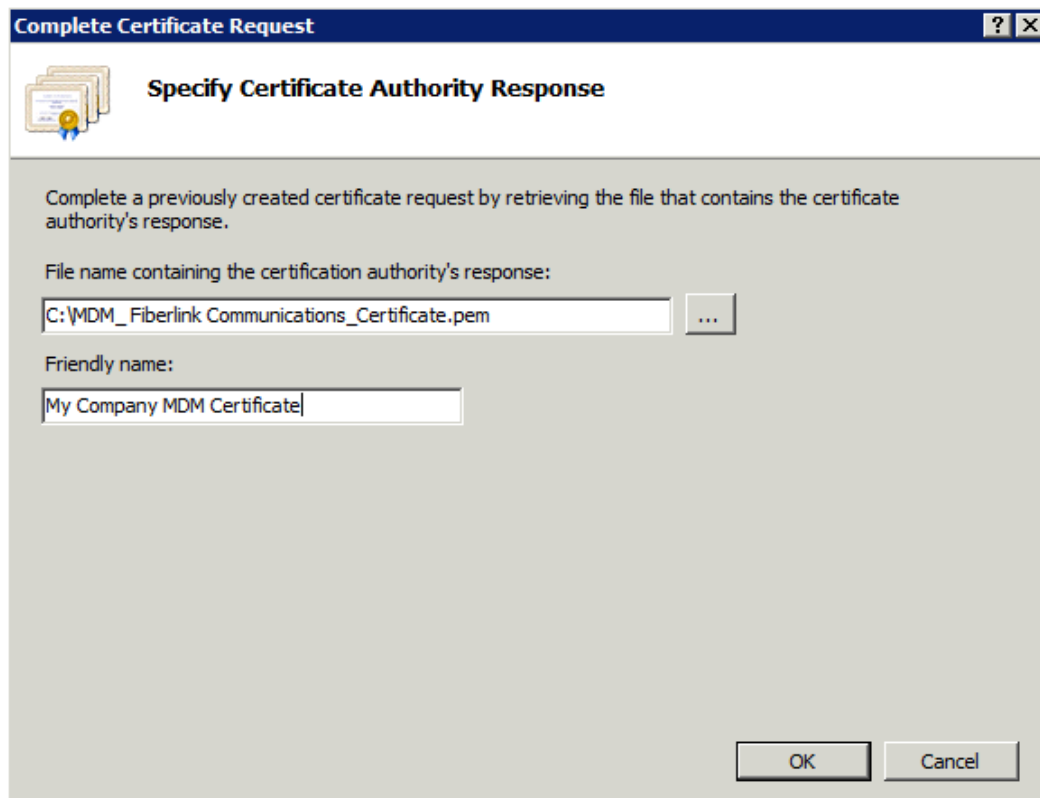
Click "Download". You should now have a file named "MDM_Fiberlink Communications_Certificate.pem".

Complete the CSR Request

1. Return to the Windows server and click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.



2. In the Actions menu, click **Complete Certificate Request**. The Specify Certificate Authority Response page displays.



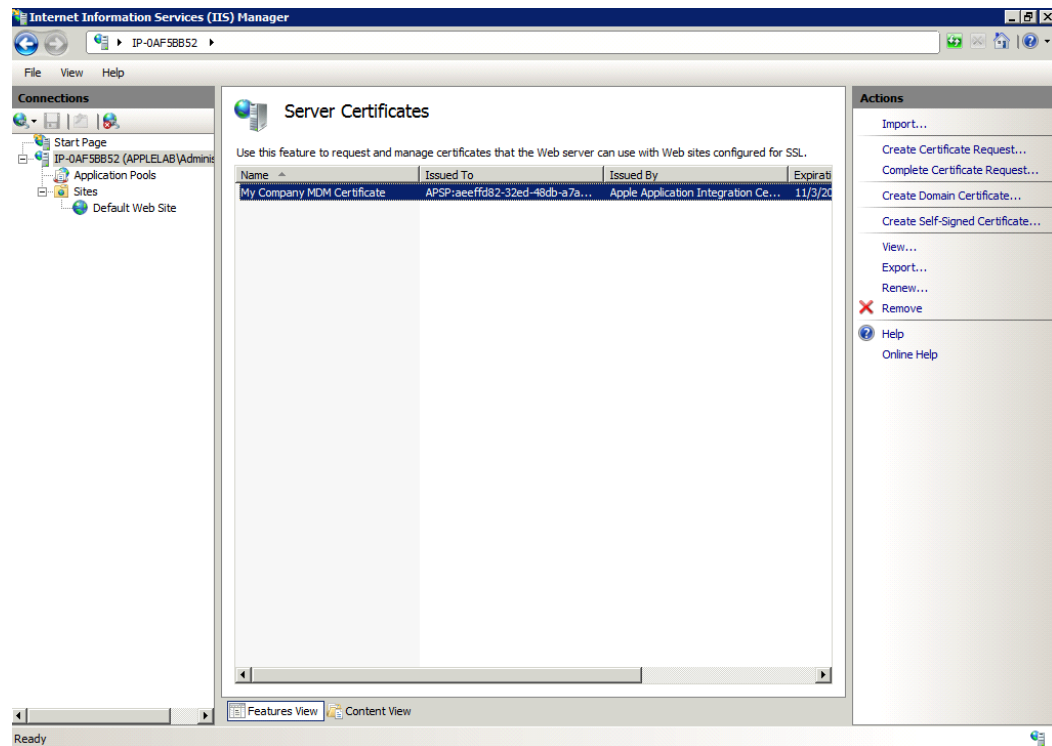
3. Browse to the Apple certificate file, by default **MDM_Fiberlink Communications_Certificate.pem**, on the server and enter a Friendly name that can distinguish the certificate from others. For example, you could name it *My Company MDM Certificate*.

*Note: You may have to change the expected extension to *.* to see the file.*

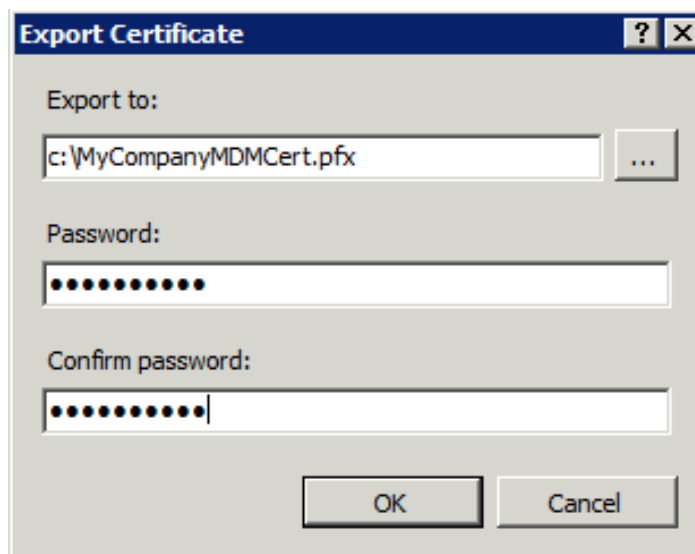
4. Click **OK** to include the certificate in the list of Server Certificates.

Export the APNs Certificate

1. The new certificate now displays on the Server Certificates page.



2. While viewing the Server Certificates page, click the certificate Friendly name to highlight the certificate, and select **Export** on the right menu bar. The Export Certificate dialog opens.



3. Enter a path to save the file in .pfx format. Enter a new password and enter again to confirm. Click **OK** to save the certificate file to your desktop in .pfx format.

Note: If .pfx is not available as a File Format, then you are not exporting the certificate correctly.

You are now ready to use the APNs certificate (*.pfx) and the password that you created to export the certificate. Refer to *Uploading the APNs Certificate to MaaS360 for Mobile Devices*.

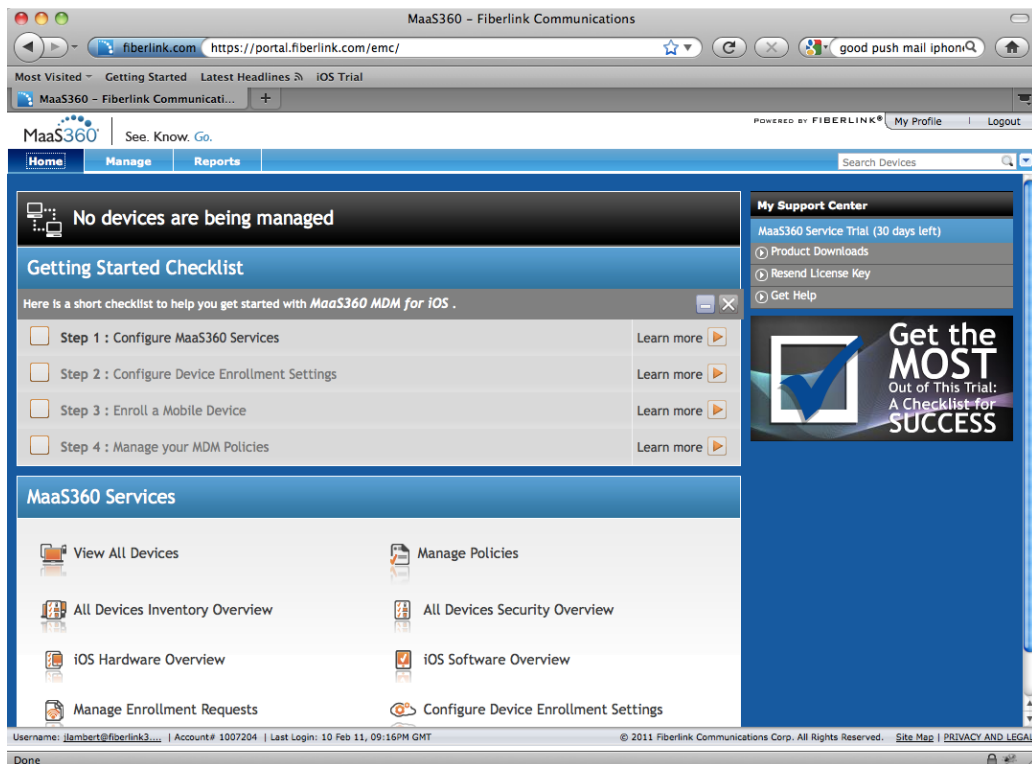
Uploading the APNs Certificate to MaaS360 for Mobile Devices

After you upload the APNs certificate to MaaS360 for Mobile Devices, you will be able to manage your iOS devices through MaaS360. Before you begin, you will need to have the following:

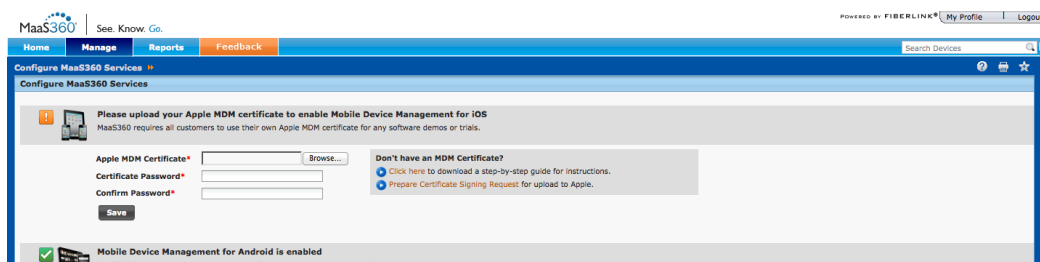
- APNs certificate file in .pfx (Windows) or .p12 (Mac) format (not .cer).
- The password you created when you exported the certificate file.
- MaaS360 for Mobile Devices web console URL, with proper username and password.

Follow these steps to complete the process:

1. Using your browser navigate to the MaaS360 for Mobile Devices console at <https://portal.fiberlink.com/emc/>. The Getting Started Checklist displays. Note at the top of the page the message: “No devices are being managed.” Once you enroll an iOS device, you should be able to see real time information about it.

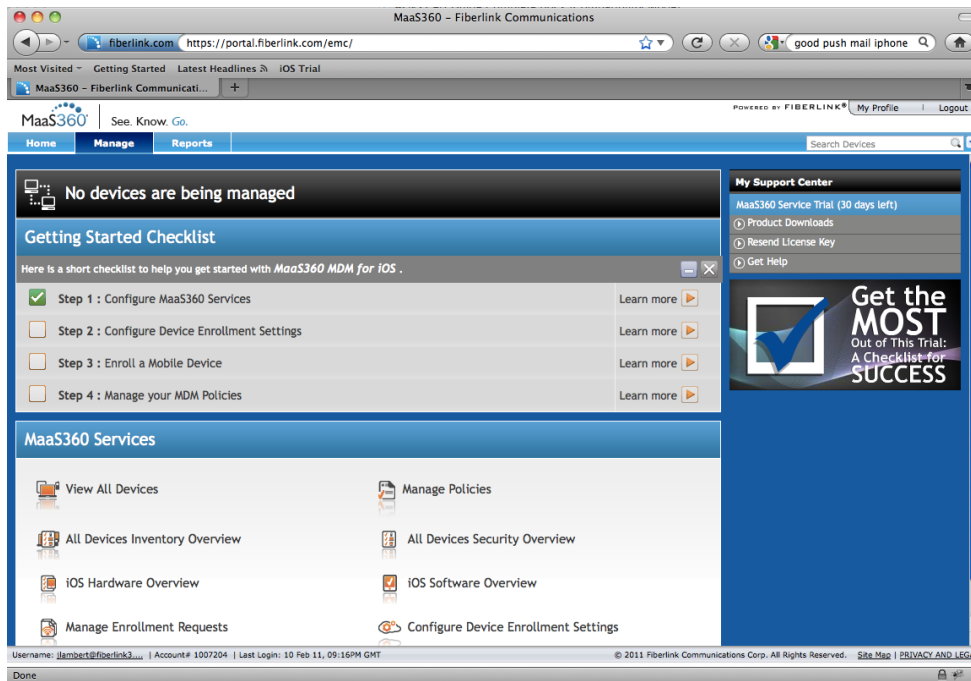


2. Click to place a check mark in the box next to **Step 1: Configure MaaS360 Services**. The Upload Certificate page displays. All fields are required.

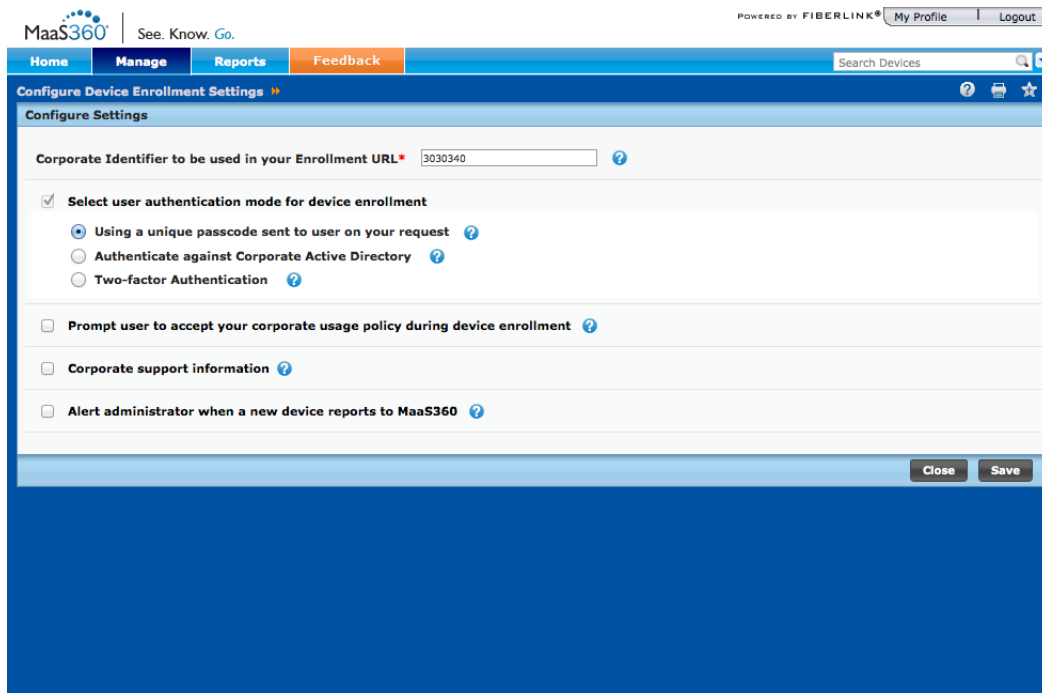


3. Enter the path and name of the **Apple MDM Certificate**, or click the Browse button to locate the path.

4. Enter the **Certificate Password** that you used to export the certificate, and re-enter the Password to confirm.
5. Click **Save**, to upload the file and return to the Getting Started Checklist, showing that Step 1 is now completed.

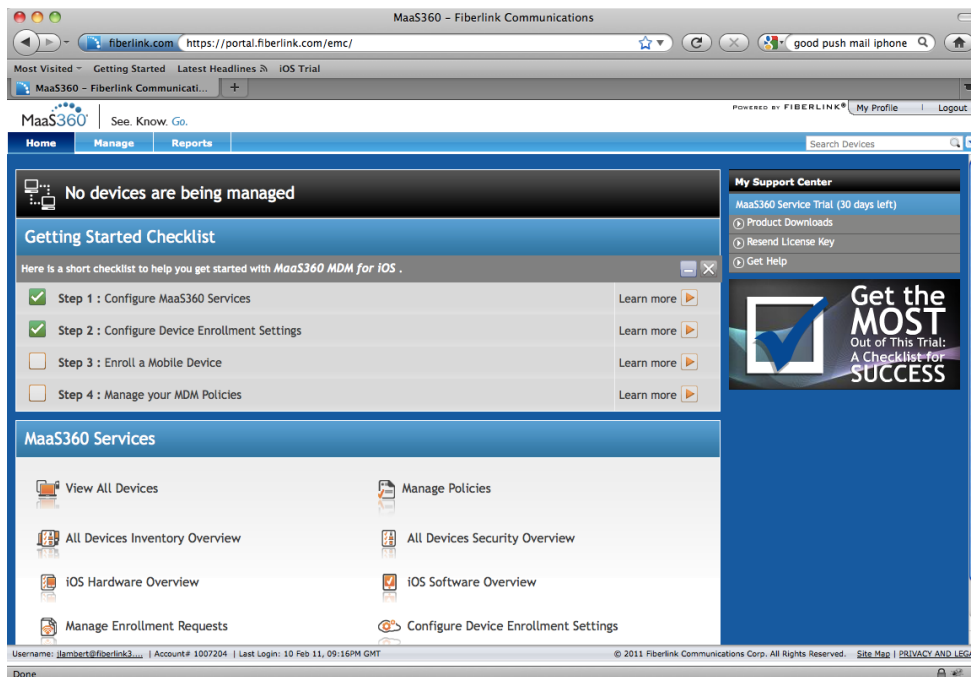


6. Click to place a check mark in the box next to **Step 2: Configure Device Enrollment Settings**. The Configure Settings page displays.

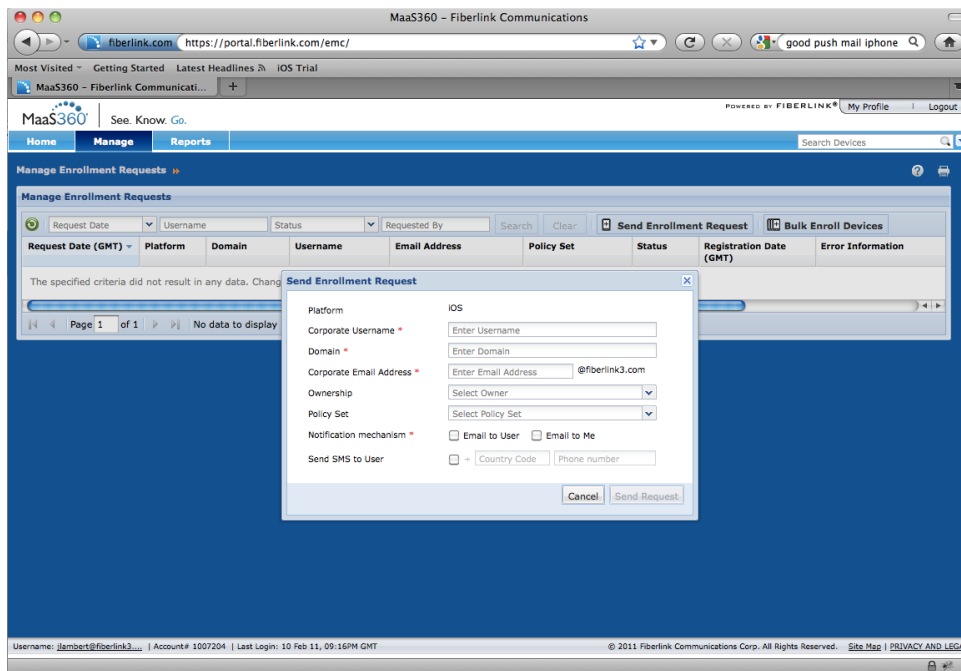


7. Ensure that **Select user authentication mode for device enrollment** is checked, and that the option below that is set at **Using a unique Passcode sent to user on your request**.

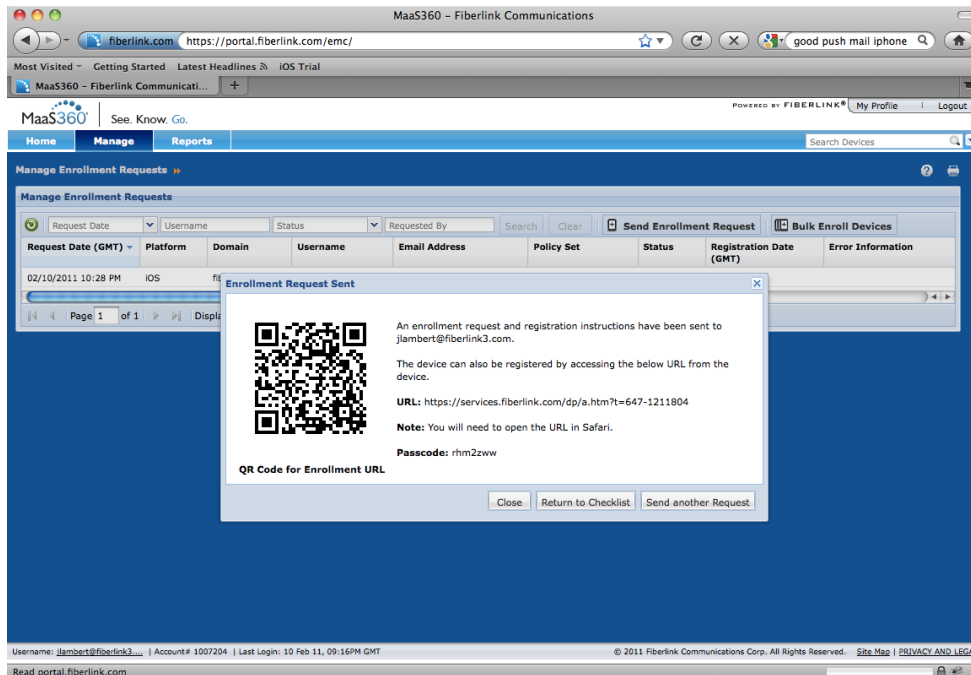
8. Click **Save** to return to the Getting Started Checklist, showing that Step 2 is now completed.



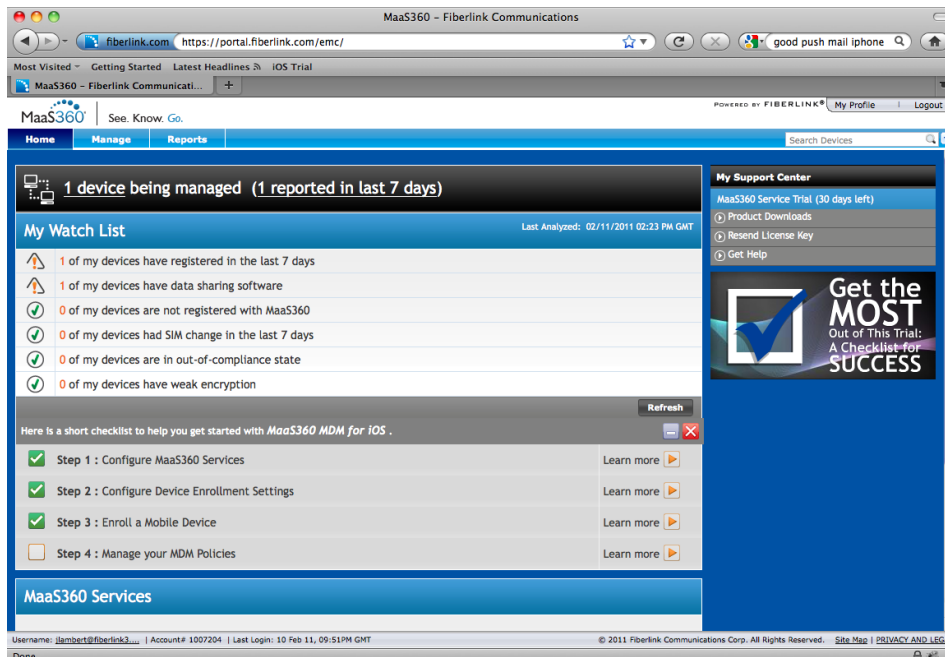
9. Click to place a check mark in the box next to **Step 3: Enroll an Mobile Device**. The Manage Enrollment Requests page displays. You are now ready to enroll a specific iOS device.
10. Enter all required fields for the iOS device, including **Corporate Username**, **Domain**, **Corporate Email Address** and **Notification Mechanism**. The example shows representative entries, along with a possible message you will receive if something is not entered properly.



11. Click **Send Request**. If the information is acceptable, you will receive a confirmation of **Enrollment Request Sent** and the request will be listed with its details. You can also register iOS devices directly from the devices, using the URL indicated by the message.



12. Click **Return to Checklist** to save your changes and return to the Getting Started Checklist, showing that Step 3 is now completed.



You have successfully generated an APNs certificate and uploaded it to the MaaS360 for Mobile Devices web console. You're now ready to manage your iOS devices. You will also see a message above My Watch List showing any devices that are being managed, including devices that were recently enrolled.

Refer to MaaS360 documentation for advanced information on enrolling and managing your iOS devices.