



**TREND MICRO™**  
**Mobile Security**  
Comprehensive security for enterprise handhelds

# **Guide for Generating Apple Push Notification Service Certificate**



# Contents

- Generating and Using APNs Certificate ..... 5
  - Understanding APNs Certificate ..... 6
  - Generating an APNs Certificate ..... 7
    - Initial Steps..... 7
    - Generating an APNs Certificate from a Mac Workstation ..... 8
      - Step 1—Generating a Certificate Signing Request (CSR) ..... 8
      - Step 2— Uploading CSR to your Apple development portal and generate the APNs certificate ..... 9
      - Step 3— Downloading and Installing your APNs Certificate..... 14
    - Generating an APNs Certificate from Windows Server ..... 17
      - Step 1—Generating a Certificate Signing Request (CSR) ..... 17
      - Step 2— Uploading CSR to your Apple development portal and generate the APNs certificate... 19
      - Step 3— Downloading and Installing your APNs certificate ..... 20
- Uploading APNs Certificate to Mobile Security Server ..... 23
  - To upload APNS certificate to Mobile Security:..... 23



## Chapter 1

# Generating and Using APNs Certificate

Installing Trend Micro Mobile Security for Enterprise requires Apple Push Notification service (APNs) certificate to manage iOS devices.

The process includes the following two steps:

1. Acquire an APNs certificate from your Apple development portal
2. Upload APNs certificate to Trend Micro Mobile Security for Enterprise Mobile Device Management (MDM) server

# Understanding APNs Certificate

The Apple Push Notification service (APNs) enables Trend Micro Mobile Security for Enterprise Mobile Device Management (MDM) server to securely communicate to your devices over-the-air (OTA). Each organization needs its own APNs certificate to ensure a secure mechanism for their devices to communicate across Apple's push notification network.

Acquiring an APNs certificate is a partnership directly between your organization and Apple. Trend Micro Mobile Security for Enterprise cannot provide or issue an APNs certificate to your organization.

Trend Micro Mobile Security for Enterprise uses your APNs certificate to send notifications to your devices when the Administrator requests information or manage your iOS devices. Only the notification is sent through the APNs server.

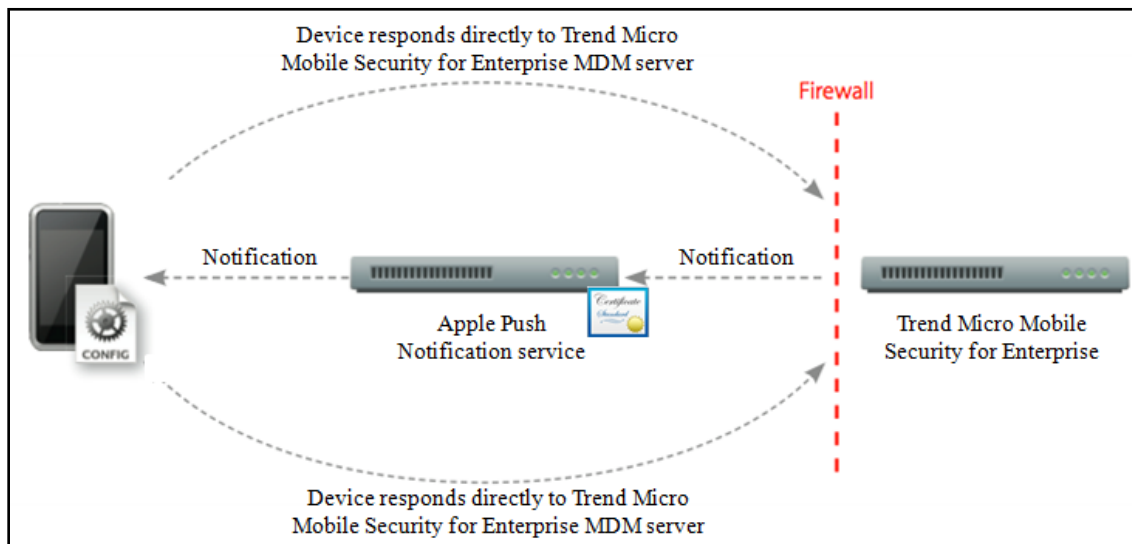


Figure 1 - Notification Process

# Generating an APNs Certificate

This section explains the process of generating Apple Push Notification Service certificate for iOS mobile devices management.

## Initial Steps

The following are the basic steps for Generating APNs certificate:

1. Create a Certificate Signing Request (CSR)
2. Upload the CSR to your Apple Development portal (Apple will sign your certificate)
3. Download the signed certificate from your Apple Development portal and complete the initial CSR request

---

**Note:** Make sure that you have the following before you begin:

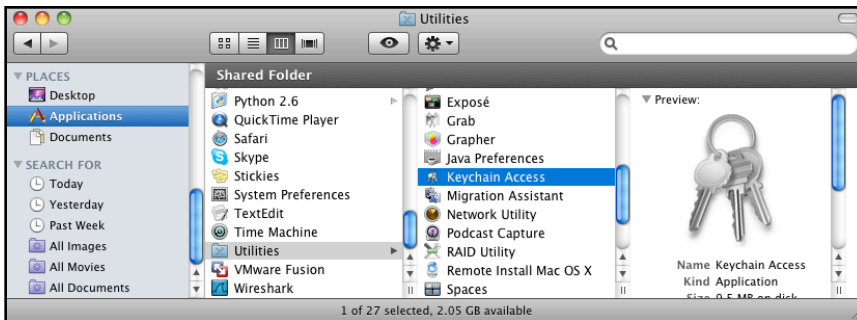
- Apple Enterprise Developer account ([developer.apple.com/programs/ios/enterprise](https://developer.apple.com/programs/ios/enterprise))
  - Your developer account role must be Agent (Admin role will not work)
  - Mac OS X workstation or Windows Server with Administrator permissions
  - Safari or Firefox Web browser
-

# Generating an APNs Certificate from a Mac Workstation

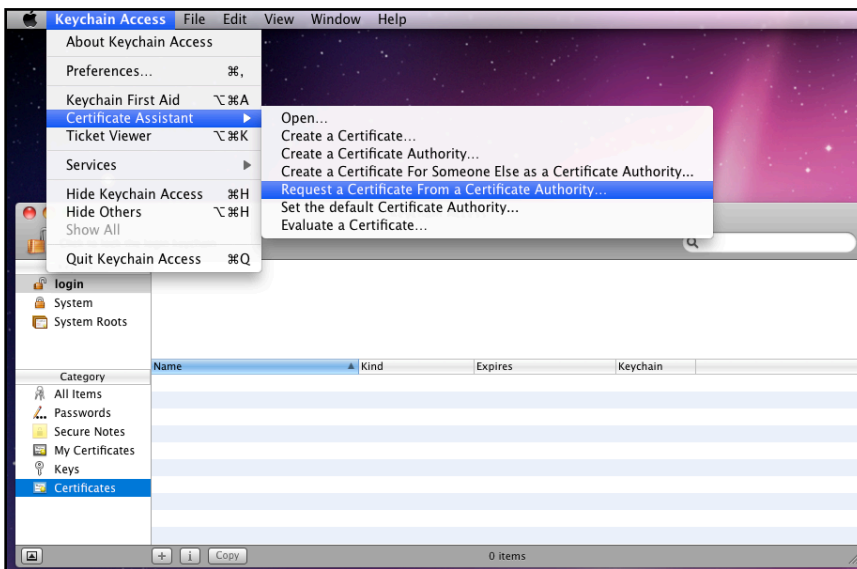
The following steps will guide you to generate an APNs certificate using a Mac OS X workstation. For Windows Server steps you may skip this section.

## Step 1—Generating a Certificate Signing Request (CSR)

1. On your Mac computer, go to **Applications > Utilities > Keychain Access**.

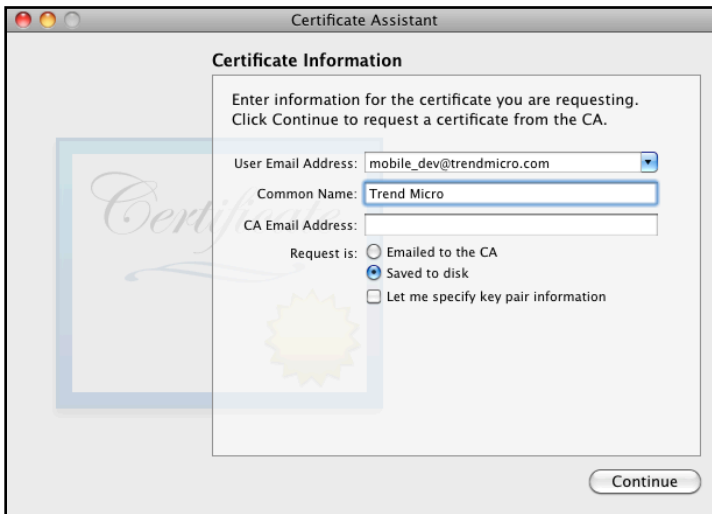


2. On the left pane, select login in the Keychain section, and then select **Certificates** in the Category section.
3. From the top menu bar, select **Keychain Access > Certificate Assistant > Request a Certificate From a Certificate Authority**. The **Certificate Assistant** wizard displays.

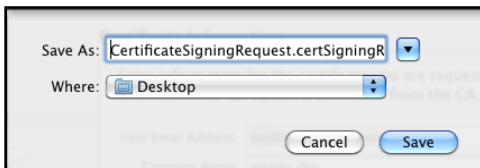


4. Type the email address and registered Apple Developer account name in **User Email Address** and **Common Name** fields.

5. Select **Saved to disk**, and then click **Continue**.

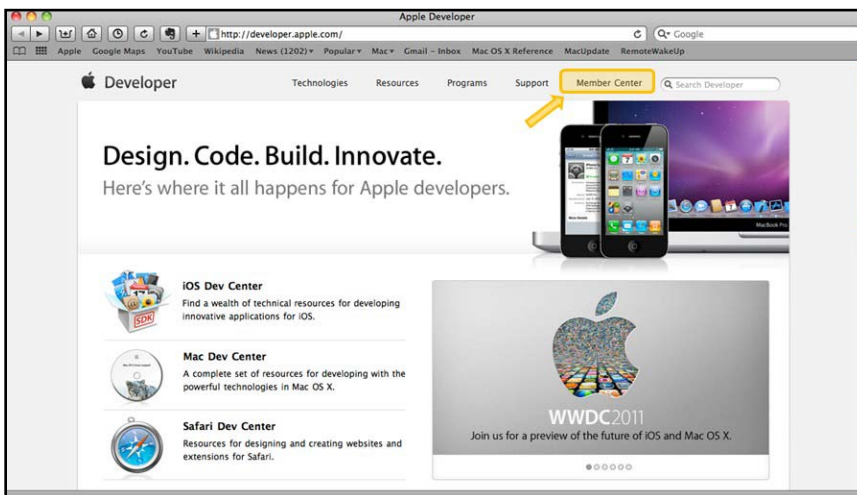


6. Select the location where you want to save the file, and then click **Save**. You have now created a CSR request and are ready to upload it to your Apple development portal.

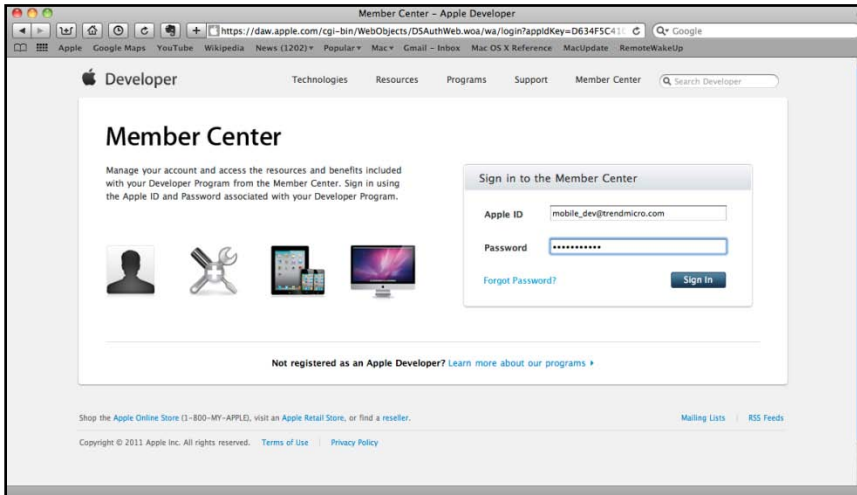


## Step 2— Uploading CSR to your Apple development portal and generate the APNs certificate

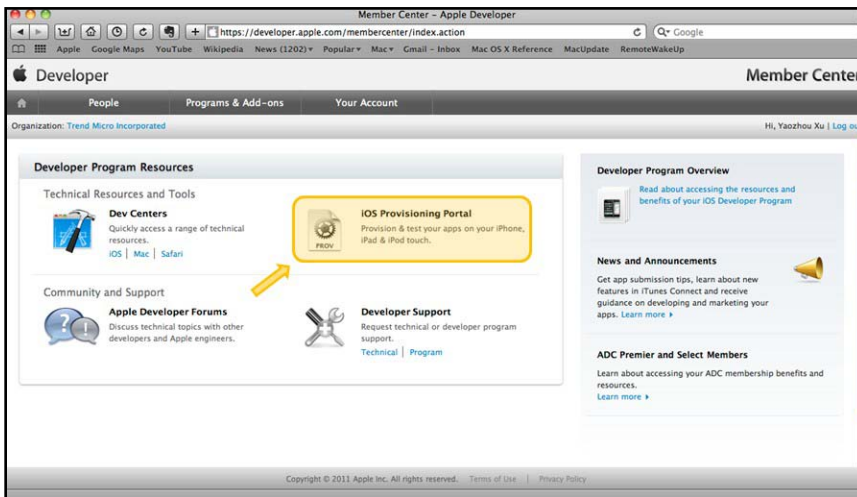
1. On the Web browser, navigate to <https://developer.apple.com/>.
2. Click the **Member Center** link.



3. Sign in with your Apple ID and password.



4. Click iOS Provisioning Portal.

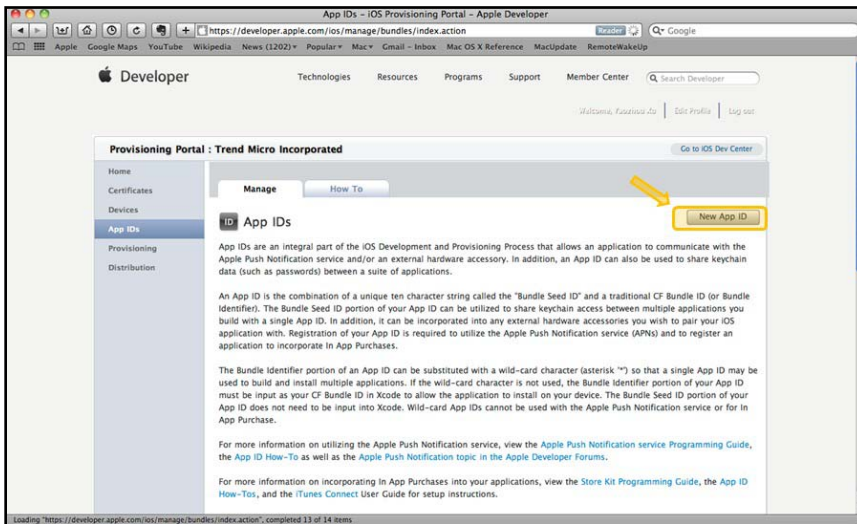


---

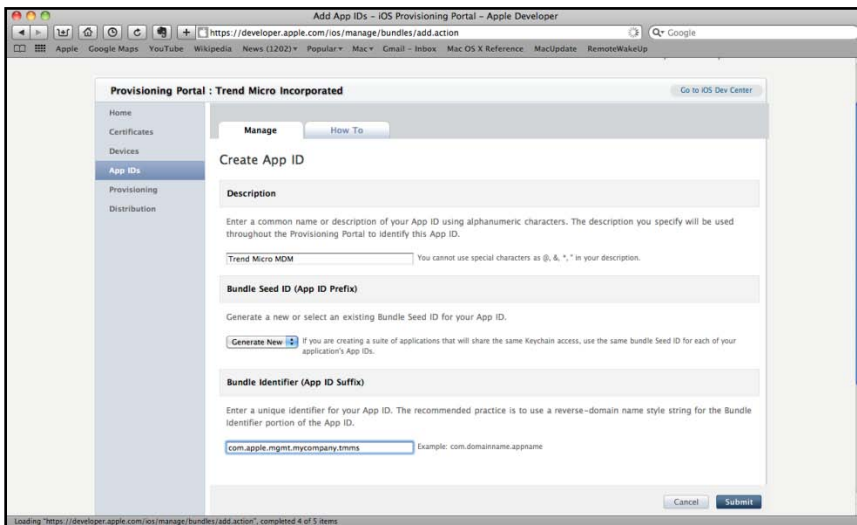
**Tip:** If you do not see the iOS Provisioning Portal, your development account has not been setup for iOS development.

---

- On the left pane, click **App IDs**, and then click **New App ID**.



- Fill in the applicable fields. **The Bundle Identifier (App ID Suffix) notation** field must be **“com.apple.mgmt.mycompany.tmm”** (replace mycompany with your company name).
- Click **Submit**. The App ID that you have just added, appears in the list.



**Note:** Note down The Bundle Identifier (App ID Suffix) notation value. You will need to provide this value to the Trend Micro Mobile Security for Enterprise MDM server.

8. Click **Configure**.

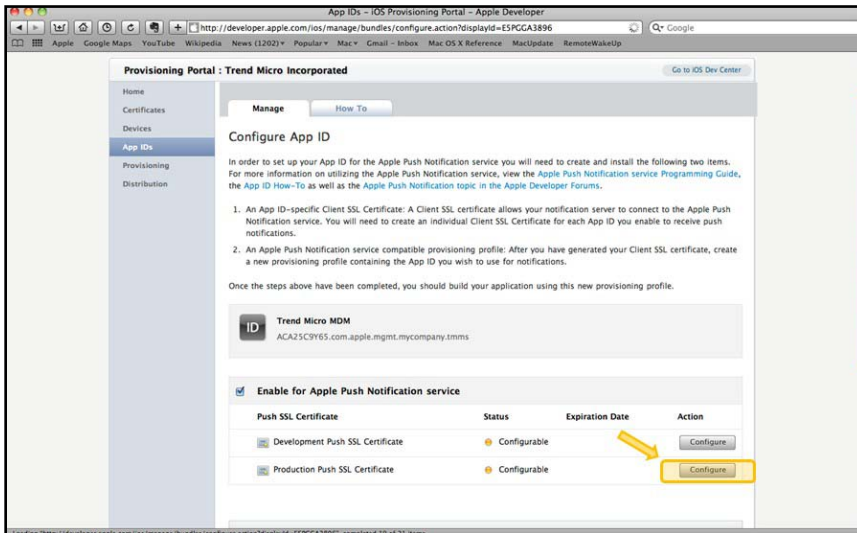


---

**Tip:** If you do not see or cannot click **Configure**, verify that you are signed in with the Agent role.

---

9. Select Enable for Apple Push Notification service, and then click Configure for Production Push SSL Certificate.

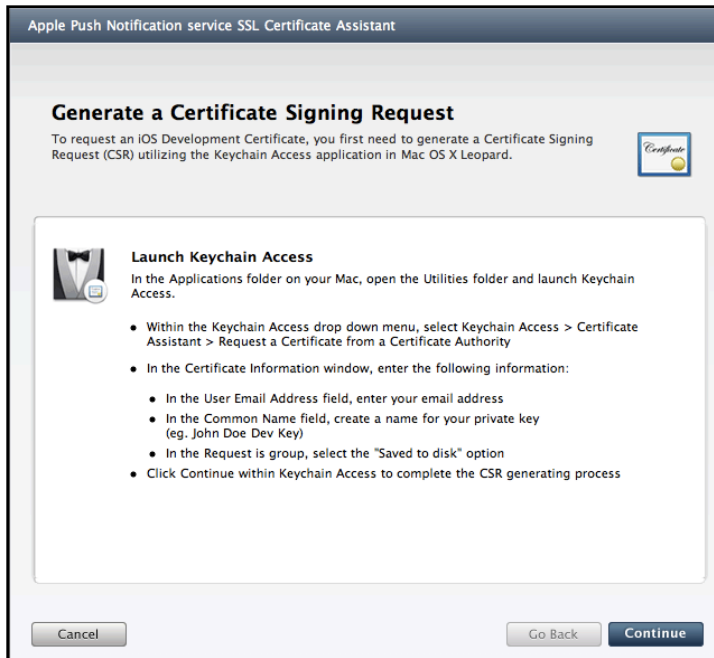


---

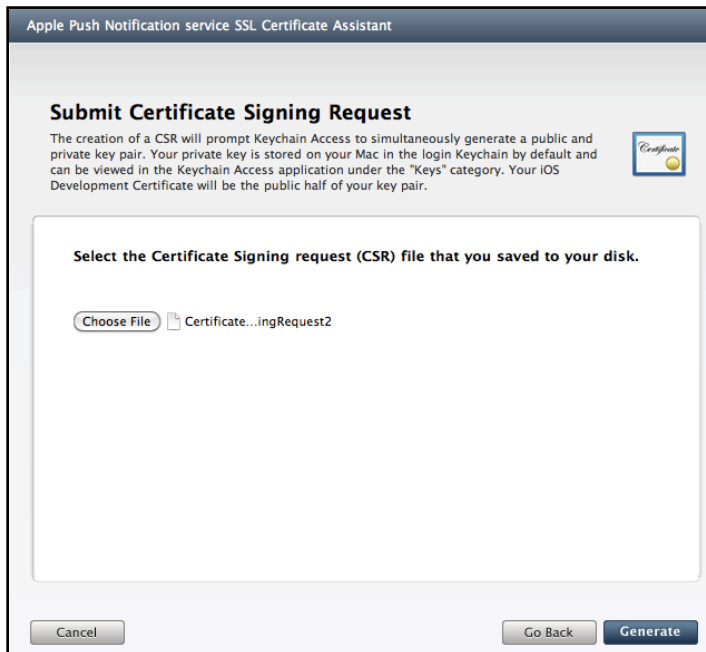
**Tip:** If you are unable to select **Enable for Apple Push Notification service**, try using Safari or Firefox Web browser, and verify that you are signed in with the Agent role.

---

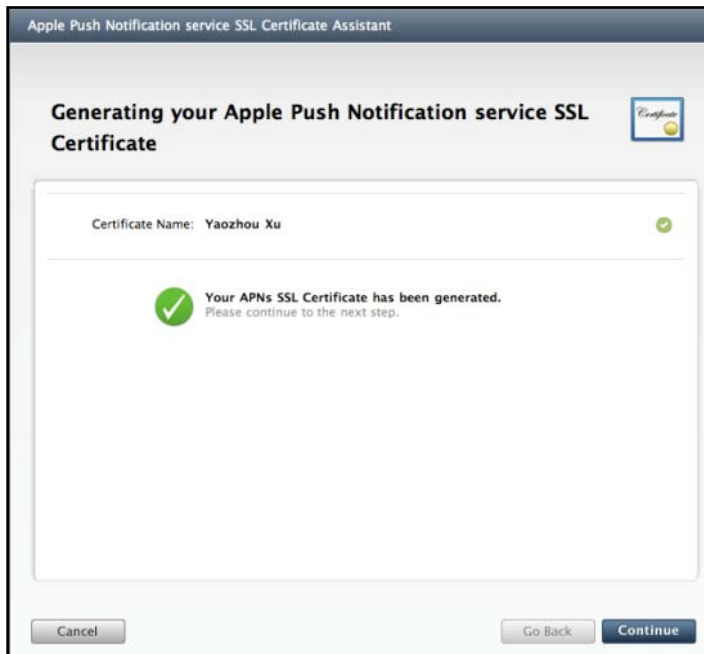
10. **SSL Certificate Assistant** wizard will appear, instructing you to create a Certificate Signing Request (that you have already created in Step 1). Click **Continue**.



11. Click **Choose File** and upload the Certificate Signing Request file that you created in Step 1. (For example, CertificateSigningRequest.certSigningRequest2).
12. Click **Generate**.



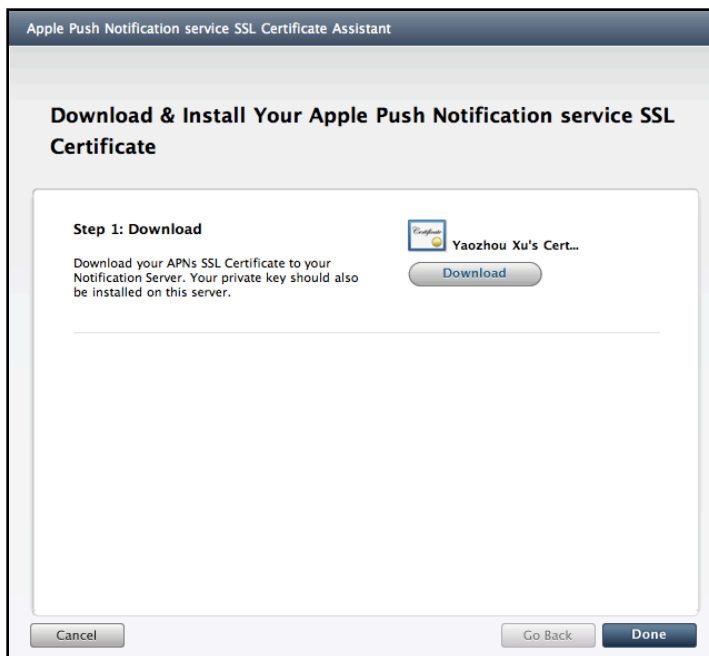
When completed, the following screen will appear:



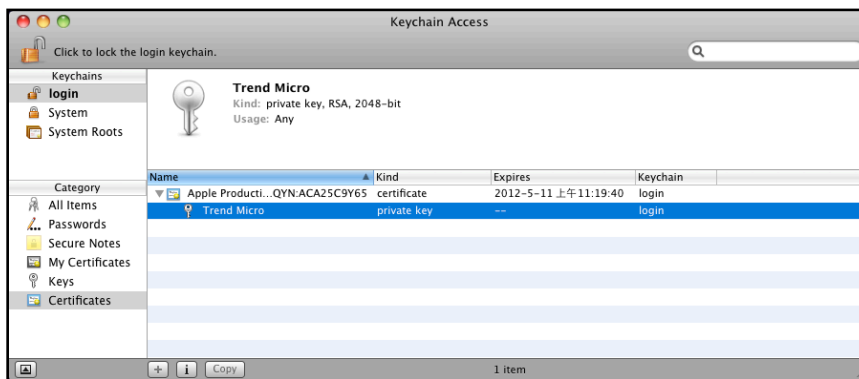
13. Click **Continue** to move to *Step 3— Downloading and Installing your APNs Certificate*.

### Step 3— Downloading and Installing your APNs Certificate

1. Click **Download** to save the .cer file to your computer.

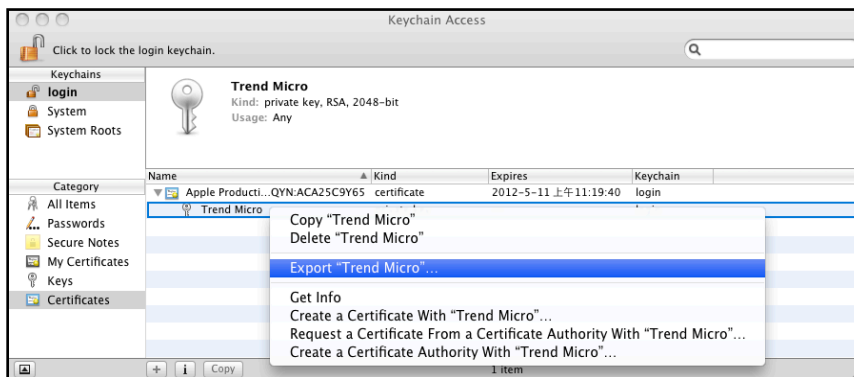


2. Go the location where you downloaded the file, and then double-click the file to automatically uploaded it to Keychain Access and complete the signing request.
3. Go to **Applications > Utilities > Keychain Access**.
4. On the left pane, select **login** in the Keychain section, and then select **Certificates** in the Category section.
5. Verify that your Apple Production Push Services certificate appears on the list, and it has an associate private key beneath it when you expand it. If you can see the certificate, follow the next steps to export the certificate and upload it to the Trend Micro Mobile Security for Enterprise MDM server.

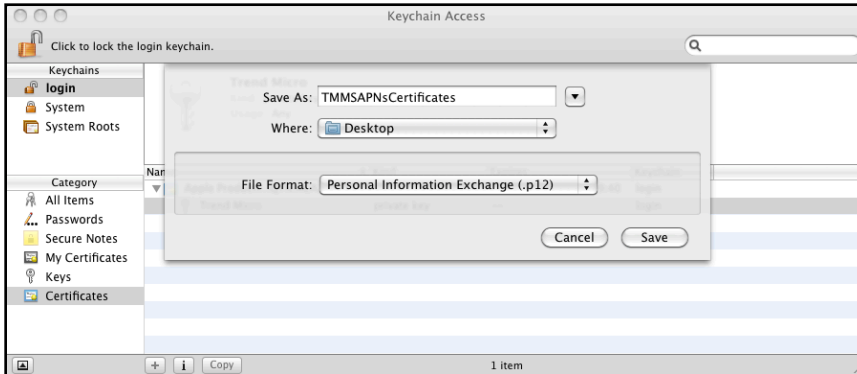


**Tip:** If you do not see your APNs certificate or the private key is not showing, verify you have the **login** keychain selected, the **Certificates** category selected and your certificate key has been expanded as show in the figure. If you still do not see your certificate, repeat all of the steps above.

6. Right-click (or control+click) on the private key and click **Export**.



7. Choose the file name and location where you want to save the file, and then select Personal Information Exchange (.p12) file format.



---

**Tip:** If you only have the option to save as a .cer file rather than a .p12 , then you are not correctly exporting the certificate. Make sure you selected the **private key** to export in the last step, and your file format is **Personal Information Exchange (.p12)**.

---

8. Click **Save**.
9. Choose a password for exporting, and then click **OK**.



---

**Tip:** Make sure to remember the password, or keep it in the secure place. The password will be required when uploading the certificate to Trend Micro Mobile Security for Enterprise MDM server.

---

After completing all these steps, you should have the following items:

- APNs certificate (.p12 format, not .cer format)
- The password that you set when exporting the certificate

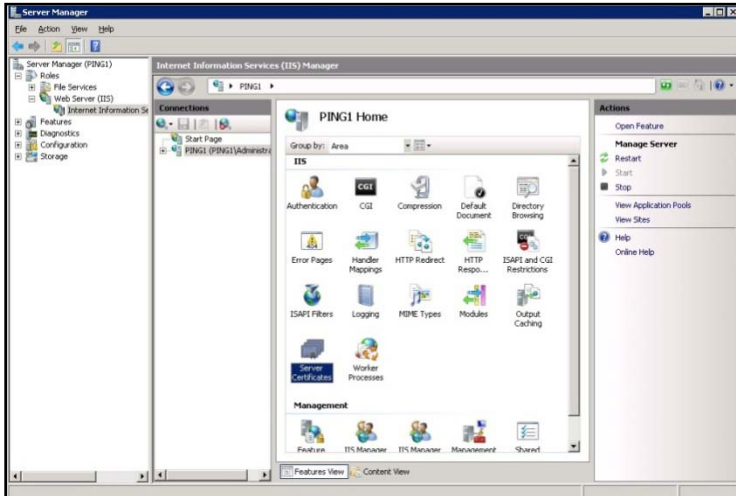
You are now ready to upload your certificate to Trend Micro Mobile Security server.

## Generating an APNs Certificate from Windows Server

The following steps will guide you to generate an APNs certificate from a Windows Server. If you have already generated your certificate from a Mac OS X workstation, you can skip this section and upload your certificate to Trend Micro Mobile Security for Enterprise MDM server.

### Step 1—Generating a Certificate Signing Request (CSR)

1. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**, and select the server name.
2. Double-click **Server Certificates**.

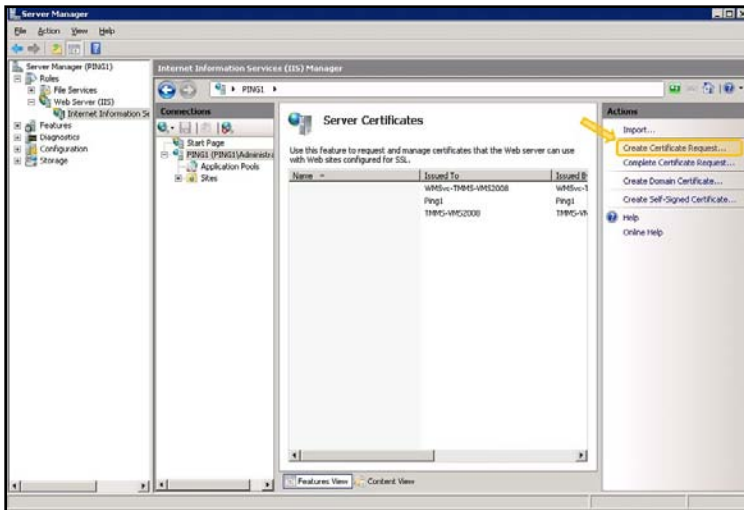


---

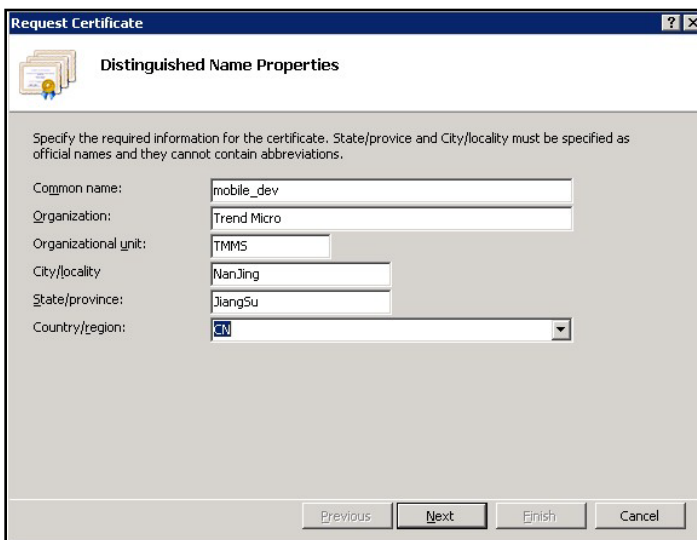
**Note:** The version of IIS server is 7.0 in this document.

---

- From the **Actions** pane on the right, click **Create Certificate Request**. The Request Certificate wizard appears.

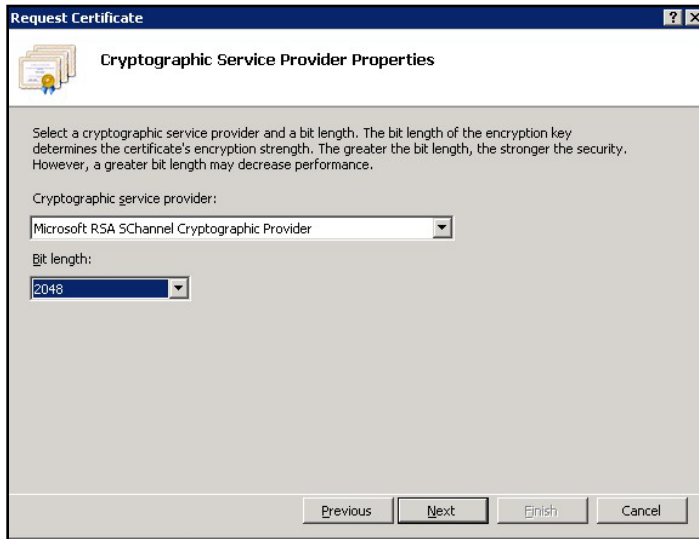


- In the **Distinguished Name Properties** window, type the following:
  - Common Name**—the name associated with your Apple Developer account
  - Organization**—the legally registered name of your organization/company
  - Organizational unit**—the name of your department within the organization
  - City/locality**—the city in which your organization is located
  - State/province**—the state or province in which your organization is located
  - Country/region**—the country or region in which your organization is located

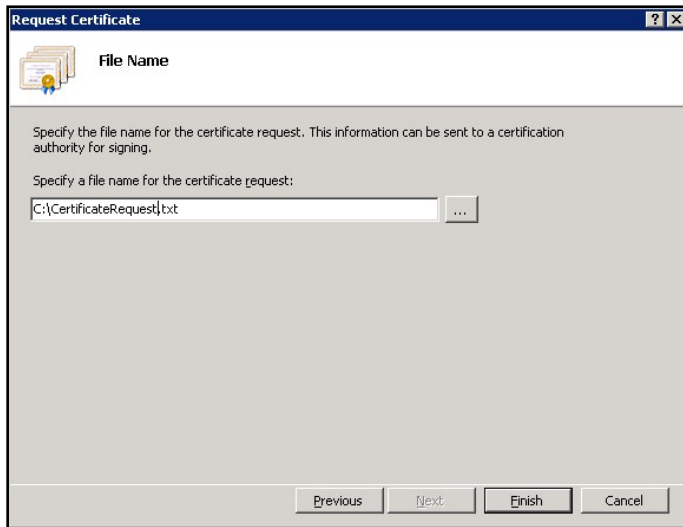


- Click **Next**. Cryptographic Service Provider Properties window appears.

6. Select **Microsoft RSA SChannel Cryptographic Provider** in the **Cryptographic service provider** field and **2048** in the **Bit length** field, and then click **Next**.



7. Select a location where you want to save the certificate request file. Make sure to remember the filename and the location where you save the file.



8. Click **Finish**. You have now created a CSR request and are ready to upload it to your Apple development portal.

## Step 2— Uploading CSR to your Apple development portal and generate the APNs certificate

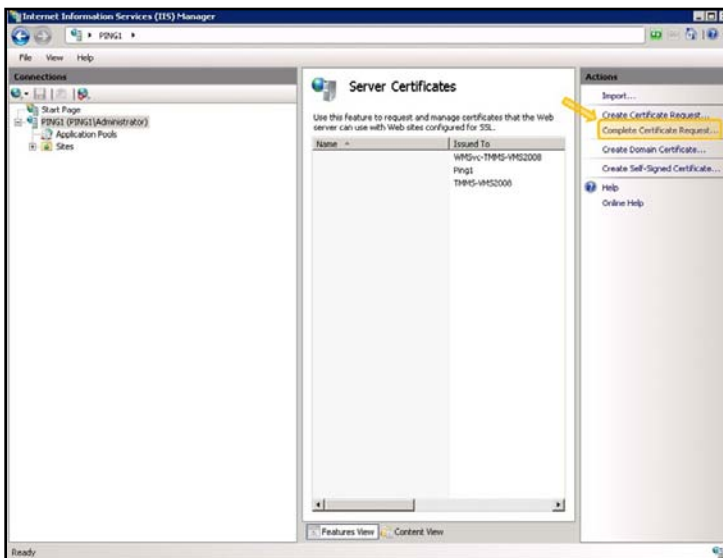
Refer to [Step 2— Uploading CSR to your Apple development portal and generate the APNs certificate](#) for Map OS X for the procedure.

### Step 3— Downloading and Installing your APNs certificate

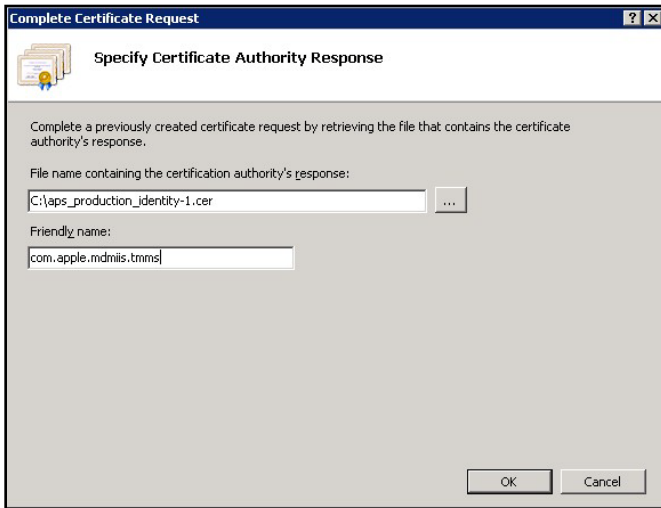
1. Click **Download** to save the .cer file to your computer.



2. Copy the .cer certificate file to the same Windows Server computer where you created the certificate request file.
3. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**, select the server name, and then double-click Server Certificates
4. From the **Actions** pane on the right, click **Complete Certificate Request**. The Complete Certificate Request wizard appears.

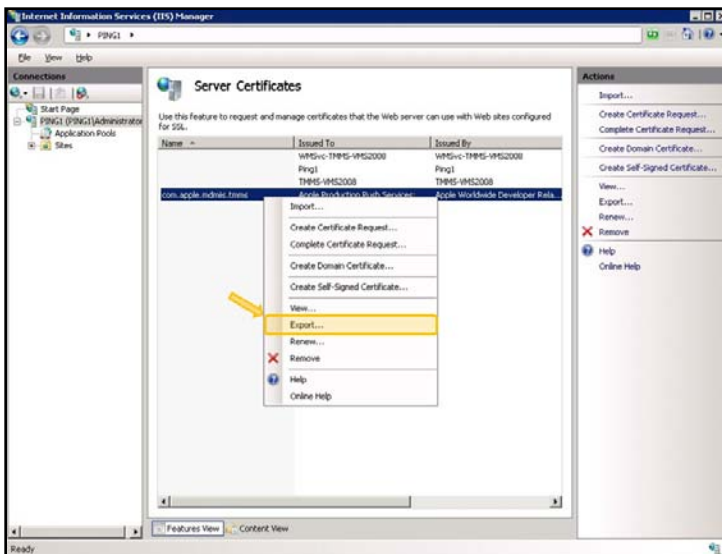


5. Select the .cer certificate file that you downloaded from the Apple Developer Portal, and type **Trend Micro Mobile Security for Enterprise MDM APNs** in the **Friendly name** field.

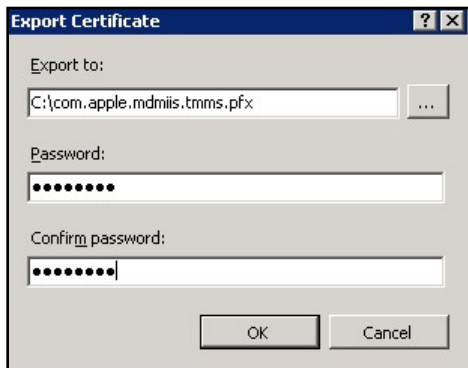


**Tip:** The friendly name is not a part of the certificate itself, but is used by the server administrator to easily distinguish the certificate.

6. Select **OK**. The certificate will be installed on the server.
7. Verify that your Apple Production Push Services certificate appears on the **Server Certificates** list. If you can see the certificate, follow the next steps to export the certificate and upload it to the Trend Micro Mobile Security for Enterprise MDM server.
8. Right-click on the certificate in the **Server Certificates** list, and then click **Export**.



9. Select the location where you want to save the file, choose a password for exporting, and then click **OK**.



---

**Tip:** If you only have the option to save as a .cer file rather than a .pfx, then you are not correctly exporting the certificate. Make sure you selected the correct file to export.

---

---

**Note:** Make sure to remember the password, or keep it in the secure place. The password will be required when uploading the certificate to Trend Micro Mobile Security for Enterprise MDM server.

---

After completing all these steps, you should have the following items:

- APNs certificate (.pfx format, not .cer format)
- The **password** that you set when exporting the certificate

You are now ready to upload your certificate to Trend Micro Mobile Security server.

# Uploading APNs Certificate to Mobile Security Server

This section explains the process of uploading Apple Push Notification Service (APNS) certificate to Trend Micro Mobile Security for Enterprise server to start managing iOS devices.

---

**Note:** Make sure that you have the following before you begin:

- APNs certificate file (the **.pfx** or **.p12** format, not the **.cer** format)
  - The **password** that you had set when exporting the certificate
  - The administrator **account** of Trend Micro Mobile Security for Enterprise MDM server
- 

## To upload APNS certificate to Mobile Security:

1. Open Internet Explorer, and log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Do one of the following:
  - Click **Administration > Certificate Management**, click **Add**, select the Apple Push Notification Server certificate from the hard disk, and then click **Save**.



- Click **Administration** > **Policy Server Settings**, click **iOS Settings** tab, and then select the Apple Push Notification Server certificate from the hard disk in the **Certificate** field, and then click **Save**.

The screenshot shows the 'Policy Server Settings' web interface. At the top, there are tabs for 'Summary', 'Device Management', 'Updates', 'Logs', 'Notification', and 'Administration'. Below these is the 'Policy Server Settings' header with a 'Help' icon. The 'iOS Settings' tab is selected. Underneath, there are sub-tabs for 'Common Settings', 'iOS Settings', and 'BlackBerry Settings'. The 'Simple Certificate Enrollment Protocol (SCEP) Settings' section contains the following fields:

- SCEP user URL: http://10.64.40.238/certsrv/mscep/
- SCEP admin URL: http://10.64.40.238/certsrv/mscep/
- User account: administrator
- User password: [masked]
- Certificate name: enrollment
- Subject: O=Trend, CN=Enroll

The 'Apple Push Notification service (APNs) Settings' section is circled in red and contains:

- Certificate type: Production (selected) / Development
- Certificate: Apple Production IOS Push Services: Q64GK8FQY
- APNs name: com.apple.mgmt.trend.mdm.internalbeta

The 'Profile Signing Credential' section contains:

- Profile Signing Credential: Apple Production IOS Push Services: Q64GK8FQY

At the bottom, there are 'Save' and 'Cancel' buttons.

After completing these steps, you can now manage your iOS mobile devices. Refer to the [Installation and Deployment Guide](#) and [Administrator's Guide](#) for the detailed installation and management procedures.