APNs Certificate Request Guide

- APNs Certificate Request Guide
  - Renew an APNs Certificate
Overview

This document describes how to setup and create an APNs (Apple Push Notification service) certificate from Apple for use with Zenprise Device Manager as described in the iOS Mobile Device Management (MDM) guidelines.

This document shows you how to generate a certificate signing request (CSR) for submission to Apple on either a Windows server using Microsoft IIS or on a Mac computer (one or the other). Optionally, you can use OpenSSL to generate the signing request as well.

**NOTE:** The APNs certificate from Apple enables mobile device management via the Apple Push Network. If you accidentally or intentionally revoked the certificate, you will lose the ability to manage your devices.

Table of Contents

1. Overview
2. Table of Contents
3. Steps to Request an APNs Certificate
   3.1.1.1. * From Apple: MDM Push Certificate Migration Information
   3.1.1.2. What you need to do
   3.1.1.3. Creating MDM push certificates
4. Generate a Certificate Signing Request with Microsoft IIS
5. Generate a CSR with Mac OS X
6. Submit Newly Created CSR to Zenprise for Signing
7. Submit CSR to Apple
8. Generate a p12 APNs Certificate Using Microsoft IIS
   8.1. Step 1: Complete the certificate request in Microsoft IIS
   8.2. Step 2: Export the certificate as a .pfx (p12) certificate
8.3. **Step 3: Install Zenprise Device Manager and import the APNs certificate**

9. **Generate an APNs Certificate on Mac OS X**

10. **Import (or Replace) an APNs Certificate**

11. **Upload APNs to Zencloud (Zencloud Users Only)**

12. **Alternate Option - Generating APNs Using OpenSSL**

   12.1. **Generate a Certificate Signing Request with OpenSSL**

   12.2. **Generate a p12 APNs Certificate Using OpenSSL**

      12.2.1. **Step 1: Create a p12 certificate**

      12.2.2. **Step 2: Install the APNs Certificate on Device Manager**

12.3. **Troubleshooting**

   12.3.1. **Certificate Installation Error**

      12.3.1.1. **Problem**

      12.3.1.2. **Cause**

      12.3.1.3. **Solution**

---

**Steps to Request an APNs Certificate**

The table below outlines the steps required to request an APNs certificate from Apple for mobile device management:

<table>
<thead>
<tr>
<th>Steps</th>
<th>APNs Certificate Request Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generate a Certificate Signing Request (CSR) with Microsoft IIS (.txt)</td>
</tr>
<tr>
<td>2</td>
<td>Submit CSR to Zenprise for signing</td>
</tr>
<tr>
<td>3</td>
<td>Zenprise signs the CSR with its MDM signing certificate (.plist)</td>
</tr>
<tr>
<td>4</td>
<td>Submit the signed CSR to Apple</td>
</tr>
<tr>
<td>5</td>
<td>Download the APNs certificate from Apple (.pem)</td>
</tr>
<tr>
<td>6</td>
<td>Export the APNs certificate as a p12 certificate (.pfx or .p12)</td>
</tr>
</tbody>
</table>
* From Apple: MDM Push Certificate Migration Information

MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificates Portal. This will impact the creation of new MDM push certificates and the renewal, revocation and downloading of existing MDM push certificates. This does not impact other (non-MDM) APNs certificates.

What you need to do

If your MDM push certificate was created in the iOS Developer Enterprise Program:

- It has been migrated for you automatically.
- You can renew it here in the Apple Push Certificates Portal without impacting your users (and the topic will not change).
- However, you still need to use the iOS Developer Enterprise Program to revoke or download a pre-existing cert

If none of your MDM push certificates are near expiration, no action is needed at this time. If you do have an MDM push certificate that is approaching expiration, contact your MDM solution provider, then have your iOS Developer Program Agent log in to the Apple Push Certificates Portal with their Apple ID.

Creating MDM push certificates

All new MDM push certificates must be created in the Apple Push Certificates Portal.

To create a new MDM push certificate, contact your MDM solution provider, then visit Apple Push Certificates Portal and login with a valid Apple ID. The iOS Developer Enterprise Program will no longer allow the creation of an App ID with a Bundle Identifier (APNs topic) that contains com.apple.mgmt.*

Generate a Certificate Signing Request with Microsoft IIS

The first step for customers is to create a certificate signing request. On Windows 2008 R2 Server, a CSR can be generated from any Internet Information Server (IIS) using the following steps.

1. Open Microsoft IIS.

2. Double-click the **Server Certificates** icon for IIS.
3. The Server Certificates window will open. Click **Create Certificate Request**.

4. Fill in the appropriate Distinguished Name (DN) information and click **Next**.
5. Select "Microsoft RSA SChannel Cryptographic Provider" for the Cryptographic Service Provider and "2048" for bit length. Click Next.

6. Enter a filename and specify a location to save the CSR. Click Finish.
Generate a CSR with Mac OS X

1. On a Macintosh computer running Mac OS X start the Keychain Access application located under the Utility folder inside the Applications folder.

2. Open the Keychain Access menu and choose Preferences. On the Certificates tab, change the options for OCSP and CRL to Off. Close the Preferences window.

3. Open the Keychain Access menu and choose Request a Certificate From a Certificate Authority... from the Certificate Assistant extended menu.

4. The Certificate Assistant will now ask you to enter information to start your CSR. Enter your desired Email Address, Common Name, choose the Saved to disk option and check the box to Let me specify key pair information. The email address and common name can be that of the individual or a role account responsible for the management of certificates.

5. Click Continue to proceed.

6. Enter a name for your certificate signing request (CSR) file and save it to a location that you can easily retrieve the certificate request file. Click Save.

7. The next screen specifies the key pair information. Choose the Key Size of 2048 bits and the RSA algorithm. Click Continue.

8. The generated and saved CSR file is now ready for upload when stepping through the next part of the Apple APNs certificate request process in Section 4. Click Done when the assistant completes the CSR process.

Submit Newly Created CSR to Zenprise for Signing

Before you can submit the certificate to Apple, you need to submit the newly created CSR to your Zenprise sales representative (or, to support@zenprise.com) so we can sign it for use with ZDM. The signed file will come in the .plist format.

1. Email the CSR file to your Zenprise account team.

2. Zenprise will prepare an MDM signed CSR and return it to you as a .plist file.
Submit CSR to Apple

After receiving your CSR from Zenprise, you must submit it to Apple to obtain an APNs certificate.

1. Go to https://identity.apple.com/pushcert

   Note: It has been reported that there are problems logging into the Apple Push Portal. A workaround for this issue is to login to the Apple Developer Portal (http://developer.apple.com/devcenter/ios/index.action) before going to the identity.apple.com link above. For some reason, this appears to circumvent some of the problems with the push portal.

2. Click on Create a Certificate.

3. If this is the first time you are creating a certificate with Apple, select the 'I have read and agree to these terms and conditions' check box and click Accept.

4. Click on Choose File to upload your CSR.

5. Click on Upload.

6. You should receive a confirmation message upon success as shown below:
1. Click on **Download** to retrieve your MDM (**.pem**) certificate.

   **Note:** If you are using Internet Explorer and the file extension is missing, click Cancel twice, and then download from the next window.

---

### Generate a p12 APNs Certificate Using Microsoft IIS

The following steps outline how to use the Apple issued MDM certificate with Zenprise.

**Step 1:** Complete the certificate request in Microsoft IIS

**Step 2:** Export the certificate as a **.pfx** (p12) certificate

**Step 3:** Install Zenprise Device Manager and import the APNs certificate

---

### Step 1: Complete the certificate request in Microsoft IIS

1. Open Microsoft IIS.

2. Click on the **Server Certificates** icon.
3. The Server Certificates window will open. Click on **Complete Certificate Request**.

4. Browse to the Certificate.pem file from Apple. Enter a "**Friendly Name**" for the certificate. Click **OK**.
Step 2: Export the certificate as a .pfx (p12) certificate

1. Click on the certificate that you just completed in Step 1 above.
2. Click Export.
3. Specify a location and filename for the .pfx (p12) certificate and a password. Click OK.

**NOTE:** You will need the password for the certificate in the installation of Device Manager.
4. Copy the *.pfx certificate to the server that Device Manager will be installed on.

**Step 3: Install Zenprise Device Manager and import the APNs certificate**

To install Device Manager refer to the Zenprise Device Manager Installation Guide.

**Generate an APNs Certificate on Mac OS X**

1. Locate the Production identity (.pem) certificate downloaded from the iOS Provisioning Portal. Double-click the certificate file to import it into the Keychain. If prompted to add certificate to a specific keychain simply keep the default ‘login’ keychain selected and click OK.

2. The newly added certificate will appear in your list of certificates. Select the newly imported certificate and control-click or choose Export from the File menu to begin the step to export the certificate into a PKCS#12, or Personal Information Format (.p12) certificate.

3. Name the certificate file being exported as something unique for use with Zenprise Device Manager server. Choose a folder location for the saved certificate, choose the Personal Information Exchange (.p12) file format and click Save.

4. Enter a password for exporting the certificate. Using a unique, strong password is recommended. This password will need to be retained for later use.

5. The Keychain Access application will prompt for the password to the “login” or selected keychain. Enter the password and click OK.

6. The saved certificate is now ready for use with Zenprise Device Manager server. Be sure to keep the certificate and password safe for later use and reference.

**Note:** If you don’t plan to keep and preserve the computer and user account originally used to generate the CSR and complete the certificate export process it is recommended that you save and/or export the Personal and Public Keys originally associated from the local system. Otherwise access to the APNS certificates for reuse will be voided and the entire CSR and APNs process will have to be repeated.

**Import (or Replace) an APNs Certificate**

If you have requested and received a new APNs certificate, please follow these instructions for importing your APNs certificate for the first time, or if you are replacing an existing one:

1. Log in to ZDM as an administrator, or a user who has access to the About tab.

2. Select the About tab. and then click the Update APNs Certificate button.

3. In the Update APNs Certificate dialog, browse to find the appropriate file path to the APNs certificate (.pfx) and enter a new password.

4. Click Load APNs Certificate to load the file.

5. Click Update.
Upload APNs to Zencloud (Zencloud Users Only)

If you are using Zencloud, follow these instructions for uploading your signed APNs to Zencloud:

1. Log in to Zencloud using your Zencloud credentials:
   
   
   Click the **Upload APNS** button.

2. On the APSN Certificate Upload page, click Choose File to select your certificate:

3. Enter your APNs password, and then click **Upload**.

Alternate Option - Generating APNs Using Open SSL

If you would prefer not to use IIS for the APNs certificate request process, you can use OpenSSL instead by performing the tasks below.

Generate a Certificate Signing Request with OpenSSL

The first step for customers is to create a certificate signing request. In order to do so, you can use OpenSSL to generate the certificate request.

   or [http://www.openssl.org/source/](http://www.openssl.org/source/) (other OSes)

2. Create a CSR for submission to Zenprise.

   openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048

   **NOTE:** You will need both files that are generated from this process -
   - **Customer.key.pem** and **CompanyAPNScertificate.csr**

3. You will see the following prompt for certificate Distinguished Name information

   **You are about to be asked to enter information that will be incorporated into your certificate request.**
   **What you are about to enter is what is called a Distinguished Name or a DN.**
   **There are quite a few fields but you can leave some blank**
   **For some fields there will be a default value,**
   **If you enter ".", the field will be left blank.**
   
   -----
   **Country Name (2 letter code) [AU]:** US
   **State or Province Name (full name) [Some-State]:** CA
   **Locality Name (eg, city) []:** RWC
   **Organization Name (eg, company) [Internet Widgits Pty Ltd]:** Customer
4. Enter a password for the CSR private key.

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:
An optional company name []:

5. Send the CSR to Zenprise

6. Zenprise will prepare an MDM signed CSR and return it to you.

---

**Generate a p12 APNs Certificate Using OpenSSL**

The following steps outline how to use the Apple issued MDM certificate with Zenprise.

**Step 1: Create a p12 certificate**

1. Create a p12 certificate with the following command:

   `openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12`

2. Enter a password for the p12 certificate file.

   **NOTE: You will need the password for the certificate in the installation of Device Manager.**

3. Note the location for the p12 certificate file and copy it to the server where you will be installing Zenprise Device Manager.

**Step 2: Install the APNs Certificate on Device Manager**

To install Device Manager refer to the [Zenprise Device Manager Installation Guide](#).
Troubleshooting

When creating your APNs certificate, you might receive error messages or run into issue. This section provides troubleshooting solutions for common problems in the APNs creation process.

Certificate Installation Error

“A certificate chain could not be built to a trusted root authority”

Problem

When downloading a certificate or completing the certificate request for the xxxx.pem APNS certificate provided by Apple into Internet Information Services (IIS) Manager, you might receive the following error "A certificate chain could not be built to a trusted root authority".

Cause

The Apple Root Certificate is not installed on your server.

The Apple Root Certificate Authority should be set on your server as a certificate chain built to a trusted root authority. The Apple Root Certificates are available at the following link:

http://www.apple.com/certificateauthority/

Solution

1. Download and save the following certificates to an appropriate location the following
   a. Apple Inc. Root Certificate
   b. Apple Computer, Inc. Root Certificate
   c. Apple Application Integration Certificate
2. From the MS Windows Server console
   a. Select "Start - Run"
   b. Enter "MMC" and press "Enter"
   c. Select "File - Add/Remove Snap-in"
   d. In the left column list select "Certificates", then select "Add" and "Ok"
   e. A wizard will be presented, select the radio button "Computer account" and click "Next"
   f. Select the radio button "Local computer" and click "Finish" and then click "Ok"
   g. In the left frame, expand "Certificates (Local Computer)", then expand "Trusted Root Certification Authorities", and select "Certificates"
3. In the right frame in an area with only white space "Right click" and select "All Tasks - Import"
4. A wizard will be presented, select the downloaded Apple Root Certificate the which is in the format *.pem (.csr) then selecting "Next".
   a. Place the following Apple Root Certificates into "Trusted Root Certification Authorities - Certificates":
      1. Apple Inc. Root Certificate
      2. Apple Computer, Inc. Root Certificate
   b. In the next window, ensure place the above two certificates into the following store which has Trusted Root Certification Authorities - Certificates selected.
   c. Repeat steps 3 to 4 to apply additional Apple Root Certificates.
5. In the left frame, expand "Certificates (Local Computer)", then expand "Trusted Root Certification Authorities", and select "Certificates"
6. To Import the Apple Application Integration Certificate:
   1. Go-to above step 2-g:
      i. In the left frame, expand "Certificates (Local Computer)", then expand "Personals", and select "Certificates"
   2. A wizard will be presented, select the downloaded Apple Application Integration Certificate which is in the format *.pem (.csr) then selecting "Next".
      i. Place the following Apple Application Integration Certificate into "Personal - Certificates"
      ii. In the next window, ensure place the above certificates into the following store which has Personal - Certificates selected.
7. Return to IIS manager and attempt to complete the certificate signing request and the error should no longer occur.

© 2012 Zenprise, Inc. – All rights reserved.
Renew an APNs Certificate

In order to renew an APNs certificate, you need to perform the same steps you would if you were creating a new certificate from scratch, and then visit the Apple Push Certificates Portal and upload the new certificate. The only difference is that when you visit the Apple certificate portal, you click the Renew button.

To determine when your APNs certificate will expire, in ZDM, select the About tab, and look in the APNs certificate information section:

To renew an APNs Certificate, you need to perform the following tasks:

1. Generate a Certificate Signing Request with Microsoft IIS
2. Submit Newly Created CSR To Zenprise for Signing
3. Submitting a CSR to Apple
   (Here, after logging in you will see your existing certificate or a certificate that was imported from your old Apple Developers account. Choose the Renew option for that certificate.)
4. Generate a p12 APNS Certificate Using Microsoft IIS
5. Update the new APNs certificate to the ZDM server by clicking the Update APNs Certificate button from the About tab inside ZDM.
6. Then, in the Update the APNS Certificate dialog, locate the APNs file, enter the certificate password, click the **Load APNS Certificate** button and then click **Update**.

© 2012 Zenprise, Inc. – All rights reserved.