Generating and Renewing an APNs Certificate

Technical Paper
January 2012

JAMF Software has made all efforts to ensure that this guide is accurate.

JAMF Software
301 4th Ave. South
Suite 1075
Minneapolis, MN 55415
(612) 605-6625

Contents

Overview

Before you can set up mobile device management (MDM) in the Casper Suite, you need to obtain an Apple Push Notification service (APNs) certificate from Apple and upload it to the JSS.

This document explains how to generate an APNs certificate from the Apple Push Certificate Portal or Apple's iOS Developer Enterprise Program (iDEP). It also explains how to upload the certificate to the JSS and renew the certificate when needed.

Using the Apple Push Certificate Portal

Requirements

The instructions in this guide can be used with the Casper Suite v8.0 or later.

Note: In the Casper Suite v8.4 or later, the JSS guides you through the process of generating, uploading, and renewing an APNs certificate. For more information, see the "Apple Push Notification Service Certificate" section in your *Casper Suite Administrator's Guide*.

The instructions in this guide can be used on the following operating systems:

- Mac OS X 10.6 or later
- Windows 2008 or later with Visual C++ Redistributable package
- Red Hat Enterprise Linux (RHEL) 5.5 or later
- Ubuntu LTS 10.4 or later

Before you begin, make sure you have the following applications installed:

For Mac OS X

- Keychain Access
- Safari or Firefox

For Windows

- Open SSL
- Safari or Firefox

For RHEL or Ubuntu

- Open SSL
- Safari

Generating an APNs Certificate

To generate an APNs certificate from the Apple Push Certificate Portal, you must complete the following steps:

1. Create a Certificate Signing Request (CSR).
2. Generate the APNs certificate.
3. Save the APNs certificate as a .p12 file.

Step 1: Create a CSR

First, create a CSR and email it to JAMF Software. JAMF Software signs the CSR and emails it back to you in a .plist file.

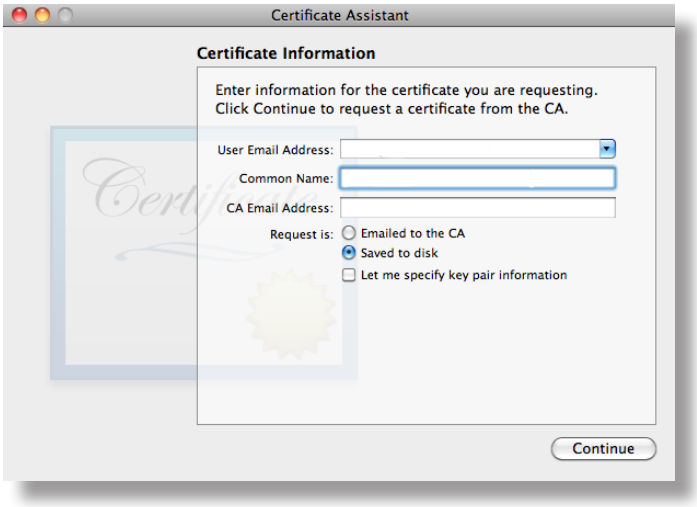
> ***Note:*** You must have an active Casper Suite activation code (trial or purchased) to obtain a signed CSR from JAMF Software.

To create a CSR on Mac OS X:

1. Open Keychain Access.
2. From the menu bar, select **Keychain Access** > **Certificate Assistant** > **Request a Certificate From a Certificate Authority**.
3. Enter the following information for the certificate:
   - **User email address**

     The Apple ID that you will use to log into the Apple Push Certificate Portal
   - **Common name**

     The unique name that will be used to identify the certificate in Keychain Access



4. Select the **Saved to disk** option, and then click **Continue**.
5. Save the CSR.
6. Email the CSR to your JAMF Software Representative.

   If you are a current customer, email the CSR to your Account Manager.

   If you are a potential customer, email the CSR to your Systems Engineer.

   A .plist file that contains the signed CSR is emailed back to you.

To create a CSR on Windows, RHEL, or Ubuntu:

1. From the command line, create the CSR and the private key by executing:

```
openssl req -out /path/to/resulting/request.csr -new -newkey
  rsa:2048 -nodes -keyout /path/to/resulting/privateKey.key
```

2. Create a Distinguished Name (DN) for the certificate request by entering the following information:

Attribute	Value
Country	Abbreviation for country or region
State or Province Name	Abbreviation for state or province
Locality Name	City or locality
Organization Name	Name of your organization
Organizational Unit Name	Department within your organization
Common Name	Unique name that will be used to identify the certificate
Email Address	Email address

3. When you are done entering information for the DN, press the Return key.
4. When prompted to enter a company name, press the Return key.
5. Email the CSR to your JAMF Software Representative.

   If you are a current customer, email the CSR to your Account Manager.

   If you are a potential customer, email the CSR to your Systems Engineer.

   A .plist file that contains the signed CSR is emailed back to you.

Step 2: Generate the APNs Certificate

Next, generate the APNs certificate by uploading the .plist file that you received from JAMF Software to the Apple Push Certificate Portal.

To generate the APNs certificate:

1. Open the web browser required for your operating system. (See the "Requirements" section for specifications.)
2. Go to the Apple Push Certificate Portal at https://identity.apple.com/pushcert/.
3. Sign in using your Apple ID and password.

> ***Note:*** It is recommended that you log in using a shared, company Apple ID.

4. Click **Create a Certificate**.

5. Read and accept the Terms of Use, and then click **Agree**.
6. Upload the .plist file that you received from JAMF Software.

7. Click **Download** to download the APNs certificate.

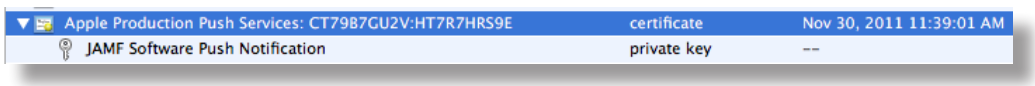
Step 3: Save the APNs Certificate as a .p12 File

Save the certificate as a .p12 file so that you can upload it to the JSS.

To save the APNs certificate as a .p12 file on Mac OS X:

1. Open Keychain Access.
2. Select **login** under the Keychain heading in the sidebar.
3. Drag the certificate that you downloaded from the Apple Push Certificate Portal into Keychain Access.
4. Click the **Certificates** category in the sidebar.
5. Click the disclosure triangle next to the certificate, and verify that a private key is associated with it.

   The name of the private key should be the common name that you entered when you generated the CSR.



6. Select the certificate and the private key.
7. From the menu bar, choose **File** > **Export Items** and save the items as a .p12 file.
   The .p12 file is a bundle that contains both the certificate and the private key.
8. Create and verify a password to secure the file, and then click **OK**.
   You will need to specify this password when you upload the certificate to the JSS.

9. Quit Keychain Access.

   The certificate is saved as a .p12 file in the location you specified.

To save the APNs certificate as a .p12 on Windows, RHEL, or Ubuntu:

1. From the command line, convert the certificate to .pem format by executing:

```
openssl x509 -inform der -in /path/to/apple/downloaded/cert.cer -out
  /path/to/formatted/cert.pem -outform PEM
```

2. Create a store for the certificate and the private key by executing:

```
openssl pkcs12 -export -in /path/to/formated/cert.pem -inkey /path/
  to/step/3/privateKey.key -out /path/to/save/push_notification_
  cert.p12 -name apns-cert
```

   This saves the certificate and the private key as a .p12 file.
   The .p12 file is a bundle that contains both the certificate and the private key.
3. Type a password to secure the file, and then press the Return key.
   You will need to specify this password when you upload the certificate to the JSS.
4. Type the password again to verify it, and then press the Return key.

Uploading the APNs Certificate to the JSS

Before you upload the APNs certificate to the JSS, make sure you have:

- The APNs certificate in .p12 format
- The password you created to secure the .p12 file

To upload the APNs certificate (.p12) to the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Global Management Framework Settings** link.
   In the Casper Suite v8.21 or earlier, click the **Mobile Device Management Settings** link.
4. Click the **Push Notification Certificate** tab.
   In the Casper Suite v8.21 or earlier, click the **APNs** tab.
5. Click the **Create a certificate using the Push Notification Certificate Assistant** link, and then click the **Upload .p12 file** button.
   In the Casper Suite v8.31 or earlier, click the **Upload** link.
6. Enter the password you created to secure the certificate, and then click **Next**.
7. Click **Save**.

Renewing an APNs Certificate

Use the instructions in this section to renew an APNs certificate obtained from the Apple Push Certificate Portal.

To renew an APNs certificate obtained from the Apple Push Certificate Portal:

1. Create a new CSR and email it to the appropriate JAMF Software Representative. (See "Step 1: Create a CSR" for complete instructions.)
   A .plist file that contains the signed CSR is emailed back to you.
2. Open the web browser required for your operating system. (See the "Requirements" section for specifications.)
3. Go to the Apple Push Certificate Portal at https://identity.apple.com/pushcert/.
4. Sign in using your Apple ID and password.

> ***Note:*** It is recommended that you log in using a shared, company Apple ID.

5. Click the **Renew** button next to the APNs certificate you want to renew.
6. Upload the new .plist file that you received from JAMF Software.
7. Click **Download** to download the new certificate.
8. Save the certificate as a .p12 file. (See "Step 3: Save the APNs Certificate as a .p12 File" for complete instructions.)
9. Replace the old certificate by uploading the new one to the JSS. (See "Uploading an APNs Certificate to the JSS" for complete instructions.)

Using Apple's Developer Enterprise Program

Requirements

The instructions in this guide can be used with the Casper Suite v8.0 or later.

To generate an APNs certificate from iDEP, you or a member of your organization must be enrolled in iDEP as a registered Team Agent.

Note: Only registered Team Agents can access the iOS Provisioning Portal from which the APNs certificate is generated.

This instructions in this guide can be used on the following operating systems:

- Mac OS X 10.5 or later
- Windows 2008 or later with Visual C++ Redistributable package
- Red Hat Enterprise Linux (RHEL) 5.5 or later
- Ubuntu LTS 10.4 or later

Before you begin, make sure you have the following applications installed:

For Mac OS X

- Keychain Access
- Safari or Firefox

For Windows

- Open SSL
- Safari or Firefox

For RHEL or Ubuntu

- Open SSL
- Safari

Generating an APNs Certificate

To generate an APNs certificate from iDEP, you must complete the following steps:

1. Create a Certificate Signing Request (CSR).
2. Generate the APNs certificate.
3. Save the APNs certificate as a .p12 file.

Step 1: Create a CSR

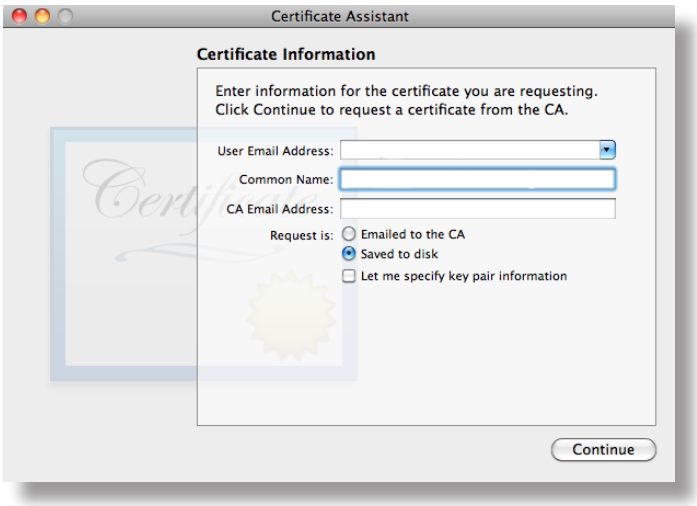
First, create the CSR that you will upload to iDEP.

To create a CSR on Mac OS X:

1. Open Keychain Access.
2. From the menu bar, select **Keychain Access** > **Certificate Assistant** > **Request a Certificate From a Certificate Authority**.
3. Enter the following information for the certificate:
   - **User email address**

     Your email address
   - **Common name**

     The unique name that will be used to identify the certificate in Keychain Access



4. Select the **Saved to disk** option, and then click **Continue**.
5. Save the CSR.

To create a CSR on Windows, RHEL, or Ubuntu:

1. From the command line, create the CSR and the private key by executing:

```
openssl req -out /path/to/resulting/request.csr -new -newkey
  rsa:2048 -nodes -keyout /path/to/resulting/privateKey.key
```

2. Create a Distinguished Name (DN) for the certificate request by entering the following information:

Attribute	Value
Country	Abbreviation for country or region
State or Province Name	Abbreviation for state or province
Locality Name	City or locality
Organization Name	Name of your organization
Organizational Unit Name	Department within your organization
Common Name	Name associated with the Apple Developer Account
Email Address	Email address

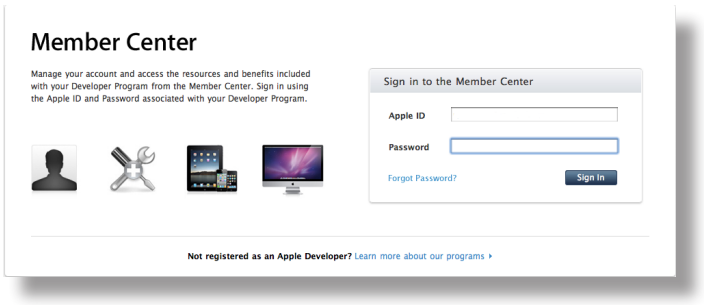
3. When you are done entering information for the DN, press the Return key.
4. When prompted to enter a company name, press the Return key.

Step 2: Generate the APNs Certificate

Next, generate the APNs certificate by uploading the CSR to iDEP's iOS Provisioning Portal.

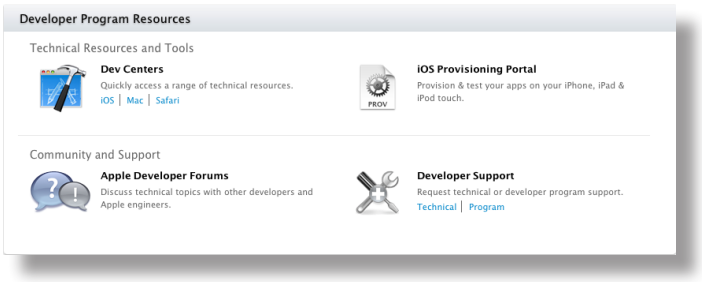
To generate the APNs certificate:

1. Open the web browser required for your operating system. (See the "Requirements" section for specifications.)
2. Go to the Apple Developer Connection website at http://developer.apple.com.
3. Click **Member Center** at the top of the page.
4. Sign in using your Apple ID and password.



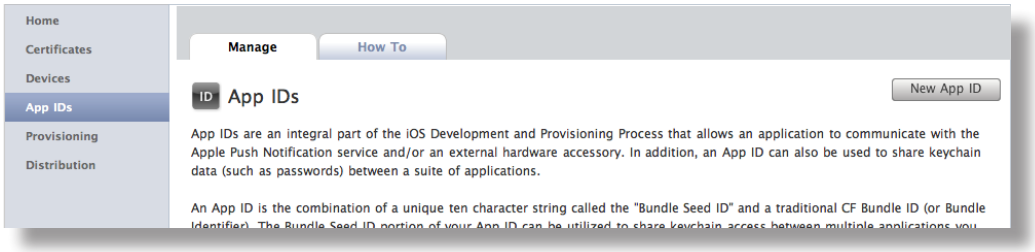
5. Under Dev Centers, click the **iOS** link.

6. Click **iOS Provisioning Portal.**



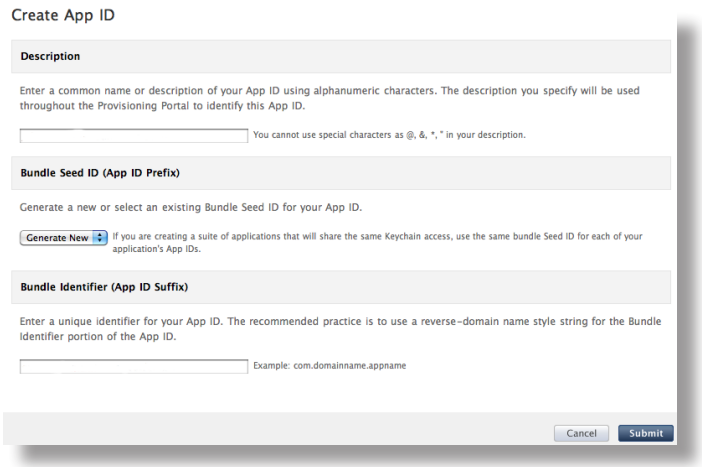
7. In the sidebar, click **App IDs**.

8. Click the **New App ID** button.

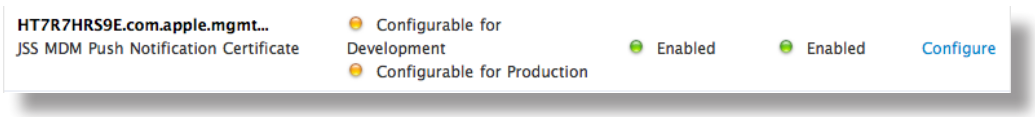


9. Enter a description and unique bundle identifier for the App ID, and then click **Submit**.

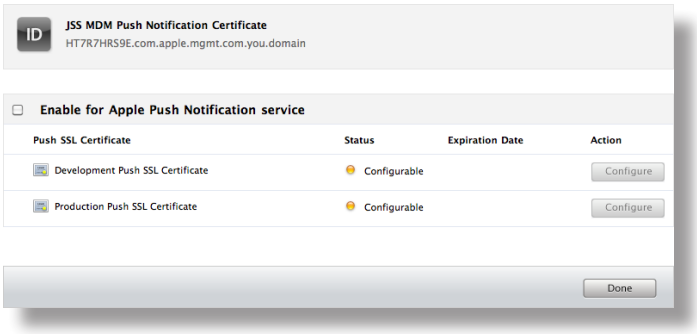
> ***Important:*** The unique bundle identifier must begin with com.apple.mgmt and end with a unique string. For example: com.apple.mgmt.com.yourorganization.domain



10. Find the certificate and click **Configure** across from it.



11. Select the **Enable for Apple Push Notification service** checkbox.



12. Click **Configure** across from the certificate labeled **Production Push SSL Certificate**.

13. When the Apple Push Notification Service SSL Certificate Assistant appears, follow the onscreen instructions to generate the certificate.

Step 3: Save the APNs Certificate as a .p12 File

Save the certificate as a .p12 file so that you can upload it to the JSS.

To save the APNs certificate as a .p12 file on Mac OS X:

1. Open Keychain Access.

2. Select **login** under the Keychain heading in the sidebar.

3. Drag the certificate you generated in "Step 2: Generate the APNs Certificate" into Keychain Access.

4. Click the **Certificates** category in the sidebar.

5. Click the disclosure triangle next to the certificate, and verify that a private key is associated with it.
   The name of the private key should be the common name that you entered when you generated the CSR.

6. Select the certificate and the private key.

7. From the menu bar, choose **File** > **Export Items** and save the items as a .p12 file.
   The .p12 file is a bundle that contains both the certificate and the private key.

8. Create and verify a password to secure the file, and then click **OK**.
   You will need to specify this password when you upload the certificate to the JSS.

9. Quit Keychain Access.

   The certificate is saved as a .p12 file in the location you specified.

To save the APNs certificate as a .p12 file on Windows, RHEL, or Ubuntu:

1. From the command line, convert the certificate to .pem format by executing:

```
openssl x509 -inform der -in /path/to/apple/downloaded/cert.cer -out
  /path/to/formatted/cert.pem -outform PEM
```

2. Create a store for the certificate and the private key by executing:

```
openssl pkcs12 -export -in /path/to/formated/cert.pem -inkey /path/
  to/step/3/privateKey.key -out /path/to/save/push_notification_
  cert.p12 -name apns-cert
```

   This saves the certificate and the private key as a .p12 file.
   The .p12 file is a bundle that contains both the certificate and the private key.

3. Type a password to secure the file, and then press the Return key.
   You will need to specify this password when you upload the certificate to the JSS.

4. Type the password again to verify it, and then press the Return key.

Uploading an APNs Certificate to the JSS

Before you upload the APNs certificate to the JSS, make sure you have:

- The APNs certificate in .p12 format
- The password you created to secure the .p12 file

To upload an APNs certificate (.p12) to the JSS:

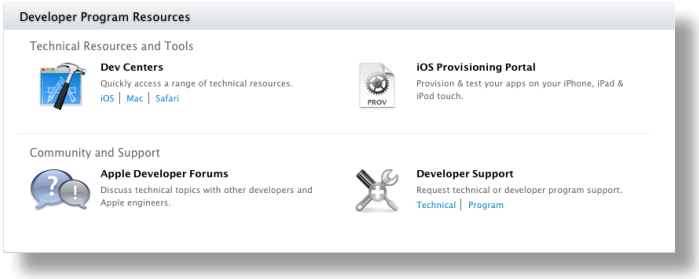
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Global Management Framework Settings** link.
   In the Casper Suite v8.21 or earlier, click the **Mobile Device Management Settings** link.
4. Click the **Push Notification Certificate** tab.
   In the Casper Suite v8.21 or earlier, click the **APNs** tab.
5. Click the **Create a certificate using the Push Notification Certificate Assistant** link, and then click the **Upload .p12 file** button.
   In the Casper Suite v8.31 or earlier, click the **Upload** link.
6. Enter the password you created to secure the certificate, and then click **Next**.
7. Click **Save.**

Renewing an APNs Certificate

Use the instructions in this section to renew an APNs certificate obtained from iDEP.

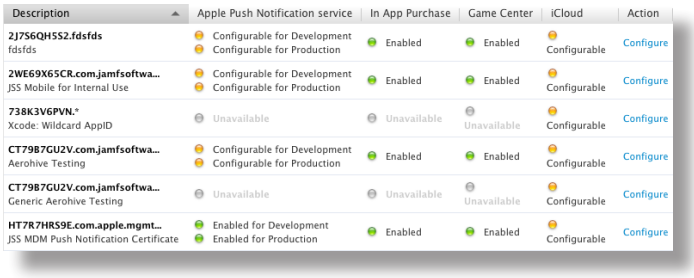
To renew an APNs certificate obtained from iDEP:

1. Create a new CSR. (See "Step 1: Create a CSR" for complete instructions.)
2. Open the web browser required for your operating system. (See the "Requirements" section for specifications.)
3. Go to the Apple Developer Connection website at http://developer.apple.com.
4. Click the **Member Center** at the top of the page.
5. Sign in using your Apple ID and password.
6. Click **iOS Provisioning Portal**.

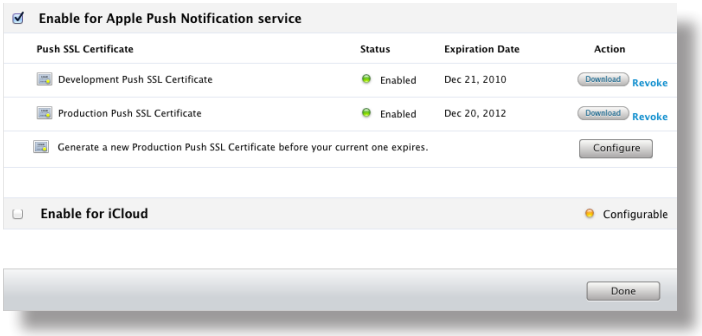


7. In the sidebar, click **App IDs**.

8. Find your existing App ID and click **Configure** across from it.



9. Find the certificate and click the **Configure** button across from it.



> ***Note:*** You can only have one production certificate enabled at a time.

10. When the Apple Notification Assistant appears, follow the onscreen instructions to renew the certificate.
11. Save the new certificate as a .p12 file. (See "Step 3: Save the APNs Certificate as a .p12 File" for complete instructions.)
12. Replace the old certificate by uploading the new one to the JSS. (See "Uploading an APNs Certificate to the JSS" for complete instructions.)