Generating an Apple Push Notification Service (APNS) Certificate

ZENworks® Mobile Management 2.8.x

September 2013

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Table of Contents

Apple Push Notification Service (APNs)

What Is APNs

Apple Push Notification service (APNs) is a highly secure and efficient system for communicating with iOS devices over-the-air (OTA). Each device establishes an accredited and encrypted IP connection with the service. The provider, in this case your *ZENworks Mobile Management* server, connects with and sends its notification to the APNs, which pushes the notification to the target device.

An APNs certificate is required for Apple Push Notification service. The certificate must be renewed annually. This guide explains the process of obtaining the APNs certificate from Apple and provides instructions on how to upload the certificate to the *ZENworks Mobile Management* server via its dashboard.

There are various methods of generating the APNs certificate, any of which you may use. This document guides you through generating the certificate by using Microsoft Windows Internet Information Services (IIS) Manager, version 6, 7, or 8.

How APNs Works

Apple Push Notification service works in conjunction with the built-in MDM protocol of Apple iOS devices. *ZENworks Mobile Management* uses the Apple Push Notification service to send notifications to the iOS device requesting information. Only notifications, not data, are sent through the APNs server. The device responds directly to the *ZENworks Mobile Management* server.

The Apple MDM protocol provides the following functionality:

- Devices support Selective Wipe, Lock Device, and Clear Passcode
- Full Wipe and Lock Device commands are applied immediately
- You can record and access installed applications on devices
- You can record and access installed configuration profiles on devices
- You have access to additional device statistics
- Configuration profile updates require no user interaction
- Enterprise (in-house) apps
- Mobile App Management
- Manage VPP (Redemption) Codes

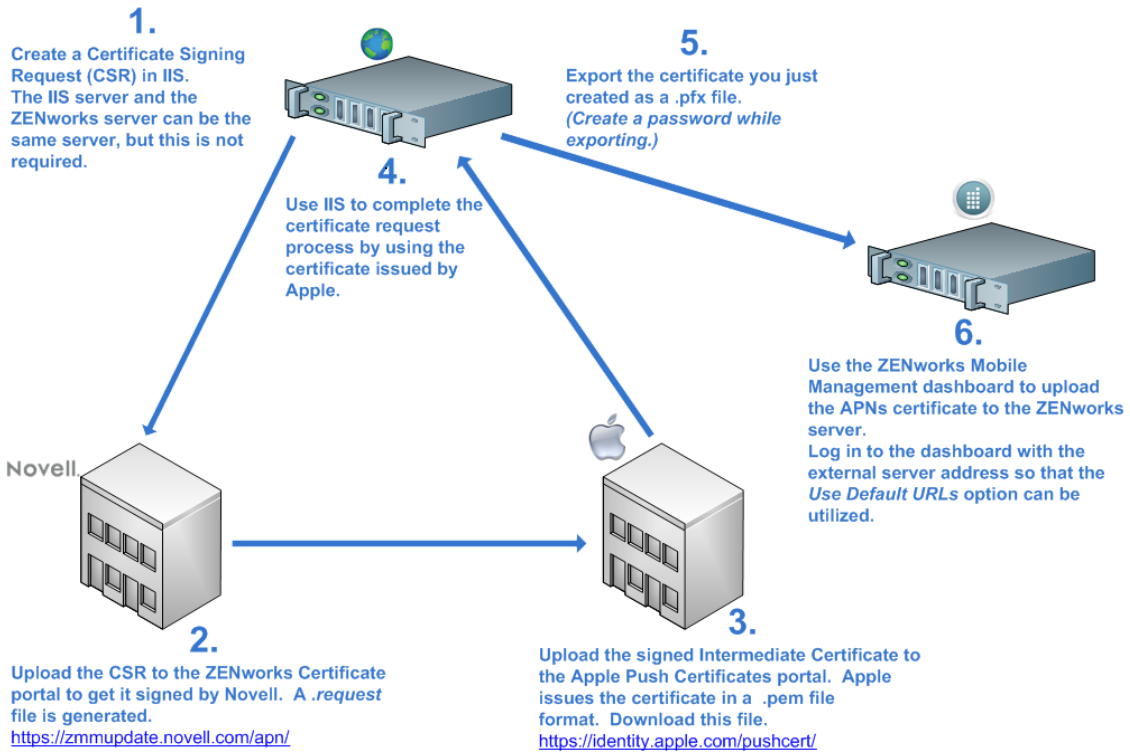
Requirements

- *ZENworks Mobile Management* version 2.5.2 or later
- An Apple ID. We recommend that you do not use a personal Apple ID, but create a separate corporate Apple ID for MDM. Associate the Apple ID with an email account that will remain with your company – not an email account that belongs to an individual in the company. This facilitates a smooth certificate renewal process each year.
- Windows Server 2003, 2008, or 2012 (you need administrator permissions)
- Firefox or Safari Web browser

An Overview of the Steps to Obtain the Apple Push Notification Service Certificate

1. Create a Certificate Signing Request (CSR). (This guide provides instructions for creating the certificate from Microsoft Windows Internet Information Services (IIS) Manager, version 6, 7, or 8. An alternate method, using OpenSSL, is documented in Appendix A.)
2. Upload the CSR to the *ZENworks Mobile Management Certificate Portal*. Novell, Inc. signs the CSR.
3. Upload the intermediate certificate (the CSR signed by Novell, Inc.) to the Apple Push Certificates Portal. Apple issues the certificate.
4. Download the signed certificate from the Apple Push Certificates Portal and complete the certificate request in IIS.
5. Export the certificate to a file.
6. Upload the certificate to the *ZENworks Mobile Management* server.

Generating an Apple Push Notification Service Certificate for use with ZENworks Mobile Management for iOS



Generating an APNs Certificate

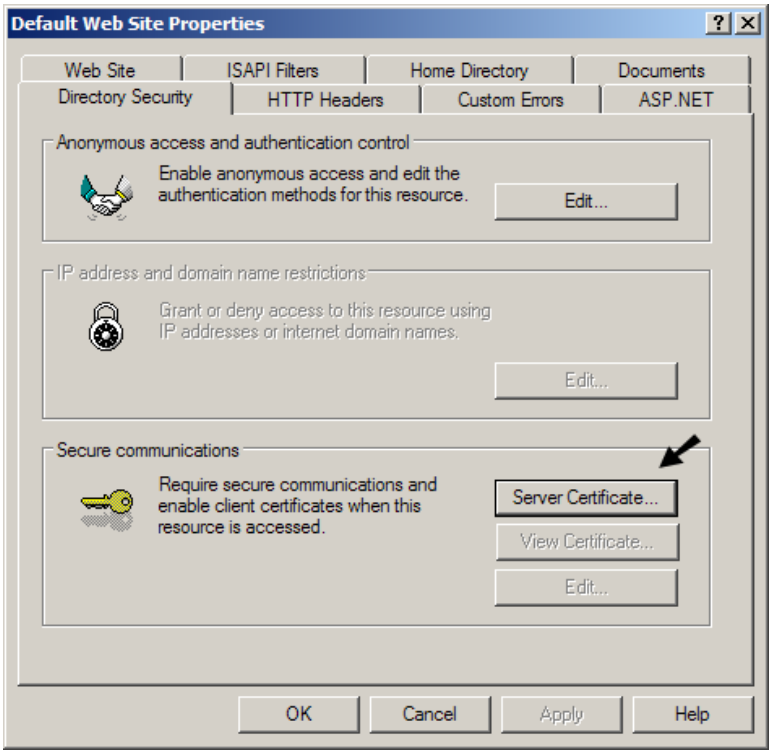
Generating an APNs Certificate from Windows Server 2003

The following instructions are for generating an APNs certificate from a Windows Server 2003 by using Internet Information Services (IIS) Manager version 6. You can skip this section if you use Windows Server 2008 or 2012. For Windows Server 2008 or 2012, see Generating an APNs Certificate from Windows Server 2008 or 2012.

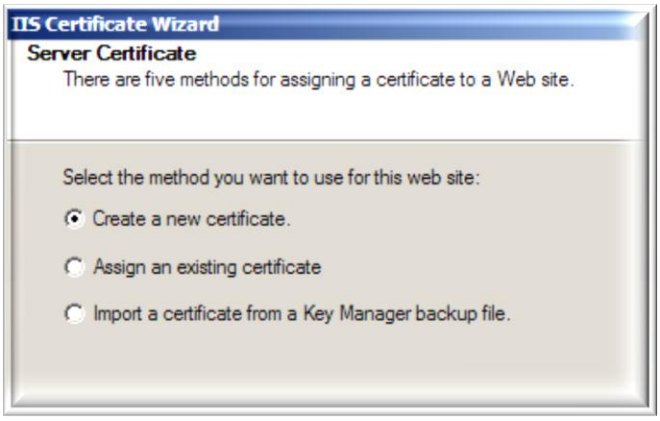
Note: Appendix A provides instructions for an alternate method of generating the APNs certificate using OpenSSL.

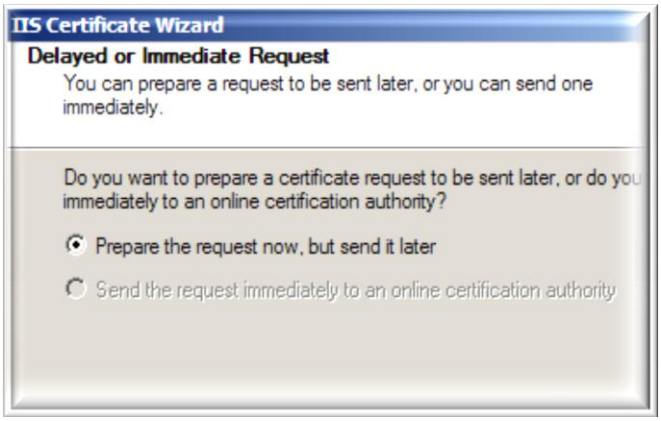
Creating the Certificate Signing Request (CSR) from IIS Manager 6

1. Select **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Right-click any Web site in the left panel. Select **Properties**.
3. Select the **Directory Security** tab and then click the **Server Certificates** button in the *Security* section of the menu. This starts the Web Server Certificate Wizard. Click **Next** to continue.

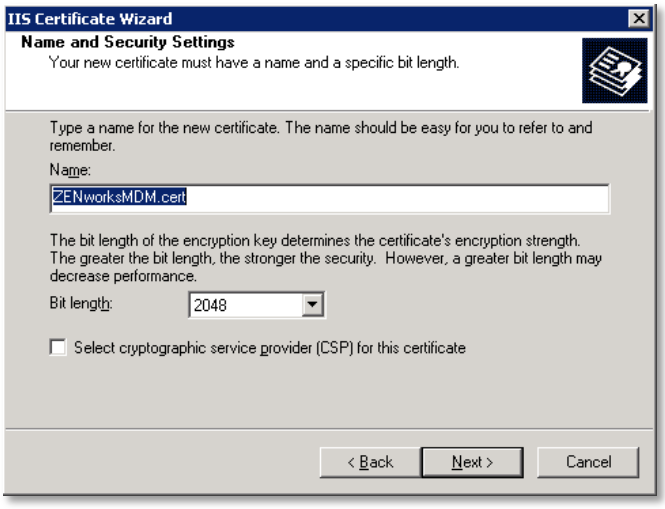


4. Select the **Create a new certificate** option and click **Next**.
5. Select **Prepare the request now, but send it later** option and click **Next**.



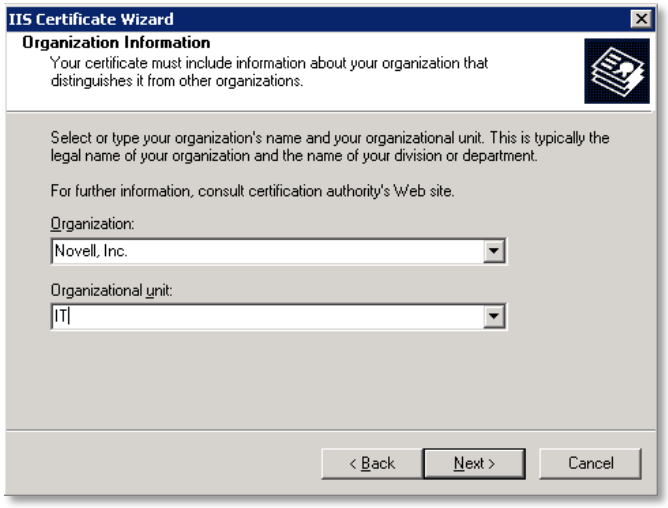


6. Enter a certificate name that is easily remembered. In the **Bit length** field, select **2048** for the encryption level, then select **Select cryptographic service provider (CSP) for this certificate**. Click **Next**.
7. From the *Available Providers* window, select **Microsoft RSA SChannel Cryptographic Provider**. Click **Next**.



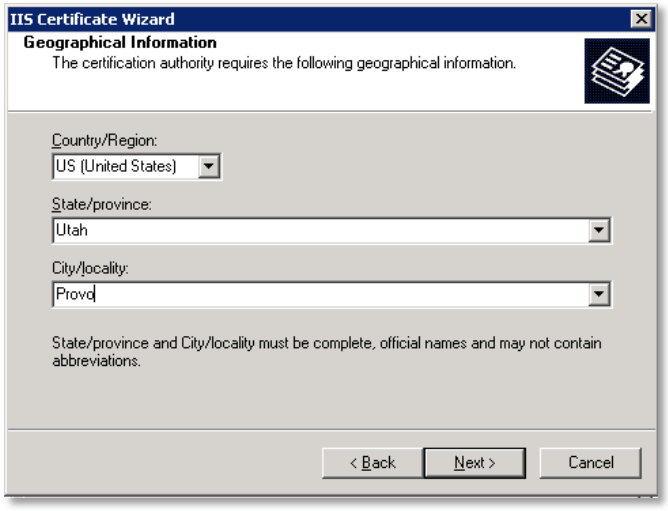
8. Enter the legal name of your **Organization** and the **Organization unit**, which is the department within your organization. Click **Next**.

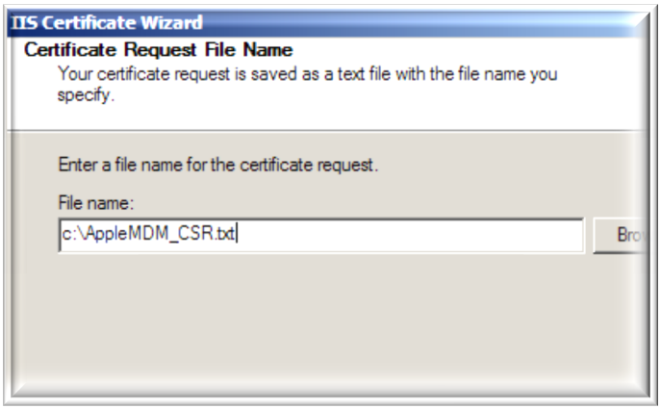
9. In the **Common name** field, enter a valid Apple ID. This does not need to be an Apple Developer account ID, but you should use an Apple ID that has been designated for managing the corporate APNs certificate. The Apple ID might be in the form of an email address, or possibly a display name. Click **Next**.



10. Enter the **Country/Region**, **State/Province**, and **City/locality** of your organization. Click **Next**.

    In the Certificate Request File Name window, save the CSR to your computer. Record the location and filename. This is the file you will upload to the *ZENworks Mobile Management Certificate Request Portal*. Click **Next**.





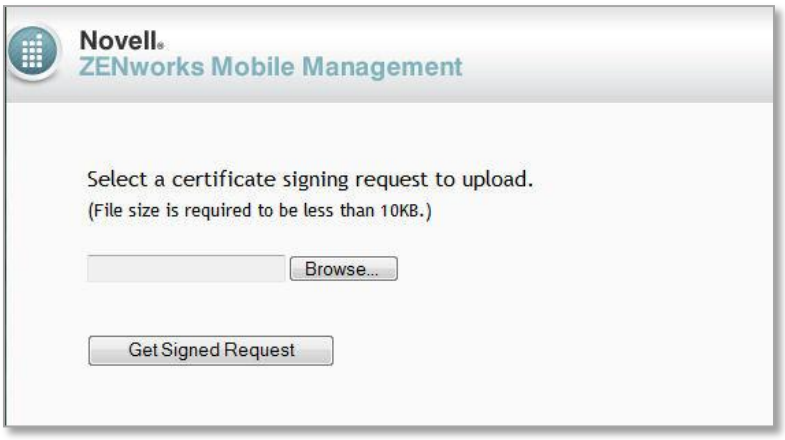
11. Review the information for the certificate request in the Request File Summary window. To make revisions, click the **Back** button. Click **Next** to accept, then click **Finish**.

Uploading the CSR to the ZENworks Mobile Management Certificate Request Portal

The CSR file you generated through IIS must be signed by Novell before you can upload it to the Apple Push Certificates Portal. You will need:

- Access to the CSR file
- Your Novell login credentials

1. Navigate to the *ZENworks Mobile Management* Certificate Portal at https://zmmupdate.novell.com/apn



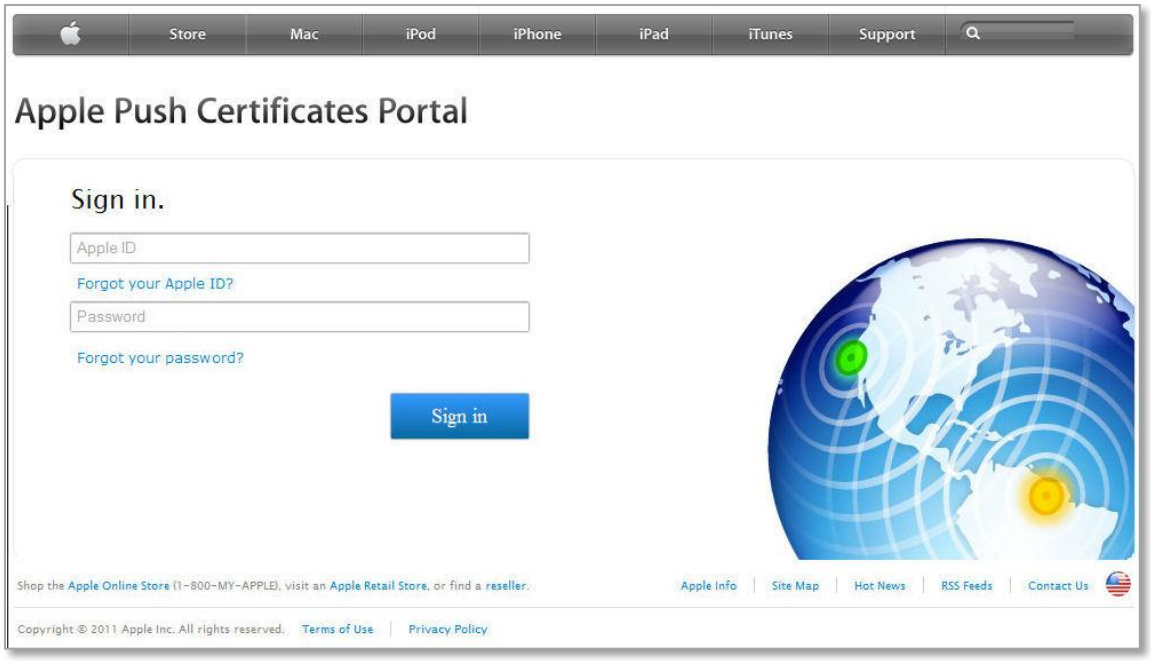
2. Browse to select the CSR file.
3. Click **Get Signed Request**.
4. Save the signed request.

You are now ready to upload the signed ***ZENworks.request*** file (the intermediate certificate) to the Apple Push Certificates Portal.

Uploading the Intermediate Certificate to the Apple Push Certificates Portal

At the Apple Push Certificates Portal, you accept a license agreement and upload the intermediate certificate that you downloaded from the ZENworks Mobile Management Certificate Portal. A new Apple signed push certificate is created for you to download.

1. Browse to the Apple Push Certificates portal at: https://identity.apple.com/pushcert/
2. Log in by using your Apple ID and password. This does not need to be an Apple Developer account ID, but you should use an Apple ID that has been designated for managing the corporate APNs certificate.



3. Select **Create a Certificate**.

4. Read the *Terms of Use* and accept the End User License Agreement.

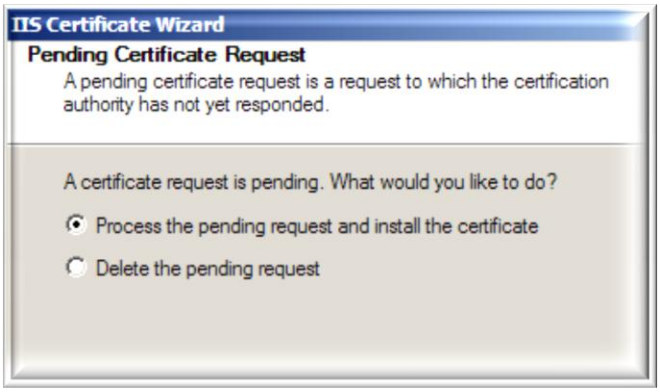
5. Select and upload the intermediate certificate you downloaded from the *ZENworks Mobile Management* Certificate Portal.

6. When the upload has finished, a new certificate for *ZENworks Mobile Management* appears. Select **Download** to download the Apple signed certificate.

You are now ready to complete the CSR and export the APNs certificate to the *ZENworks Mobile Management* server.

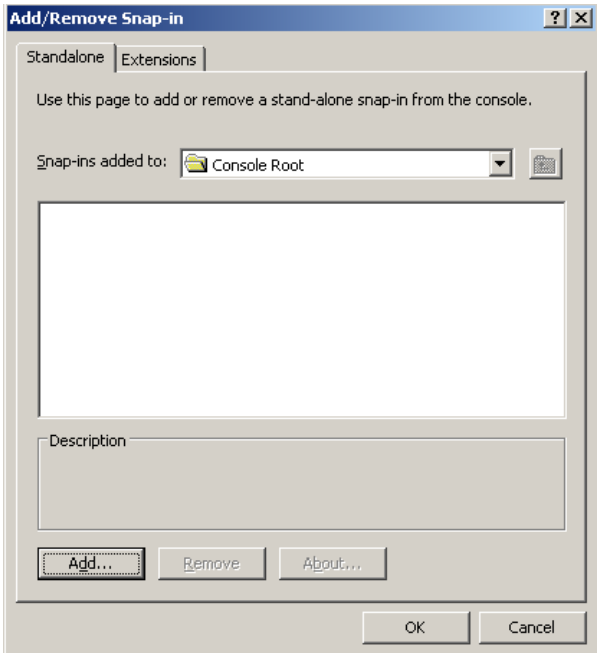
Completing the Certificate Request from IIS Manager 6

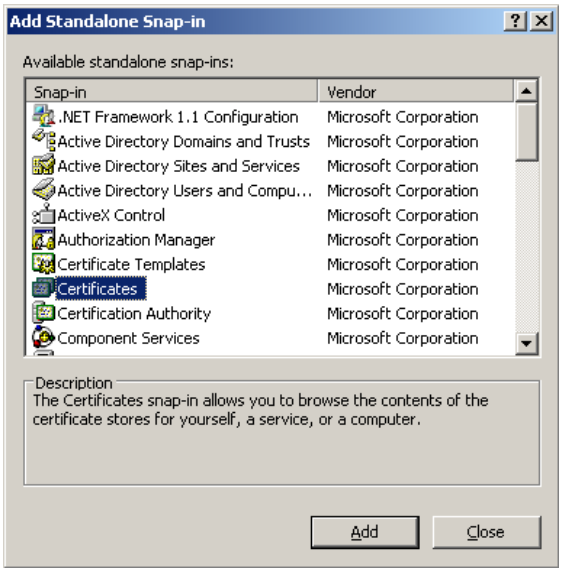
1. Return to the IIS Manager. Select **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Right-click any Web site in the left panel. Select **Properties**.
3. Select the **Directory Security** tab and then click the **Server Certificates** button in the *Security* section of the menu. This starts the Web Server Certificate Wizard. Click **Next** to continue.
4. Select the **Process the pending request and install the certificate** option and click **Next**.
5. Browse to the *aps_production_identity.pem* file that was provided by Apple. Click **Next**.



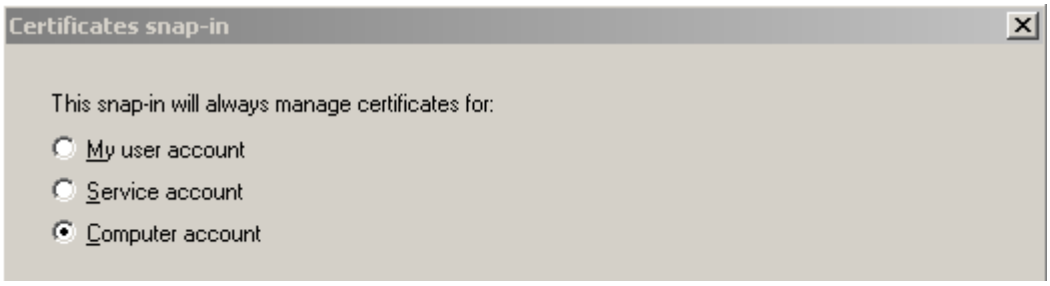
6. On the Certificate Summary screen, verify that the certificate information is correct and click **Next**, then click **Finish**.
7. Open the *Microsoft Management Console (MMC)*. Click **Start** > **Run** and enter **MMC**.
8. From the *File* menu, select **Add/Remove Snap-in**.

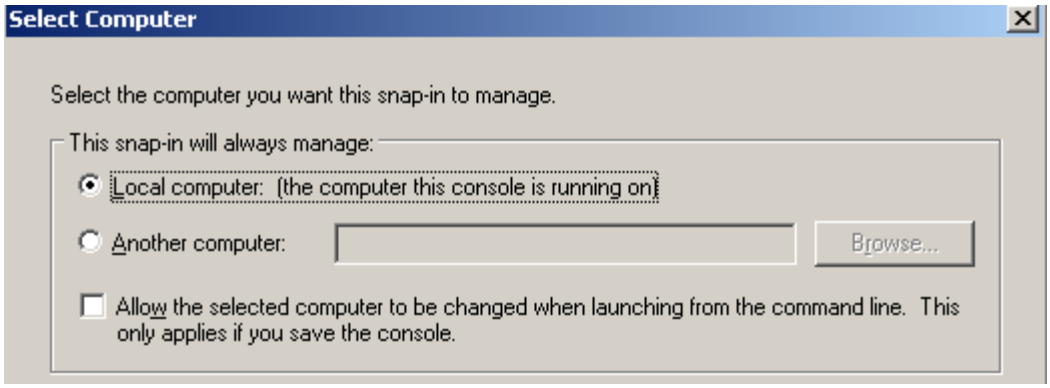
9. From the drop-down list at **Snap-ins added to**, select ***Console Root*** and click **Add.** On the *Add Standalone Snap-in* screen, select **Certificates**, then click **Add.**





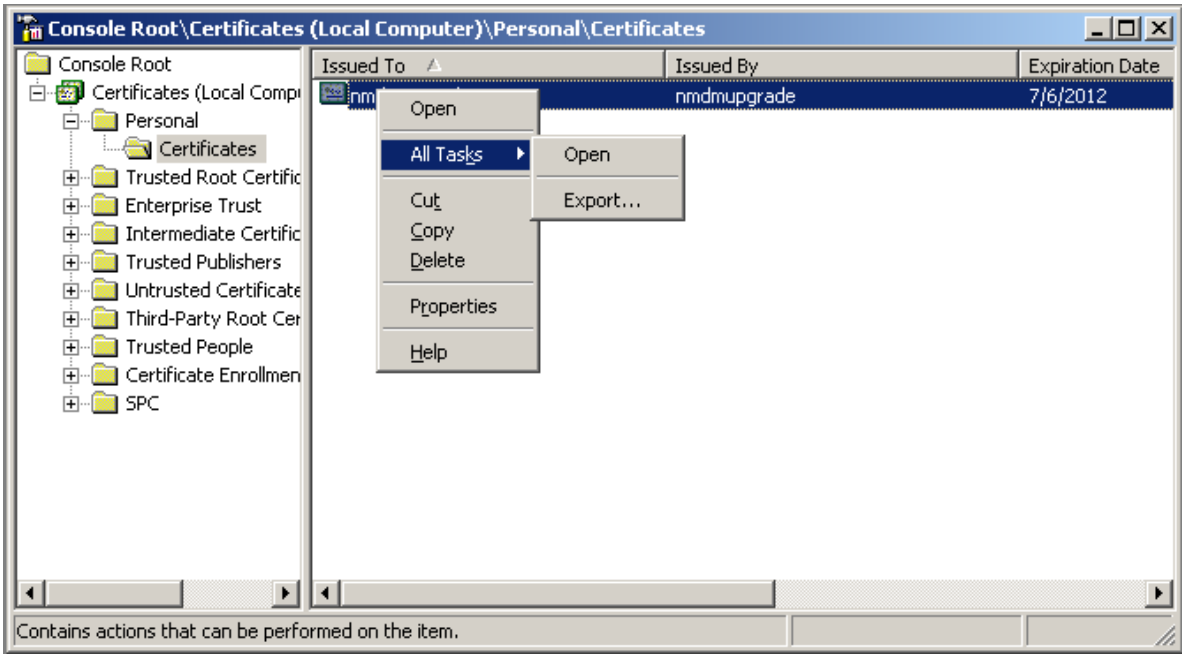
10. On the *Certificates snap-in* screen, select **Computer account** and click **Next**. Choose **Local computer** and click **Finish**.





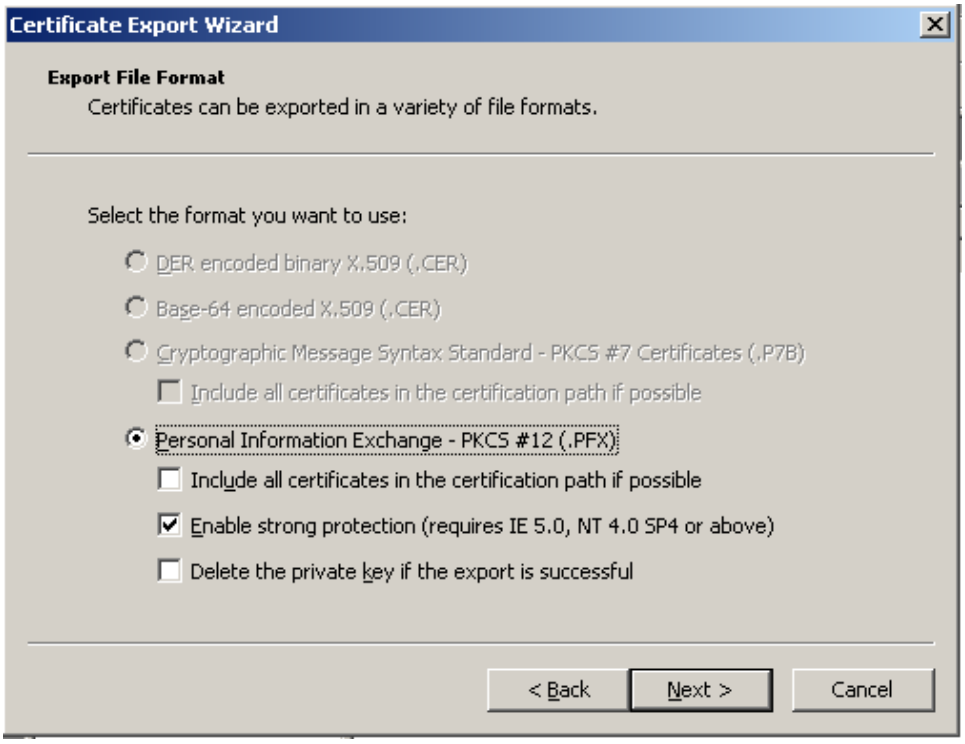
11. Click **Close**. Click **OK** on the *Add/Remove Snap-in* screen**.**

12. At the *Console Root*, expand the directory. Select **Certificates** > **Personal** > **Certificates**. Right-click on the certificate file and select **All Tasks** > **Export**. This opens the Export Wizard. Click **Next** to continue.



13. Select **Yes** to export the private key, then click **Next**.

14. Select the **Personal Information Exchange – PKCS #12 (.PFX)** format and select the **Enable strong protection** box. Click **Next**.



15. Enter and confirm a password. You will need this password when you upload the certificate to *ZENworks Mobile Management*. Click **Next**.

16. Click the Browse button and select the .pfx file that you want to export. Click Next.

17. Click **Finish** to complete the certificate export. You see a message that says the export was successful.

    Now you are ready to upload the certificate to *ZENworks Mobile Management*. You need the following:

    - APNs certificate file (.pfx format)
    - The password you set when exporting the certificate

    Continue with **Upload the APNs Certificate to *ZENworks Mobile Management***.

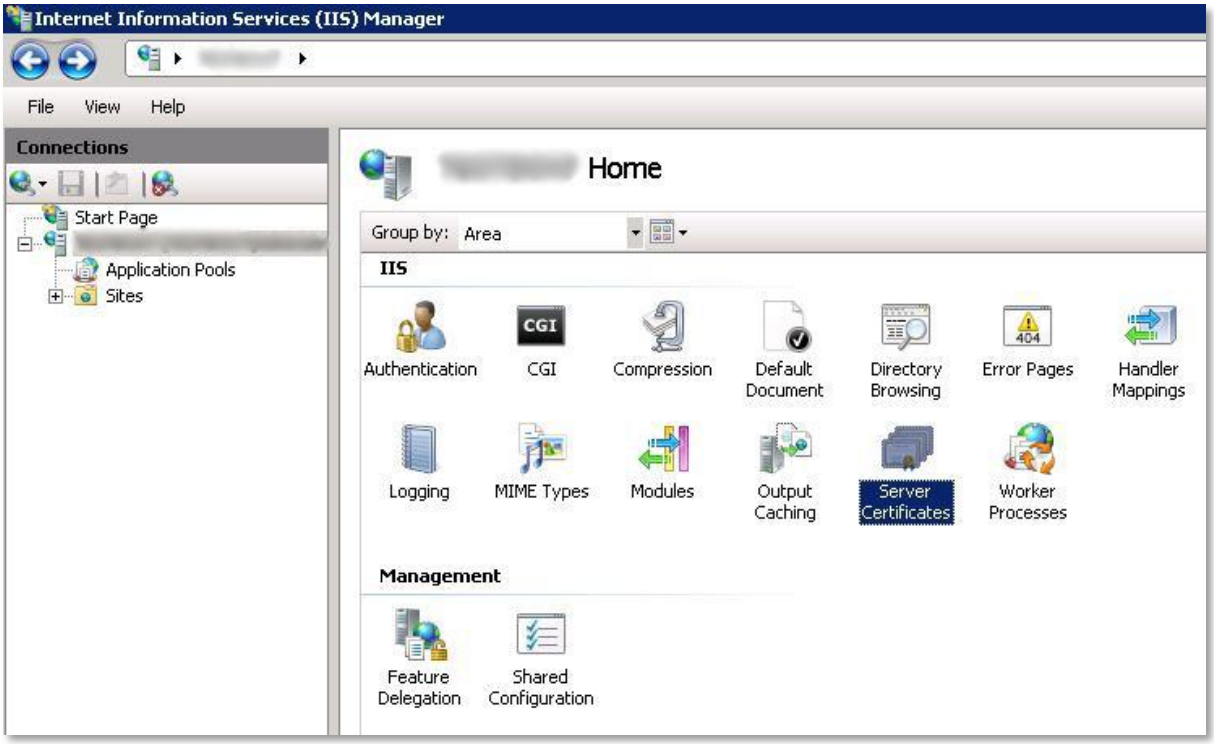
Generating an APNs Certificate from Windows Server 2008 or 2012

The following instructions are for generating an APNs certificate from Windows Server 2008 or 2012 by using Internet Information Services (IIS) Manager version 7 or 8. You can skip this section if you use Windows Server 2003. For Windows Server 2003, see Generating an APNs Certificate from Windows Server 2003.

Note: Appendix A provides instructions for an alternate method of generating the APNs certificate using OpenSSL.

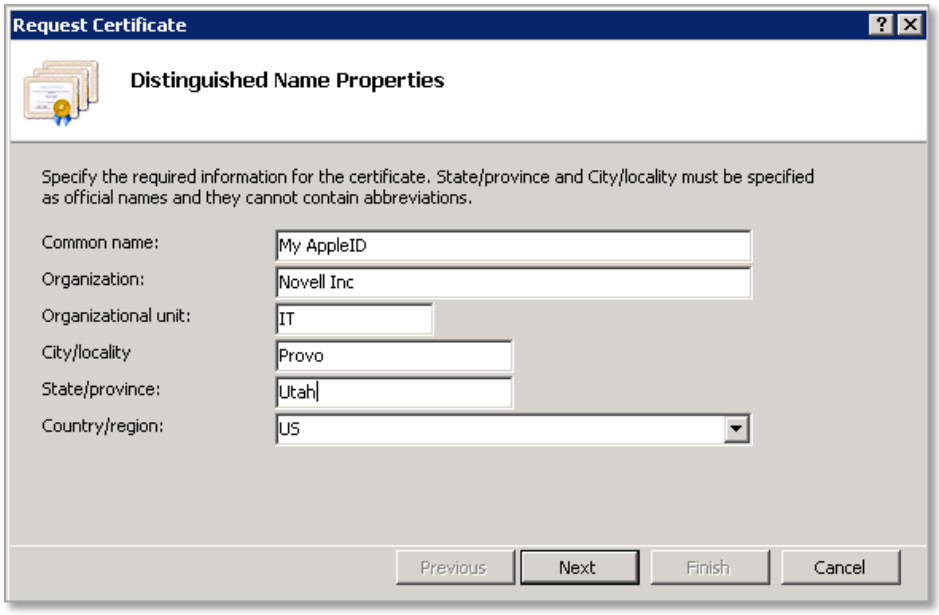
Creating the Certificate Signing Request (CSR) from IIS Manager 7 or 8

1. Navigate to **Administrative Tools** and select **Internet Information Services (IIS) Manager**.
2. Select the server name in the left panel, then double-click the **Server Certificates** option in the *Security* section of the menu.

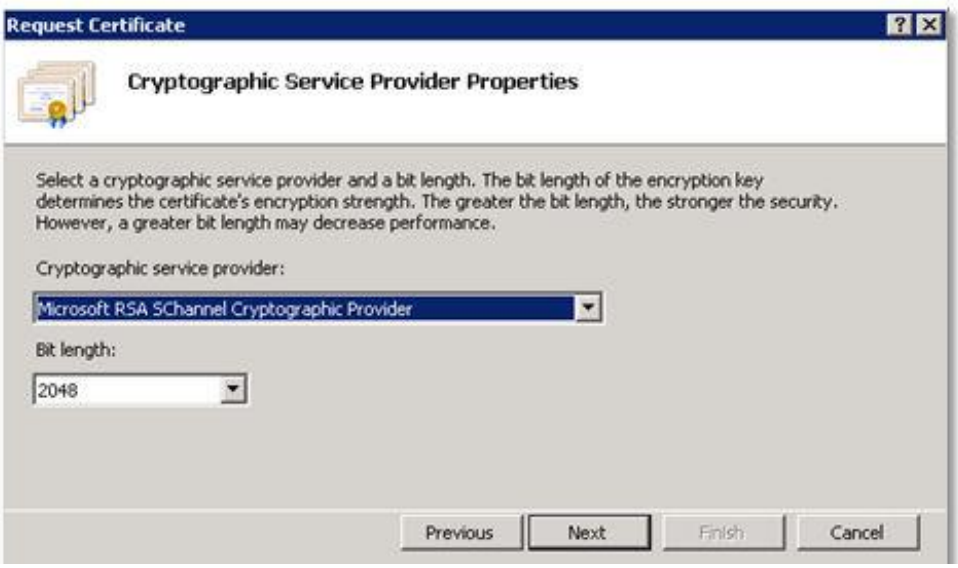


3. From the *Actions* menu in the right panel, select **Create Certificate Request.** This starts the Request Certificate Wizard.

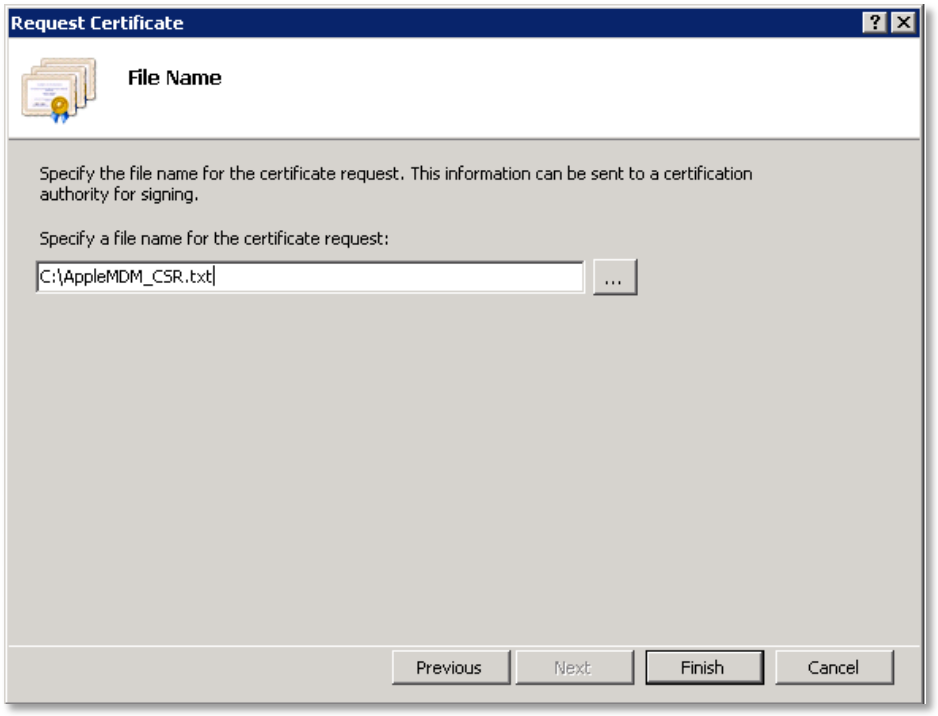
4. Enter the following in the ***Distinguished Name Properties*** window:
   - **Common name** – Enter a valid Apple ID. This does not need to be an Apple Developer account ID, but you should use an Apple ID that has been designated for managing the corporate APNs certificate. The Apple ID might be in the form of an email address, or possibly a display name.
   - **Organization** – The legal name of your organization
   - **Organization unit** – The department within your organization
   - **City/locality** – City in which your organization is located
   - **State/province** – Abbreviation for the state or province in which your organization is located
   - **Country/region** – Abbreviation for the country or region in which your organization is located



5. Select **Next**.
6. In the *Cryptographic Service Provider Properties* window, accept the default setting, **Microsoft RSA SChannel Cryptographic Provider**. In the **Bit length** field, select **2048** for the encryption level. Click **Next**.



7. In the *File Name* window, save the CSR to your computer. Record the location and filename. Click ***Finish***. This is the file you will upload to the *ZENworks Mobile Management Certificate Request Portal*.

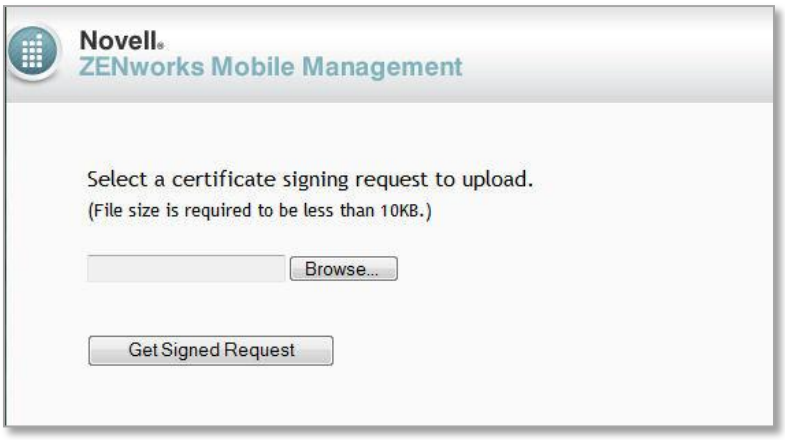


Uploading the CSR to the ZENworks Mobile Management Certificate Request Portal

The CSR file you generated by using IIS must be signed by Novell before you can upload it to the Apple Push Certificates Portal. You need:

- Access to the CSR file
- Your Novell login credentials

1. Navigate to the *ZENworks Mobile Management* Certificate Portal at: https://zmmupdate.novell.com/apn



2. Browse to select the CSR file.
3. Click **Get Signed Request**.
4. Save the signed request.

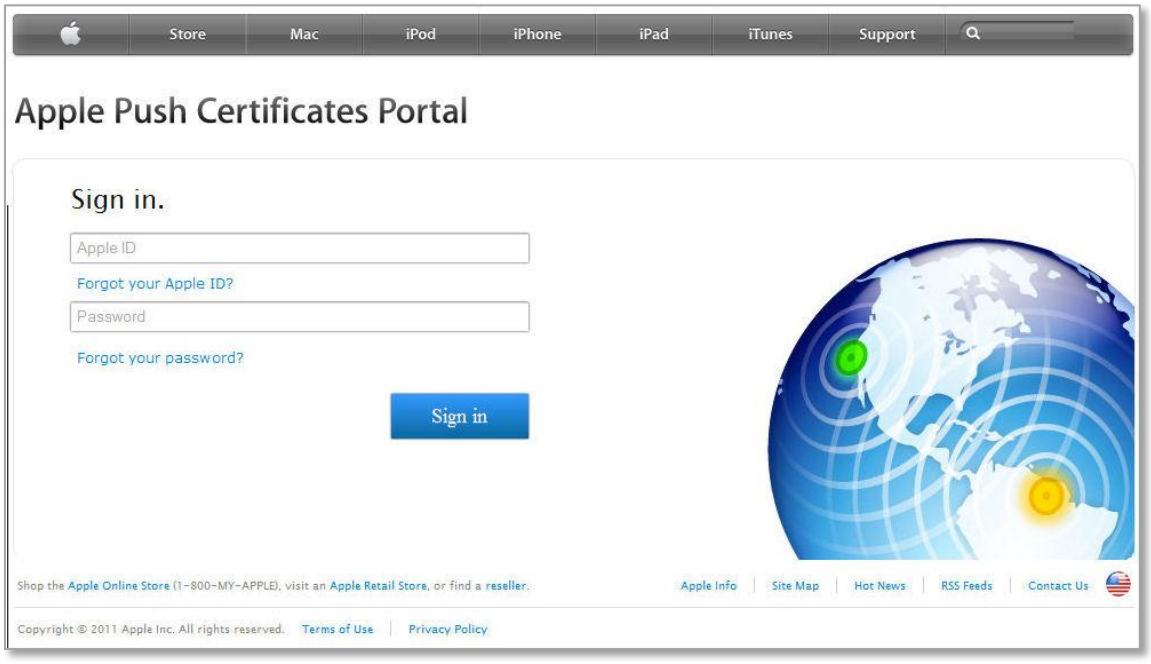
You are now ready to upload the signed ***ZENworks.request*** file (the intermediate certificate) to the Apple Push Certificates Portal.

Uploading the Intermediate Certificate to the Apple Push Certificates Portal

At the Apple Push Certificates Portal, you accept a license agreement and upload the intermediate certificate that you downloaded from the ZENworks Mobile Management Certificate Portal. A new Apple signed push certificate is created for you to download.

1. Browse to the Apple Push Certificates portal at: https://identity.apple.com/pushcert/ .

2. Log in by using your Apple ID and password. This does not need to be an Apple Developer account ID, but you should use an Apple ID that has been designated for managing the corporate APNs certificate.



3. Select **Create a Certificate**.

4. Read the *Terms of Use* and accept the End User License Agreement.

5. Select and upload the intermediate certificate you downloaded from the *ZENworks Mobile Management* Certificate Portal.

6. When the upload has finished, a new certificate for *ZENworks Mobile Management* appears. Select **Download** to download the Apple signed certificate.

You are now ready to complete the CSR and export the APNs certificate to the *ZENworks Mobile Management* server.

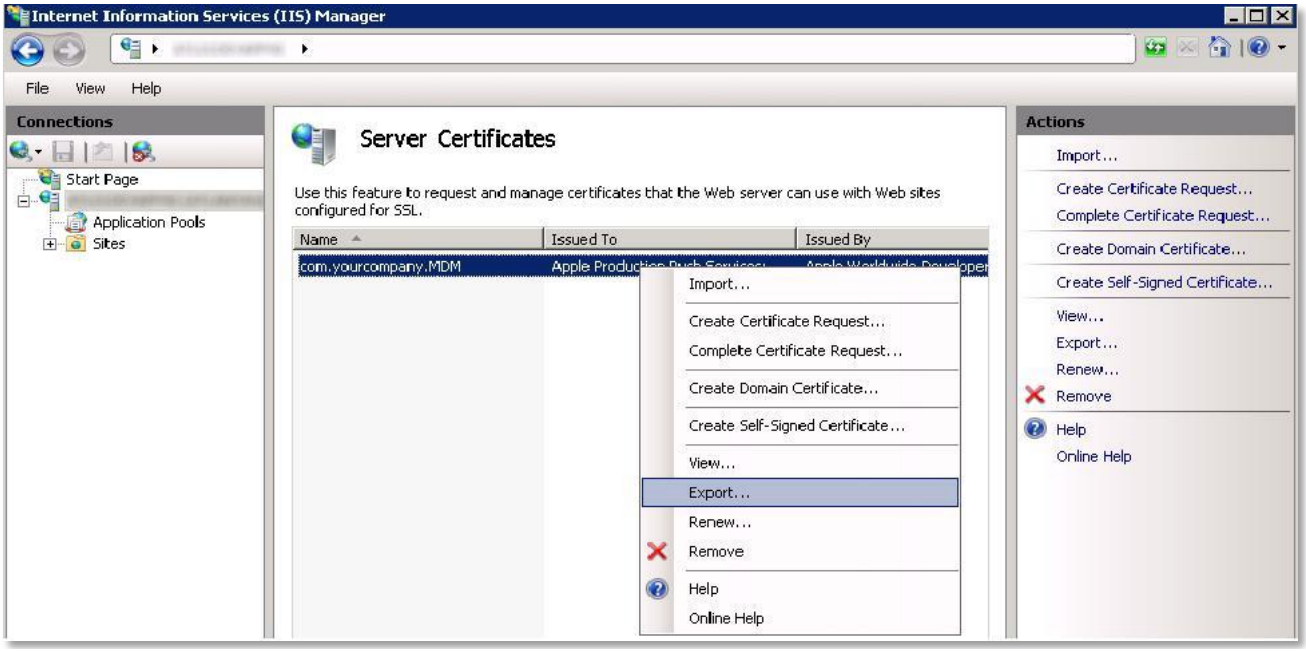
Completing the Certificate Request from IIS Manager 7 or 8

1. Return to **Internet Information Services (IIS) Manager** > **Server Certificates** and select **Complete Certificate Request** from the *Actions* menu in the right panel. This starts the Complete Certificate Request Wizard.

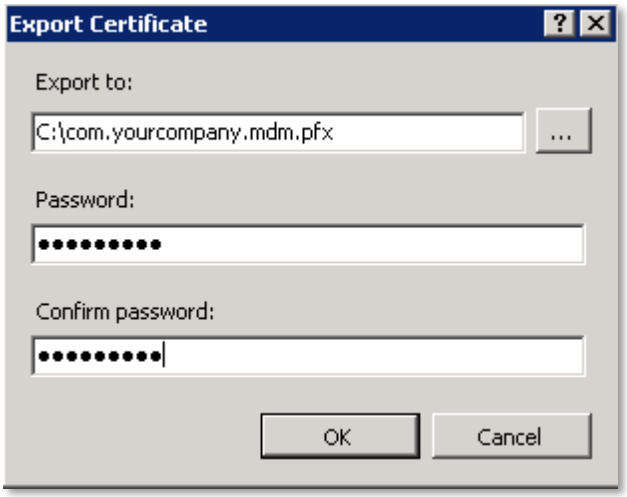
2. Browse to the *aps_production_identity.pem* file that was provided by Apple and enter a friendly name. This is simply a label you give the certificate to easily distinguish it. You might want to give it a name in which your company is identified.

3. Select **OK** to install the certificate to the server. You should see the certificate listed in the center panel of *Server Certificates*.

4. Export the certificate so that it can be uploaded to *ZENworks Mobile Management*. Right-click the certificate you just installed and select **Export**.



5. Save the file to your Desktop in the .pfx format. You must set a password. You will need this password when you upload the certificate to *ZENworks Mobile Management*.



You have successfully generated your APNs certificate.

Now you are ready to upload the certificate to *ZENworks Mobile Management*. You need the following:

- APNs certificate file (.pfx format)
- The password you set when exporting the certificate

Continue with **Upload the APNs Certificate to *ZENworks Mobile Management***.

Uploading the APNs Certificate to ZENworks Mobile Management

This section explains how to upload the APNs certificate to *ZENworks Mobile Management* by using the *ZENworks Mobile Management* dashboard. You need:

- APNs certificate file (the .pfx format)
- The password you set when exporting the certificate

1. Log in to the *ZENworks Mobile Management* dashboard and select the **System** view.
2. Select **Organization** from the left panel.
3. Click the **Upload** button next to the **APNs Certificate** field.

4. Click the **Browse** button, then navigate to and select the APNs certificate file (.pfx format).
5. In the **Certificate Password** field, enter the password you set when exporting the certificate.
6. Enter the ***Apple ID*** used to generate the certificate, if you want to display it for reference on the *Organization Settings* page. This information can be useful at renewal time.
7. Check the **Use Default URLs** box to populate the *Server URL* and *Check in URL* fields with https://<ServerAddress>/sync/iOSMDMSync.php. This is the required format of the URLs. Verify that the <*ServerAddress*> is the external address of the *ZENworks Mobile Management* server.

   Note: If you did not access the dashboard externally, do not use the default check box. Enter the *Server URL* and *Check in URL*s manually, in the format noted above.

8. Click the **Submit** button.

   After you have uploaded an APNs certificate, it appears under the APN Certificate field on the dashboard in the format com.apple.mgmt.<*random string*> (Enabled)

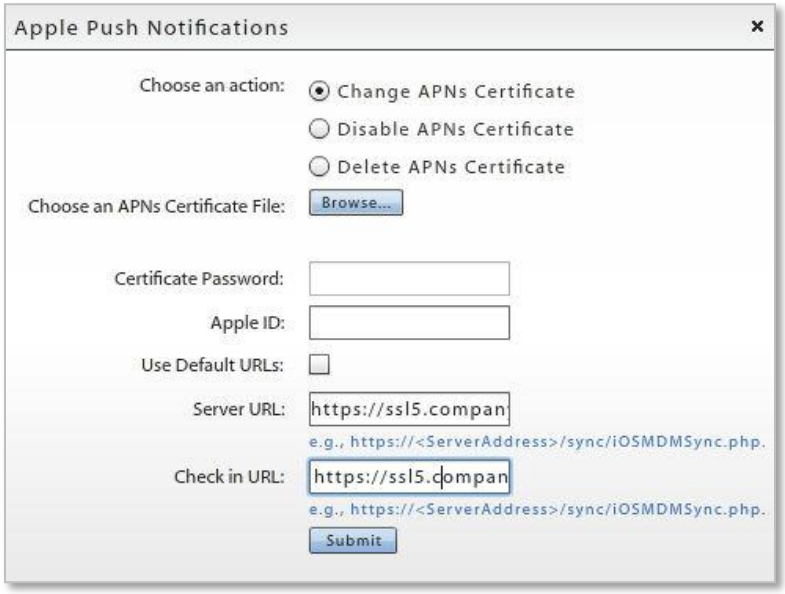
   Note: The APNs certificate must be renewed annually. The expiration date is displayed on the *Organization Settings* page. You can also use the *Test Now* button to check the certificate's validity. The test will return the certificate's activation and expiration dates.

9. Click **Save Changes** when you are finished.

Your *ZENworks Mobile Management* server is now able to trigger iOS devices with push notifications and use the built-in Apple MDM protocol.

Updating the APNs Certificate

1. Log in to the *ZENworks Mobile Management* dashboard and select the **System** view.
2. Select **Organization** from the left panel.
3. Click the **Edit** button next to the **APNs Certificate** field and make the needed changes. You can change/disable/delete the APNs certificate or edit the password, Apple ID, or URLs if necessary.



4. Click the **Submit** button.

5. Click **Save Changes** when you are finished.

   Tip: You might want to test APNs functionality after an update to the certificate by manually updating the APN profile on a device. Open *ZENworks Mobile Management* on an iOS device and tap ***Config*** > ***Load Configuration Profile***. The device installs the initial profile and, after a brief delay, it prompts for the user's Exchange password. If the prompt for Exchange credentials does not occur, resetting IIS might resolve issues preventing the APNs from processing.

Renewing an APNs Certificate

The Apple Push Notification service (APNs) certificate must be renewed annually. Organizations can keep track of the certificate's expiration date by setting an alert to occur prior to the date. The expiration date is also displayed on the *Organization Settings* page.

To set the APNs Certificate Expiration alert:

- From the ***Organization*** page select ***Compliance Manager*** > ***Alert Settings*** > ***System Alerts***.
- Enable the ***Apple Push Notification (APNs) Certificate Expiration*** alert and configure when you want the reminder to begin and how often to be reminded. The default settings are to issue the reminder 30 days prior to the expiration and repeat it every day.
- You can also choose to have an E-mail and/or SMS alert sent to an administrator.

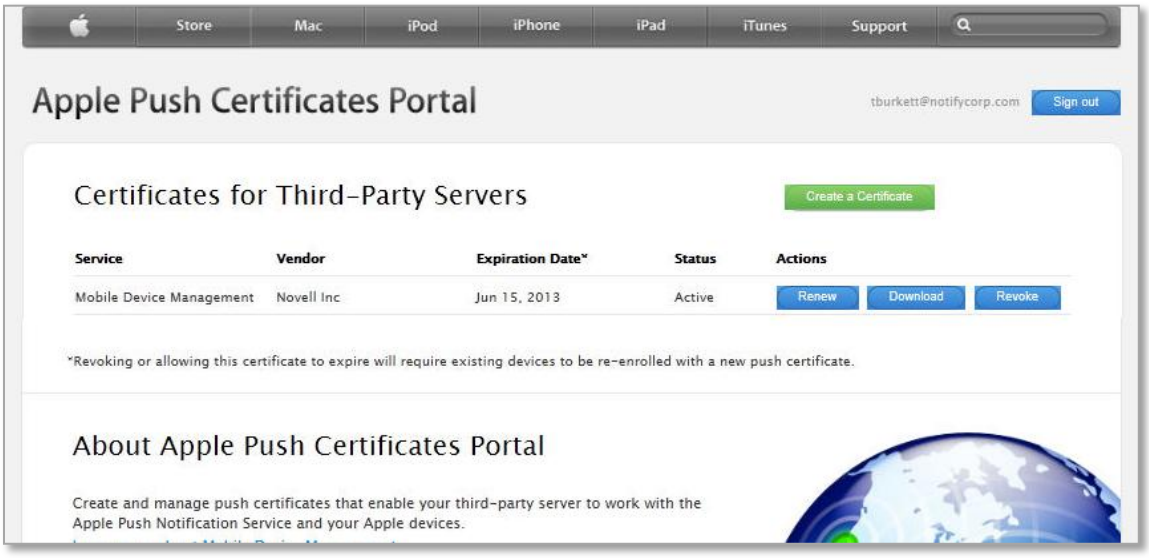
Follow the instructions below to renew the APNs certificate that was generated from the Apple Push Certificates Portal or from Apple's iOS Developer Enterprise Program (iDEP).

Essentially, you follow the same process used to obtain the original certificate. The only difference is in the steps taken on the Apple Push Certificates Portal (Steps 4-6 below.)

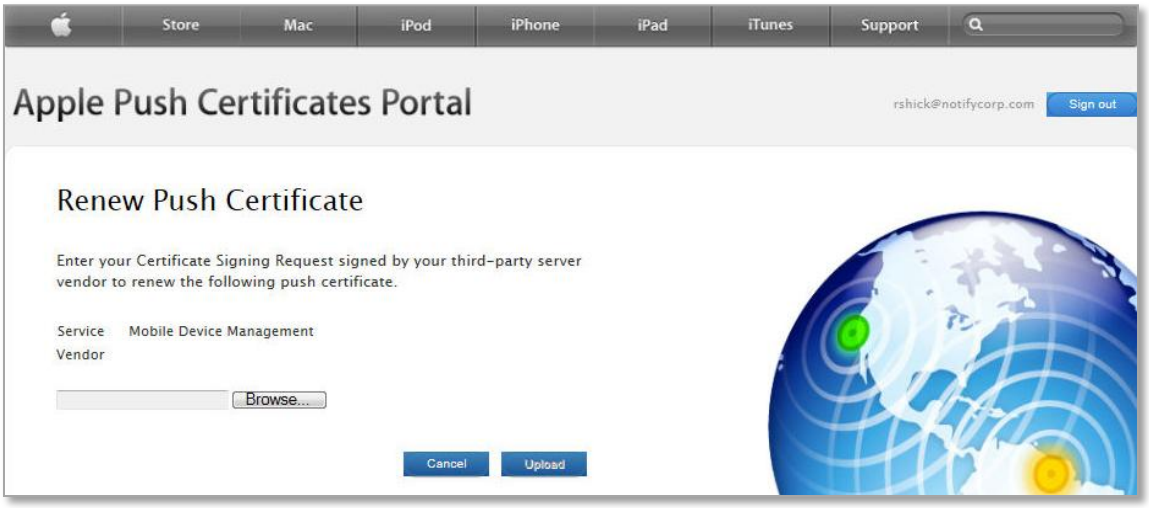
To renew an APNs certificate:

1. Create a new Certificate Signing Request (CSR) by using IIS Manager (See the complete instructions: IIS Manager 6 or IIS Manager 7/8)
2. Upload the CSR to Novell's ZENworks Mobile Management Certificate Request Portal. Click **Get Signed Request** and save the signed request file. See the complete instructions on page 22.
3. Go to the Apple Push Certificates Portal at https://identity.apple.com/pushcert/ .
    - If you originally obtained the certificate from the Apple Push Certificates Portal, log in with the Apple ID you used to generate the certificate.
    - If you originally obtained the certificate through iDEP, log in with the Apple ID for the iDEP Agent account.

4. On the page where your certificate is listed, click the **Renew** button next to the APNs certificate you are renewing.



5. On the *Renew Push Certificate* page, click the **Browse** button and select the .request file (a .plist format) to upload. Click **Upload.**



6. The page where certificates are listed displays the certificate with a new expiration date. Click the **Download** button next to the renewed certificate to download it and save it as a .pem file.
7. Use IIS to complete the CSR (See the complete instructions: IIS Manager 6 or IIS Manager 7/8)
8. From the *ZENworks Mobile Management* server dashboard, upload the renewed certificate.

   Select **System** > **Organization**.

   Click the **Edit** button next to the **APNs Certificate** field and choose **Change APNs Certificate**. (See complete instructions: *Updating the APNs Certificate*).

Appendix A: Generating the APNs Certificate Using OpenSSL

The following set of instructions can be used by those who do not want to use Internet Information Services (IIS) Manager or those who need an alternate method. These steps should work on any platform on which OpenSSL runs.

1. Install OpenSSL for Windows from http://slproweb.com/products/Win32OpenSSL.html.

2. From the command line, create the CSR and private key:

   ```
   openssl req -out apns.csr -new -newkey rsa:2048 -nodes -keyout apns.key
   ```

3. Enter the specified information with the Common Name set to your iTunes account name.

4. Follow the APNs signing instructions in this document to get the signed certificate (MDM_Novell Inc_Certificate.pem) from Apple.
   a. Uploading the CSR to the ZENworks Mobile Management Certificate Request Portal
   b. Uploading the Intermediate Certificate to the Apple Push Certificates Portal

5. Merge the key and the certificate to a .pfx file:

   ```
   openssl pkcs12 -export -out apns.pfx -inkey apns.key -in MDM_Novell
   Inc_Certificate.pem -certfile CACert.crt
   ```

6. Specify the password to be used to protect the private key.

7. Upload the APNs certificate file (in .pfx file format) to the ZENworks Mobile Management console. See Uploading the APNS Certificate to ZENworks Mobile Management, in this document.