Configuring Apple Push Notification Service for iOS Devices ZENworks. Mobile Management 3.0.x

January 2015



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.

Copyright © 2012-15 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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)	4
Generating an APNs Certificate	6
Generating an APNs Certificate from Windows Server 2003 Creating the Certificate Signing Request (CSR) from IIS Manager 6 Uploading the CSR to the ZENworks Mobile Management Certificate Request Portal	6
Uploading the Intermediate Certificate to the Apple Push Certificates P	ortal .9
Completing the Certificate Request from IIS Manager 6	
Generating an APNs Certificate from Windows Server 2008 or 2012 Creating the Certificate Signing Request (CSR) from IIS Manager 7 or Uploading the CSR to the ZENworks Mobile Management Certificate	818
Request Portal Uploading the Intermediate Certificate to the Apple Push Certificates P Completing the Certificate Request from IIS Manager 7 or 8	ortal21
Uploading the APNs Certificate to ZENworks Mobile Management	27
Applying an APNs Certificate to Multiple Organizations	29
Renewing an APNs Certificate	31
Appendix A: Generating the APNs Certificate Using OpenSSL	33

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

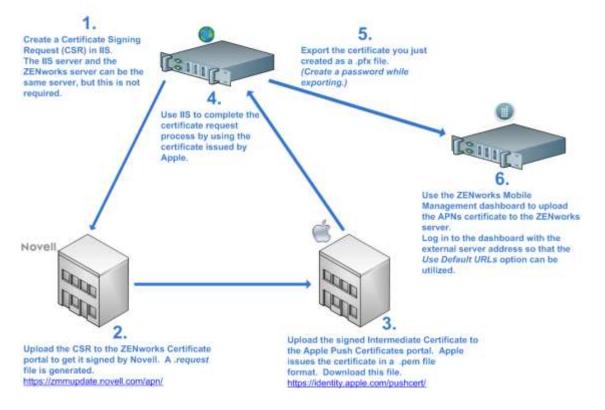
Requirements

- 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.
- 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 APNs Certificate

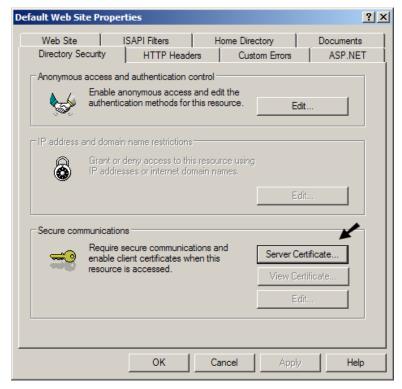
Generating an APNs Certificate from Windows Server 2003

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 <u>Generating an APNs Certificate from Windows Server 2008 or 2012</u>.

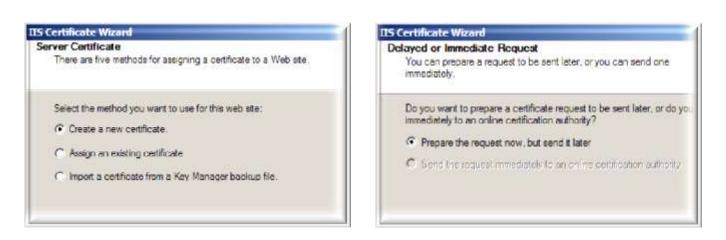
Note: <u>Appendix A</u> provides instructions for an alternate method of generating the APNs certificate using OpenSSL.

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.

IIS Certificate Wizard 🛛 🔀	IIS Certificate Wizard
Name and Security Settings Your new certificate must have a name and a specific bit length.	Available Providers The cryptographic providers you can use for your certificate are listed below
Type a name for the new certificate. The name should be easy for you to refer to and remember. Name: Image: I	Select a provider Microsoft DH SChannel Cryptographic Provider Microsoft RSA SChannel Cryptographic Provider
< <u>Back</u> Next > Cancel	

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

IIS Certificate Wizard 🛛 🗙	IIS Certificate Wizard
Organization Information Your certificate must include information about your organization that distinguishes it from other organizations.	Your Site's Common Name Your Web site's common name is its fully qualified domain name.
Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department. For further information, consult certification authority's Web site. Organization: Novell, Inc.	Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name. If the common name changes, you will need to obtain a new certificate. Common name: My AppleID
< <u>B</u> ack <u>N</u> ext > Cancel	< <u>B</u> ack <u>N</u> ext> Cancel

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**.

IIS Certificate Wizard	115 Certificate Wizard
Geographical Information The certification authority requires the following geographical information.	Certificate Request File Name Your certificate request is saved as a text file with the file name you specify.
Country/Region: US (United States) State/province: Utah City/Jocality: Provol State/province and City/Jocality must be complete, official names and may not contain abbreviations.	Enter a file name for the cotificate request. File name or AppleMDM_CSR td
< <u>B</u> ack <u>N</u> ext > Cancel	

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

Novell. ZENworks Mobile Management
Select a certificate signing request to upload. (File size is required to be less than 10KB.)
Browse
Get Signed Request
der ofgried nequest

- 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: <u>https://identity.apple.com/pushcert/</u>
- 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.

Ś	Store	Mac	iPod	iPhone	iPad	ITunes	Support	٩
ople P	Push Cer	tificates	s Portal					
Sign	in.							
Appin I	t)						-	
Forgot	your Apple 10?						6	-
Panner	P/4:							3
Forgot	your password?		Sign	in .			g.,	1
			- Cigar				- A	
							-11	(Or
the Apple Only	ne Store (1-800-699-8	VPXII, Hot on Apple	Retail Store, or find	a rateller.	Apal	with Strektop	Hot News	RSS Feeds Contact Us
un e tori à	Apple Inc. All rights re	arread. Terms of U	a Privacy Pul	-				

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.

Ś.	Store	Mac	iPod	iPhone	iPad	iTunes	5upport	a),
Apple	Push Cei	rtificate	s Portal				devisions	mithcorp.com
Upload	tte a New your Certificate Si to create a new pu	gning Request s		hind-party server				
Shop the Apple Child	ne Store (1-800-60)-#	rests were an Apple	Recall Shore, or Trul a	reation	Apple Int	e Site Map		Feeds Certain Us 👙
Conversion (Conversion)	Apple for All Symposis	aland. Terms of U	en Privacy Palle	ý.				

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.

15 Certificate Wizard	IIS Certificate Wizard
Pending Certificate Request A pending certificate request is a request to which the certification authority has not yet responded.	Process a Pending Request Process a pending certificate request by retrieving the file that contains the certification authority's response.
A certificate request is pending. What would you like to do? Process the pending request and install the certificate C Delete the pending request	Enter the path and file name of the file containing the certification authority's response. Path and file name: c:\aps_production_identity.pem Browse
	<u> ≪B</u> ack <u>N</u> ext > Cano

- 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**.

Add/Remove Snap-in	X Add Standalone Snap-in	? ×
Standalone Extensions	Available standalone snap-ins:	
Standalone Extensions Use this page to add or remove a stand-alone snap-in from the console. Snap-ins added to: Console Root	Snap-in Vendor Image: Stress of the st	
Description Add Remove	Component Services Microsoft Corporation Description The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer. <u>Add</u> <u>Close</u>	e
OK Cancel		

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

Certificates snap-in	×
This snap-in will always manage certificates for:	
O <u>M</u> y user account	
○ Service account	
Computer account	
Select Computer	×
Select the computer you want this snap-in to manage.	
This snap-in will always manage:	
• Local computer: (the computer this console is running on)	

Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

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

C Another computer:

Browse..

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.

🚡 Console Root\Certificates (Local Computer)\Personal\Certificates						
Console Root	Issued To \triangle	Issued By	Expiration Date			
En Certificates (Local Comp En En Certificates (Local Comp	Open Open	nmdmupgrade	7/6/2012			
	All Tas <u>k</u> s	• Open				
Enterprise Trust	Cut	Export				
	 Properties					
🕀 🧰 Trusted People	Help					
in						
	•		<u> </u>			
Contains actions that can be perfo	ormed on the item.		li.			

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

Certificate Export Wizard	X
Export Private Key	
You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
Do you want to export the private key with the certificate?	
Mes, export the private key	
\bigcirc No, do not export the private key	

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

Certificate Export Wizard	×
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
C DER encoded binary X.509 (.CER)	
C Bage-64 encoded X,509 (,CER)	
€ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
\square Include all certificates in the certification path if possible	
Personal Information Exchange - PKCS #12 (.PFX)	
\square Include all certificates in the certification path if possible	
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
Delete the private key if the export is successful	
< <u>B</u> ack <u>N</u> ext >	Cancel

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

Passy	word			
т	o maintain security, you must protec	t the private key by	using a password.	
т	ype and confirm a password.			
	Password:			

	Confirm password:			
	•••••			

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

ificate Export Wizard		
ile to Export		
Specify the name of the file you	i want to export	
Eile name:		
Eile name: C:\com.yourcompany.mdm.pf×	×	Browse
	×	Browse
	×	Browse
	< Back	

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 <u>Generating an APNs Certificate from Windows Server 2003</u>.

Note: <u>Appendix A</u> 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.

Act	ions
	Import
	Create Certificate Request
0.5	Complete Certificate Request
	Create Domain Certificate
	Create Self-Signed Certificate
?	Help
	Online Help

- 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

Request Certificate		? ×					
Distinguish	Distinguished Name Properties						
	nation for the certificate. State/province and City/locality must be specified cannot contain abbreviations.						
Common name:	My AppleID						
Organization:	Novell Inc						
Organizational unit:	TI						
City/locality	Provo						
State/province:	Utah						
Country/region:	US						
	Previous Next Finish Cano	el					

- 5. Select Next.
- 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.

equest Certifica	ate		? ×
Cry	ptographic Servic	e Provider Properties	
determines the However, a gre		and a bit length. The bit length of the trength. The greater the bit length, i ase performance.	
Microsoft RSA S	Channel Cryptographic P	Provider	
Bit length:			
2048			
		Previous Next	T Finish Cancel
		Previous Next	Cancer

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.*

Request Certificate	? ×
File Name	
Specify the file name for the certificate request, authority for signing.	This information can be sent to a certification
Specify a file name for the certificate request:	
C:\AppleMDM_CSR.txt	
,	
	Previous Next Finish Cancel

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

Novell. ZENworks Mobile Management
Select a certificate signing request to upload. (File size is required to be less than 10KB.)
Get Signed Request

- 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: <u>https://identity.apple.com/pushcert/</u>.

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.

	Store	Mac	iPod	iPhone	iPad	ITunes	Support	٩
ple P	ush Cer	tificates	Portal					
Sign	in.							
Appin ID	Þ						-	
Forgot	your Apple 10?						6	-
Pannen	r#:							7
Forgot	your password?						0	C Aller
			Sign	in			20	DE
							- 0	1000
hi Apple Onlin	w Store (1-800-69-A	Whill, sint an Apple	Retail Store, or find	a ratallar.	Apple	into See Map	Hot News	RSS Feeds Contact Us
un e tori à								

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.

Ś	Store	Mac	iPod	iPhone	iPad	ITunes	Support	٩
Apple	Push Ce	rtificate	s Portal				devisional	malifycary.com
Upload y	te a New your Certificate S to create a new pu	igning Request s ish certificate. Browse	Ligned by your t	- Cabine				h
	ne žisce (1-800-68)-a			e reseller	Apple Inf	Site Map		Streets Contact Us 🤤
annelight = 2013)	tight ter, All rights re-	in and Terms of U	ee. Privacy Pall	ev.				

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

 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.

Ac	tions
	Import
	Create Certificate Request
	Complete Certificate Request
	Create Domain Certificate
	Create Self-Signed Certificate
?	Help
	Online Help

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.

Complete Certificate Request	? 🗙
Specify Certificate Authority Response	
Complete a previously created certificate request by retrieving the f authority's response. File name containing the certification authority's response: C:\aps_production_identity.pem	1
Friendly name: com.yourcompany.mdm	
	OK Cancel

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*.

Export Certificate ? 🗙
Export to:
C:\com.yourcompany.mdm.pfx
Password:
•••••
Confirm password:
•••••
OK Cancel

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.

pple Push Notifications	X
Choose an APNs Certificate File:	Browse
Certificate Password:	
Apple ID: Use Default URLs:	
Server URL:	e.g., https:// <serveraddress>/sync/iOSMDMSync.php</serveraddress>
Check in URL:	e.g., https:// <serveraddress>/sync/iOSMDMSync.php</serveraddress>
	Submit

- 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 URLs* 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)

APNs Certificate: Edit Test Now com.apple.mgmt.External.abfd343b-473d-497d-a1ce-a624dc606ac1 (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.
- 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.

Apple Push Notifications	×
Choose an action:	Ochange APNs Certificate
	🔘 Disable APNs Certificate
	O Delete APNs Certificate
Choose an APNs Certificate File:	Browse
Certificate Password:	
Apple ID:	
Use Default URLs:	
Server URL:	https://ssl5.compan
	e.g., https:// <serveraddress>/sync/iOSMDMSync.php.</serveraddress>
Check in URL:	https://ssl5.compan
	e.g., https:// <serveraddress>/sync/iOSMDMSync.php.</serveraddress>
	Submit

- 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.

Applying an APNs Certificate to Multiple Organizations

If you have System Administrator privileges, you can apply an existing APNs certificate to multiple organizations on the *ZENworks Mobile Management* server.

For example, on-premise systems that have categorized various divisions of a company by creating multiple organizations will allow those organizations to share one APNs certificate.

- 1. Log in to the ZENworks Mobile Management dashboard and select the System view.
- 2. Select **Organization** from the left panel.

Edit

Test Now

 Scroll down to the *iOS Management* section of the *Organization Settings* page. Click on the link to the **System Settings** page under the *APNs Certificate* field. This option will not be available if you are not logged in as a system administrator.

APNs Certificate:

Go to System Settings to apply an APNs Certificate to multiple organizations.

You can also access *System Settings* directly by selecting **System > System Administration > System Settings**.

 On the System Settings page a list of organizations appears in the APNs Settings grid. If there is an APNs certificate associated with the organization, the Apple ID, Expiration Date, and Certificate Topic (certificate file) are listed beside it.

Organization Name	Apple ID	Expiration Date	Certificate Topic
Robin		Aug 21 2015 12:46PM	com.apple.mgmt.External.96dd653a-0735-4533-9be2-243b095d35f7
jmartin		Aug 21 2015 12:46PM	com.apple.mgmt.External.96dd653a-0735-4533-9be2-243b095d35f7
CAS	cschuster@ex07.notify	Aug 21 2015 12:46PM	com.apple.mgmt.External.96dd653a-0735-4533-9be2-243b095d35f7
Ninja			
jbyers		Aug 21 2015 12:46PM	com.apple.mgmt.External.96dd653a-0735-4533-9be2-243b095d35f7
arivera		Aug 21 2015 12:46PM	com.apple.mgmt.External.96dd653a-0735-4533-9be2-243b095d35f7
Archana		Aug 21 2015 5:46AM	com.apple.mgmt.External.96dd653a-0735-4533-9be2-243b095d35f7
cmclemore		Aug 21 2015 12:46PM	com.apple.mgmt.External.96dd653a-0735-4533-9be2-243b095d35f7

There are several functions you can perform from this grid.

- Set Up an APNs certificate for the first time for one or multiple organizations See also, <u>Generating an APNs Certificate</u> and <u>Uploading the APNs Certificate</u>.
- Renew an APNs certificate for one or multiple organizations (click Set Up) See also, <u>Renewing an APNs Certificate</u> and <u>Uploading the APNs Certificate</u>.
- **Disable/Enable** or **Delete** an APNs certificate for one or multiple organizations
- Copy an existing APNs certificate from one organization to one or multiple organizations (**Copy To**) *Caution:* Copying a certificate will overwrite any existing certificate associated with the organization(s) selected.

To select multiple consecutive organizations in the grid, hold the SHIFT key and click on the first and last organization.

To select multiple random organizations in the grid, hold the CTRL key and select organizations.

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.

Access Restrictions Alert Recipients	Alert Settings	Enabled	E-mail	SMS
Alert Settings	Access Restriction Based Alerts			
Device Platform Restrictions	Non-Access Restriction Based Alerts			
User Exceptions	Event Based Alerts			
Watch List	System Alerts			
	 Apple Push Notification (APNs) Certificate Expiration 	\mathbf{N}	(0)	(0) 🎝 🖸
	When the APNs certificate approaches its expiration date, an alert will be issued.			
	Reminder prior to expiration (Days): 30 Report Every (Days): 1			

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: <u>IIS Manager 6</u> or <u>IIS Manager 7/8</u>)
- 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 <u>complete instructions</u>.
- 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.**

	Store	Mac	Ped	Plane	Pad	กับระจ	Support	a 💦
Apple i	Push Ce	rtificate	s Porta				vista	nations and
Rene	w Push C	ertificate	2				-	
	or Certificate Sig o renew the follo			ird-party server				
Service Vendor	Mabile Device M	anagement					Q.,	AF
	6	Browse	-				FA	
			Center	Upper		100		P ON

- 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 <u>instructions: *Updating the APNs Certificate*).</u>

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. <u>Uploading the CSR to the ZENworks Mobile Management Certificate Request Portal</u>
 - 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

Note: If a certfile does not exist, the last parameter of this command (-certfile CACert.crt) can be dropped.

- 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 <u>Uploading the APNS Certificate to ZENworks Mobile Management</u>, in this document.