airwatch ™
mobile security
mobile device management
mobile application management

Generating an APNs Certificate for AirWatch MDM

Enabling iOS Mobile Device Management

airwatch ™

Table of Contents

Overview

Administrators of iOS devices must generate and upload an Apple Push Notification service (APNs) certificate in order to manage iOS devices. AirWatch helps iOS administrators quickly and easily complete this process by breaking it down into a few simple steps.

What is an APNs Certificate?

The Apple Push Notification service (APNs) is used to allow AirWatch to securely communicate to the smart device fleet over-the-air (OTA).

AirWatch uses the APNs certificate to send notifications to devices when the Administrator requests information or during a defined monitoring schedule. No data is sent through the APNs server, only the notification.
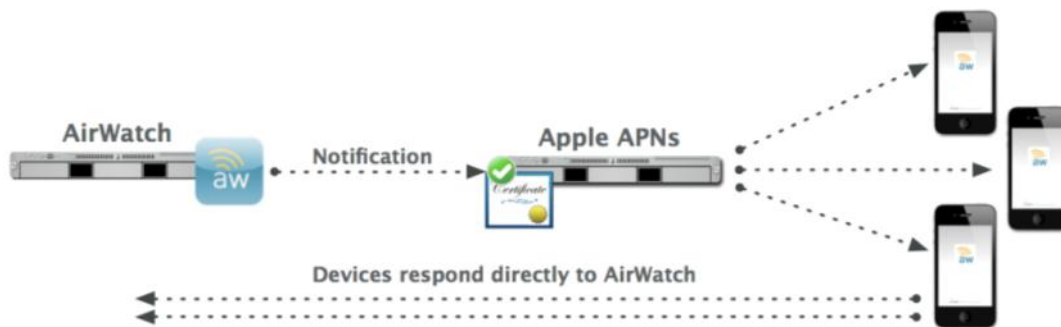
Generating an APNs Certificate for MDM

This document guides you through the process of generating your APNs certificate from Apple. There are two sets of instructions; one for creating an APNs certificate request from a Mac computer and one from a Windows server. You ONLY need to execute one or the other. They both follow the same general steps:

- Creating a Certificate Signing Request (CSR) from a Mac or Windows Server
- Signing the CSR using the AirWatch Certificate Portal
- Uploading the AirWatch-Signed CSR to the Apple Push Certificate Portal
- Completing the CSR and Exporting the APNs Certificate
- Uploading the APNs Certificate into AirWatch

Before you begin please ensure the following IT prerequisites:

- ☑ Mac OS X workstation or Windows Server with Administrator permissions
- ☑ Safari or Firefox Web browser

Generating an APNs Certificate from a Mac

The following instructions are for generating an APNs certificate using a Mac OS X workstation. For Windows Server instructions, skip this section and proceed to [Generating an APNs Certificate from a Windows Server](#).

Create a Certificate Signing Request

▶ First, you need to generate a certificate signing request. From your Mac, go to **Applications->Utilities->Keychain Access**

▶ Select the **login** Keychain from the left sidebar and **Certificates** for the category. From the top menu, select **Keychain Access->Certificate Assistant->Request a Certificate From a Certificate Authority**
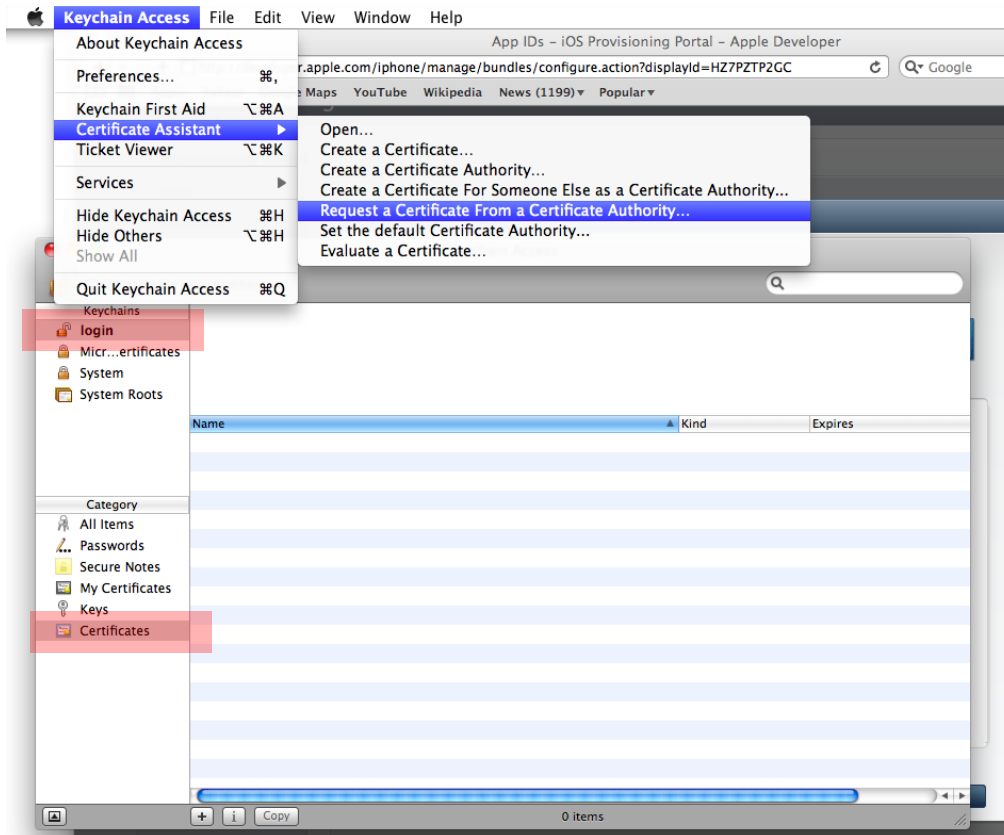
▶ The certificate wizard launches.

▶ Fill out the **Email Address** and **Common Name**. Select **Saved to disk** and select **Continue**
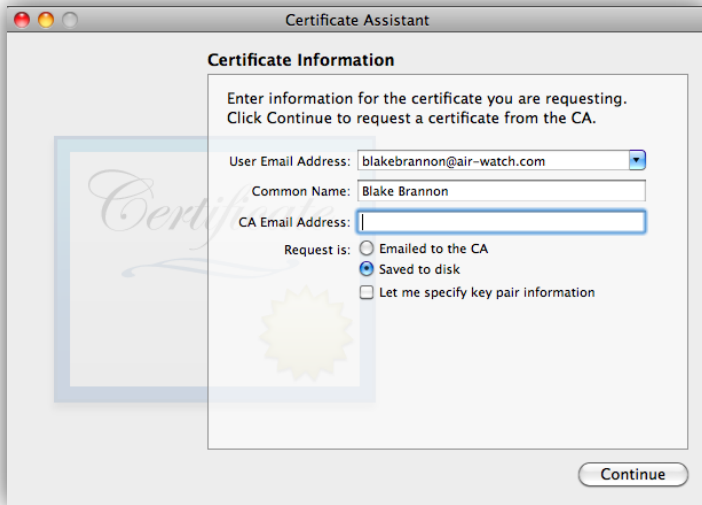
▶ Save the file to your desktop or somewhere convenient on your computer.
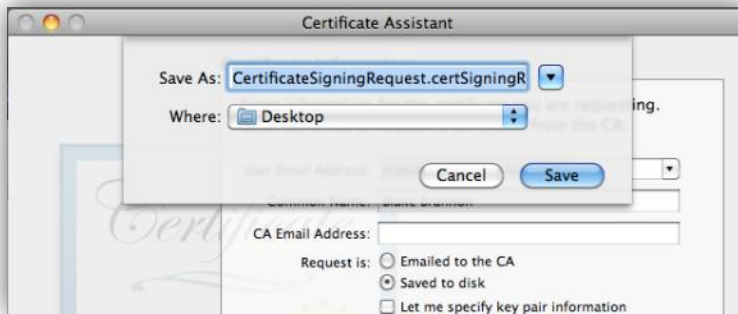
- **Note**: For a Mac, this is saved as a **.certsigningrequest** file. On a Windows Server, this is saved as a **.txt** file.

You have now created a CSR request and are ready to upload it to the AirWatch Certificate Portal.

Sign the CSR using the AirWatch Certificate Portal

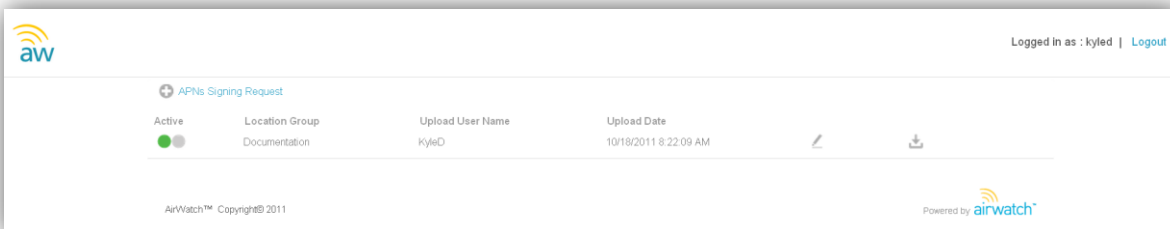▶ Navigate to the AirWatch Certificate Portal at https://awcp.air-watch.com/provisioningportal.

▶ Log in with your **AirWatch Certificate Portal Credentials** that have been provided to you in your Activation Email or through your AirWatch Representative.

- For any questions regarding the AirWatch Certificate Portal Credentials, please contact Support@Air-Watch.com

▶ Once logged in, select [APNs Signing Request] to open the APNs Signing Request form.

▶ Choose [Upload] then [Choose File] and select your previously generated .**CSR** file.

▶ Click [Save] twice to complete the APNs Signing Request.

▶ A new APNs Signing Request will be shown with the appropriate location group, user, and upload date of the CSR.
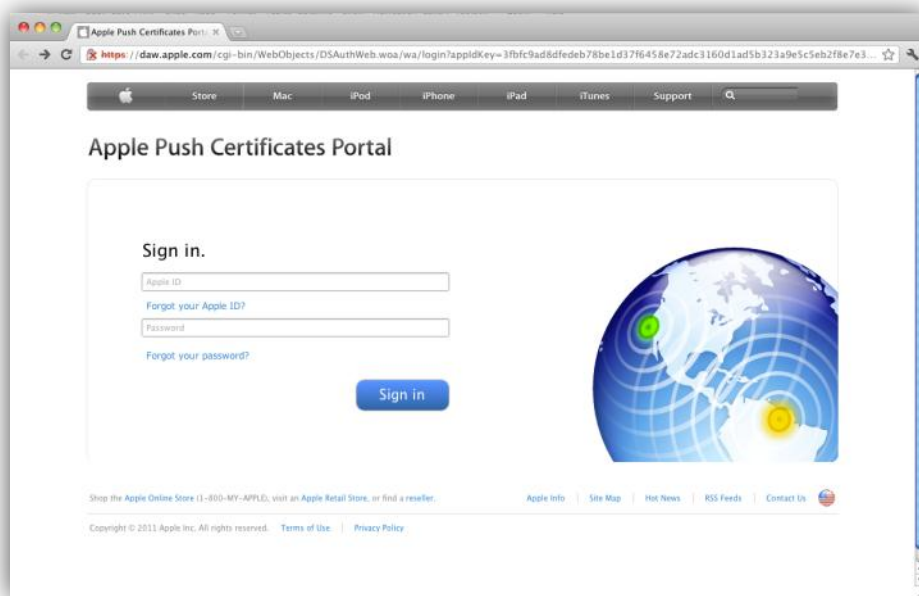

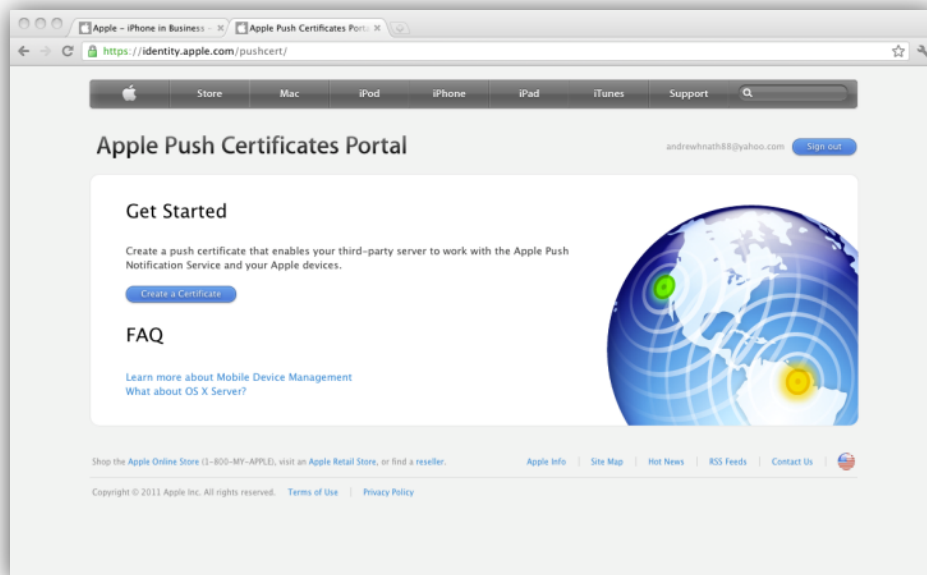▶ Select the download button to download your AirWatch-signed CSR.

You are now ready to upload your AirWatch-signed CSR to the Apple Push Certificate Portal.

Upload the AirWatch-Signed CSR to the Apple Push Certificates Portal

▶ Go to the Apple Push Certificates Portal website at https://identity.apple.com/pushcert/.

▶ Sign in using your Apple ID and password.

- This does not have to be an Apple Developer Account. It can be any AppleID.

- *Important Note: For production systems, it is strongly discouraged to use a personal apple id account. For long term maintainability, please create a new separate apple id to be used as a separate corporate apple ID for MDM, and tie it to an email account that will remain with the company even if the person who creates the account leaves the company.*

► Accept the EULA and proceed.

► Once logged in, choose **Create a Certificate** [Create a Certificate].

► Click **Browse** and upload the AirWatch-signed CSR downloaded from the AirWatch Certificate Portal.

► After uploading your CSR, a new Certificate for AirWatch MDM will appear.

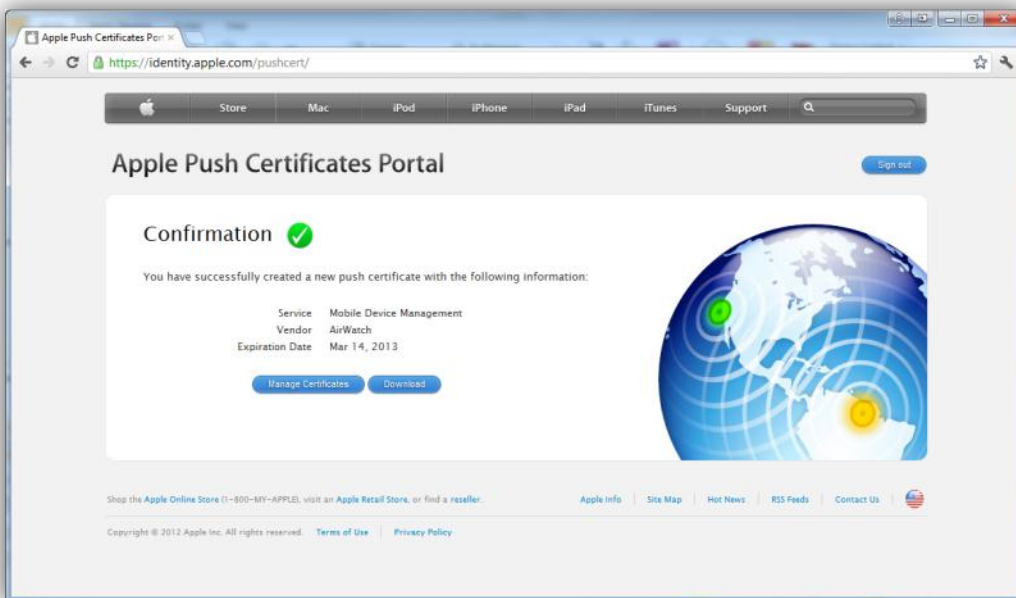► Select [Download] to download the Apple signed certificate (must be in the format of a .pem file).

You are now ready to complete the CSR and export the APNs Certificate.

airwatch™

Completing the CSR and Exporting the APNs Certificate

▶ Double-click the file to upload it to Keychain Access and complete the signing request.

▶ Verify that you can see your Apple Production Push Services certificate and it has an associate private key indented beneath it when you expand the left arrow.
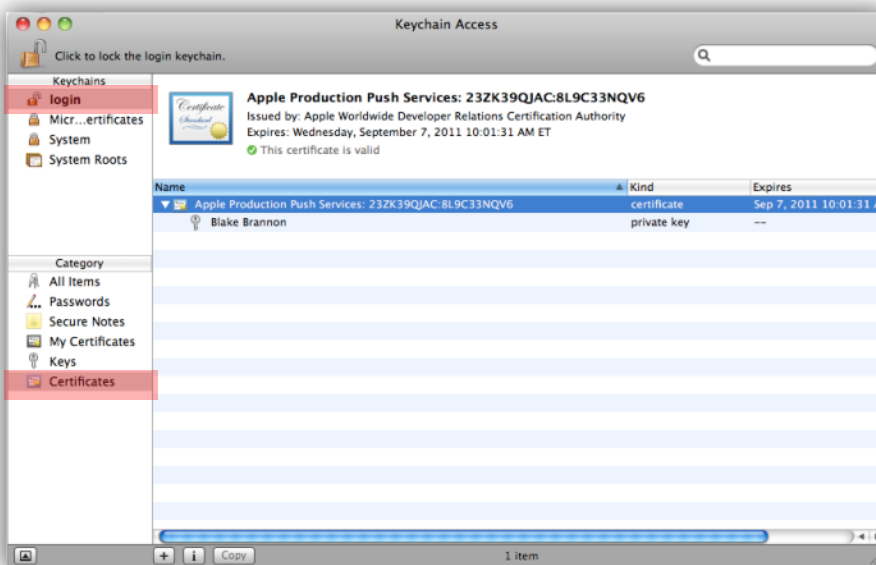
▶ *If you do not see your APNs certificate or the private key is not showing, verify you have the **login** keychain selected, the **Certificates** category selected and your certificate key has been expanded as show above. If you still do not see your certificate, repeat the generation process.

▶ Now you will need to export the APNs certificate so it can be uploaded to AirWatch. Right-click on the private key and select **Export**
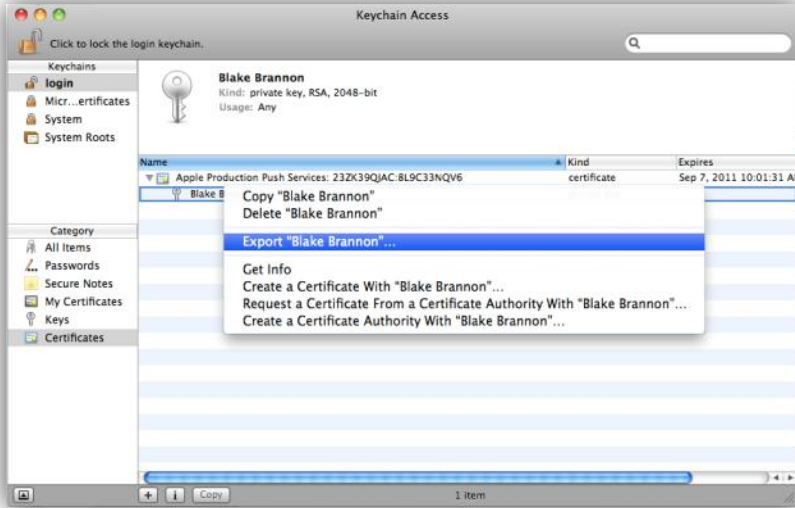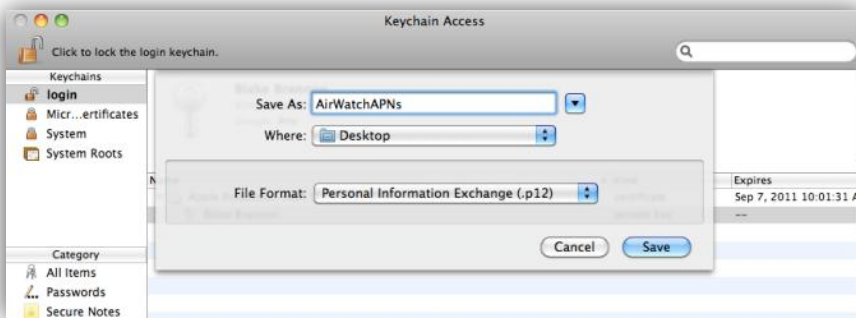

▶ Save the file to your Desktop in the **.p12** format.

▶ *If you only have the option to save as a **.cer** file rather than a **.p12** you are not correctly exporting the certificate. Ensure you screen looks exactly as pictured above and you are selecting the **private key** to export.

▶ When exporting the certificate you are required to set a password. Please take note of this as you will need it when uploading the certificate to AirWatch.

▶ You now have an APNs certificate. Upon completing this step you should have the following

● APNs certificate (**.p12 format** not .cer)

● The **password** you set when exporting the certificate

You are now ready to upload your certificate to AirWatch.

Generating an APNs Certificate from a Windows Server

The following instructions are for generating an APNs certificate from a Windows Server. This can be ANY Windows server and does not have to be done on the AirWatch server. If you have already generated your certificate from a Mac you can skip this section and upload your certificate to AirWatch.

Create a Certificate Signing Request

▶ Select Start→Administrative Tools→Internet Information Services (IIS) Manager.

▶ Select the server name.

▶ From the center menu, double-click the Server Certificates button in the Security section.
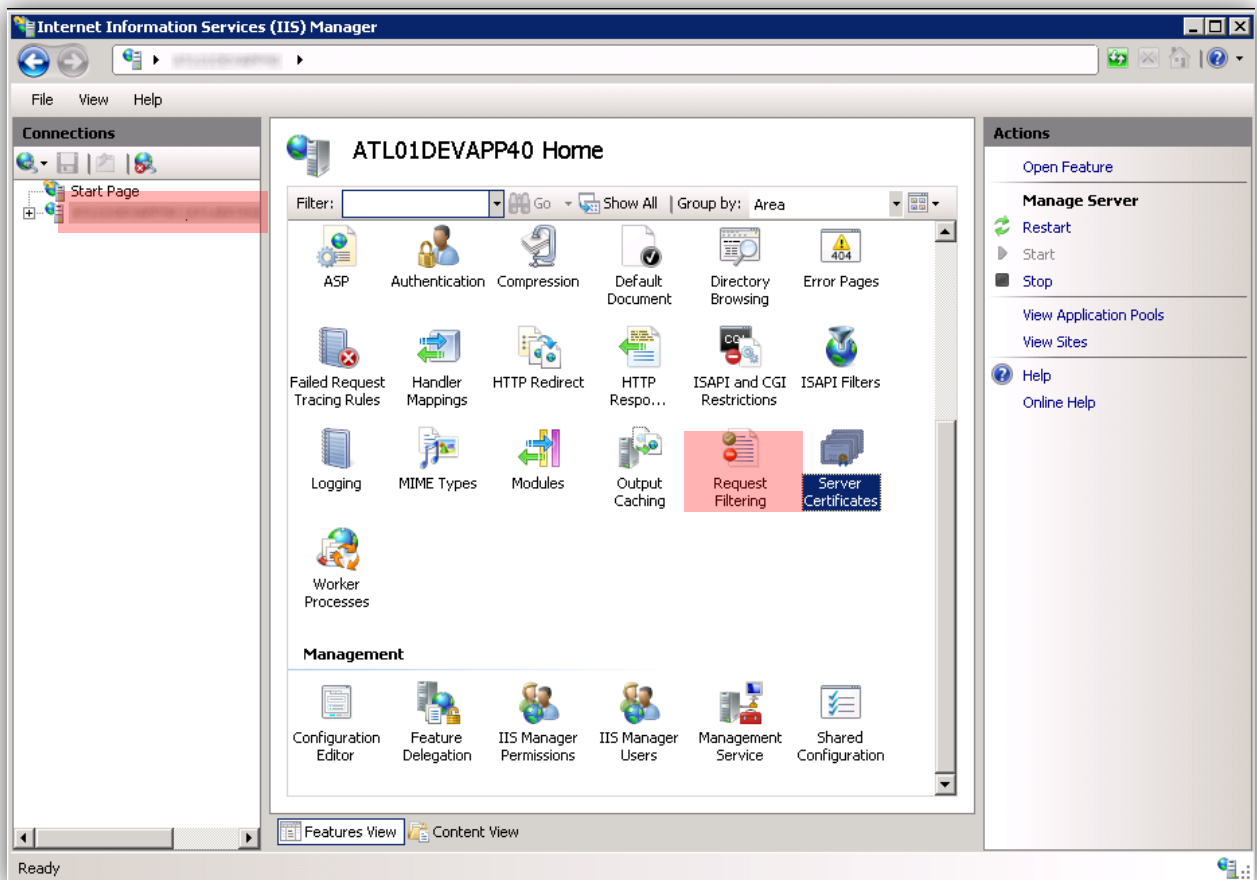
▶ Next, from the Actions menu on the right, select Create Certificate Request. This will open the Request Certificate wizard.
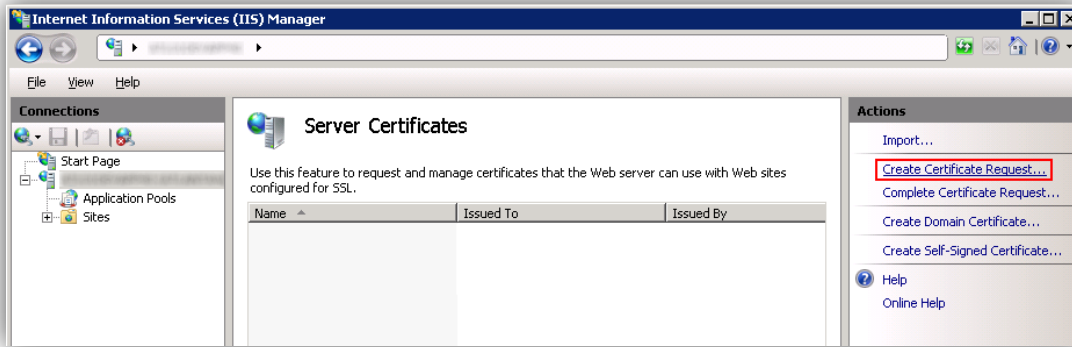

▶ In the Distinguished Name Properties window, enter the following

- Common Name - The name associated with the developer.

- Organization - The legally registered name of your organization/company

- Organizational unit - The name of your department within the organization

- City/locality - The city in which your organization is located

- State/province - The state in which your organization is located

- Country/region – The country in which your organization is located
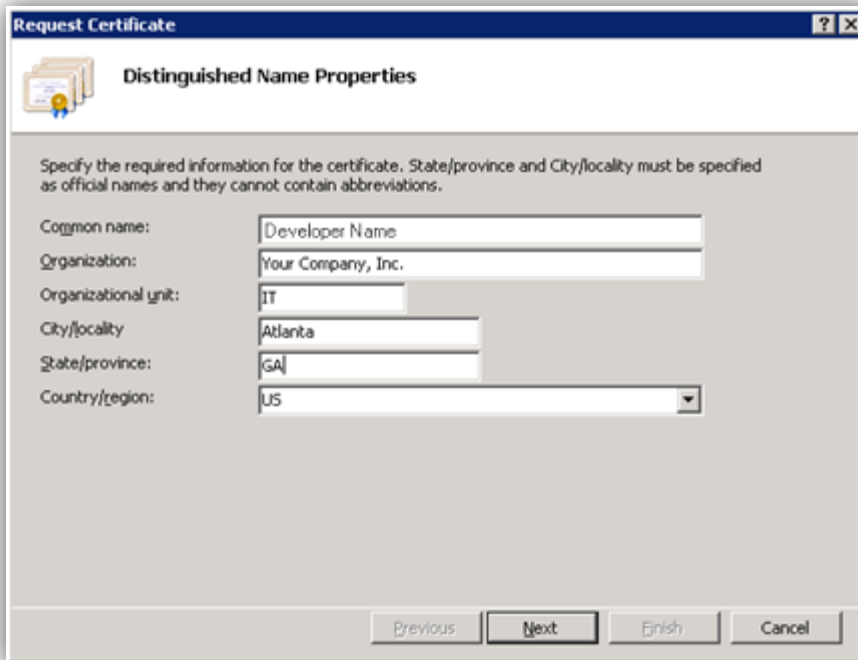
▶ Select Next

▶ In the Cryptographic Service Provider Properties window, select the following:

- Cryptographic service provider: Microsoft RSA SChannel

- Bit length: 2048
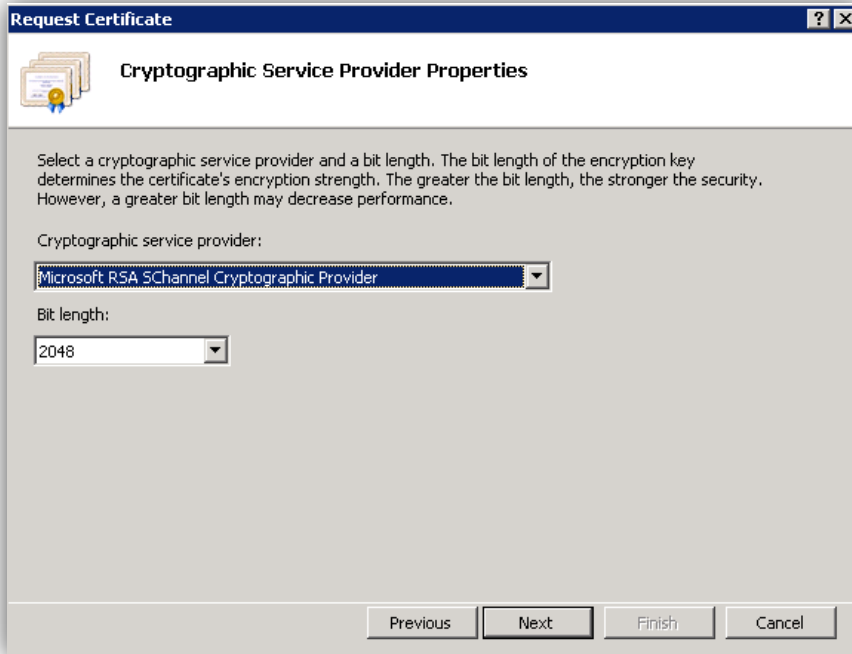
▶ Save the CSR to your desktop or another convenient location.
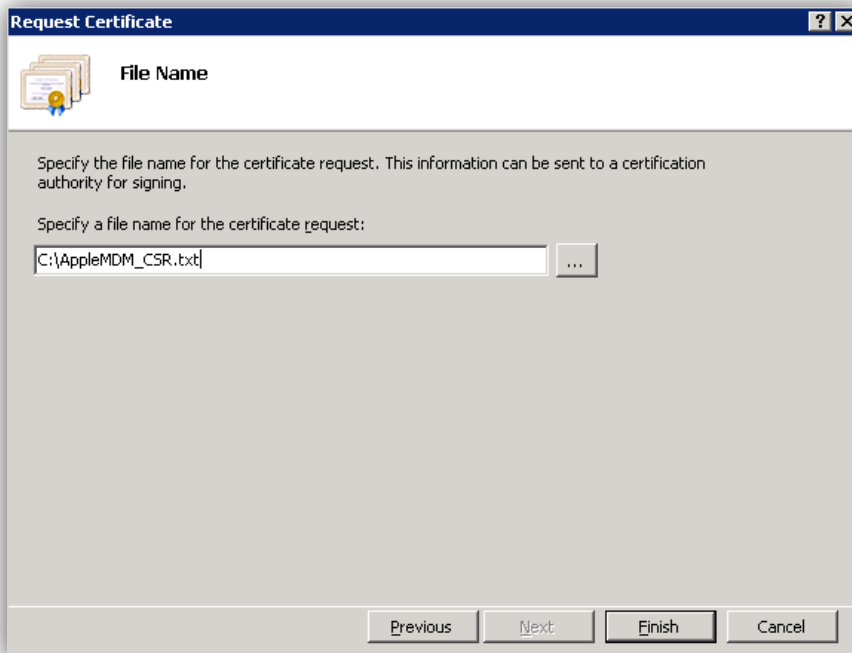
- **Note**: On a Windows Server, this is saved as a **.txt** file. For a Mac, this is saved as a **.certsigningrequest** file.

You have now created a CSR request and are ready to upload it to the AirWatch Certificate Portal.

Sign the CSR using the AirWatch Certificate Portal

▶ Navigate to the AirWatch Certificate Portal at https://awcp.air-watch.com/provisioningportal

▶ Log in with your **AirWatch Certificate Portal Credentials** that have been provided to you in your Activation Email or through your AirWatch Representative.

- For any questions regarding the AirWatch Certificate Portal Credentials, please contact Support@Air-Watch.com

▶ Once logged in, select [+ APNs Signing Request] to open the APNs Signing Request form.

▶ Choose [Upload] then [Choose File] and select your previously generated **.CSR** file.

▶ Click [Save] twice to complete the APNs Signing Request.

▶ A new APNs Signing Request will be shown with the appropriate location group, user, and upload date of the CSR.

▶ Select the download button [download icon] to download your AirWatch-signed CSR.

You are now ready to upload your AirWatch-signed CSR to the Apple Push Certificate Portal.

Upload the AirWatch-Signed CSR to the Apple Push Certificates Portal

▶ Go to the Apple Push Certificates Portal website at https://identity.apple.com/pushcert/.

▶ Sign in using your Apple ID and password.

- This does not have to be an Apple Developer Account. It can be any AppleID.

- *Important Note: For production systems, it is strongly discouraged to use a personal apple id account. For long term maintainability, please create a new separate apple id to be used as a separate corporate apple ID for MDM, and tie it to an email account that will remain with the company even if the person who creates the account leaves the company.*

▶ Accept the EULA and proceed.

▶ Once logged in, choose **Create a Certificate** .

▶ Click **Browse** and upload the AirWatch-signed CSR downloaded from the AirWatch Certificate Portal.

▶ After uploading your CSR, a new Certificate for AirWatch MDM will appear.

▶ Select [Download] to download the Apple signed certificate (must be in the format of a .pem file).

You are now ready to complete the CSR and export the APNs Certificate.

Completing the CSR and Exporting the APNs Certificate

▶ After you have copied the file to the Windows Server, go back to the **Internet Information Services (IIS) Manager->Server Certificates** and select **Complete Certificate Request** from the Actions menu on the right. This will open the Complete Certificate Request wizard.
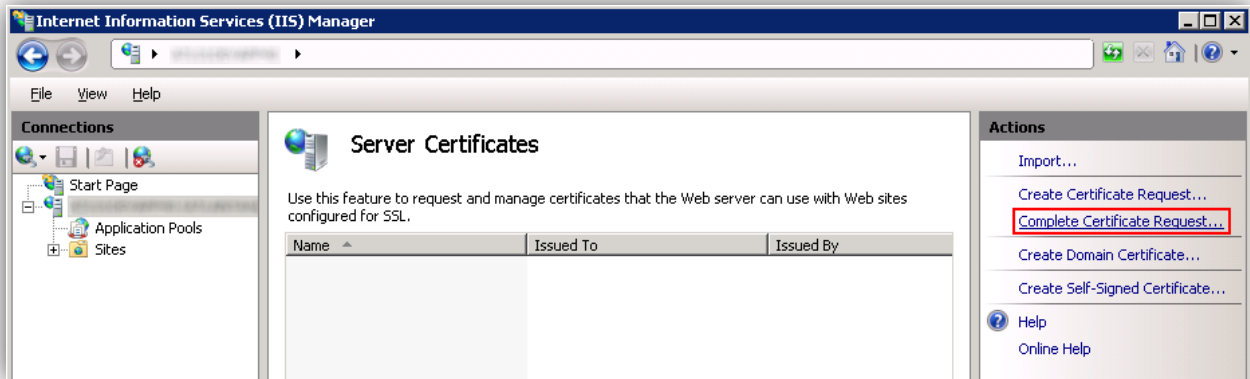

▶ Note: If you get an error downloading your certificate or completing the certificate request as described next, make sure to have an Apple Root Certificate Authority set on your server as a certificate chain needs to be built to a trusted root authority. Please ensure that the certificates given in the link below are present on your server: http://www.apple.com/certificateauthority/

▶ **Browse** to the .pem file that was provided to you from the Apple Push Certificates Portal and enter a friendly name.

▶ *The friendly name is not part of the certificate itself, but is used by the server administrator to easily distinguish the certificate. Call it **AirWatch MDM APNs**.
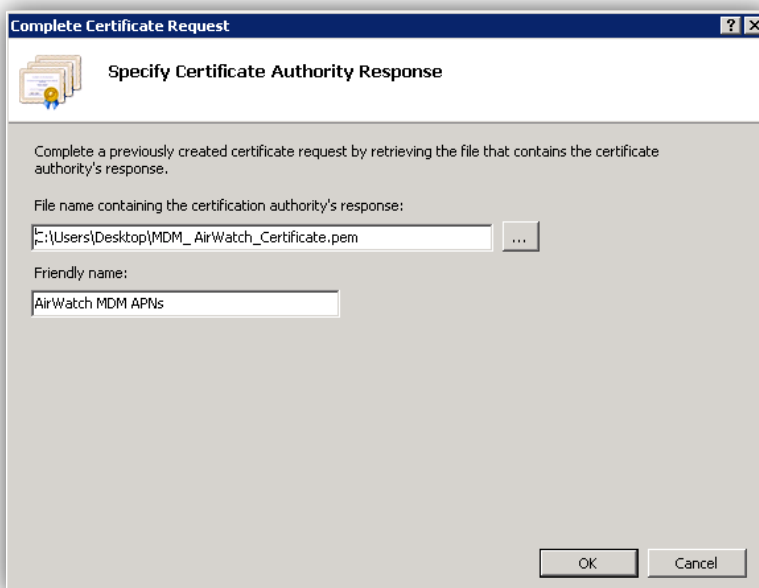
▶ Selecting **OK** will install the certificate to the server. You should now see the server listed in the Server Certificates section.

► Now you will need to export the APNs certificate so it can be uploaded to AirWatch. Right-click on the **certificate** that you just imported and select **Export**.
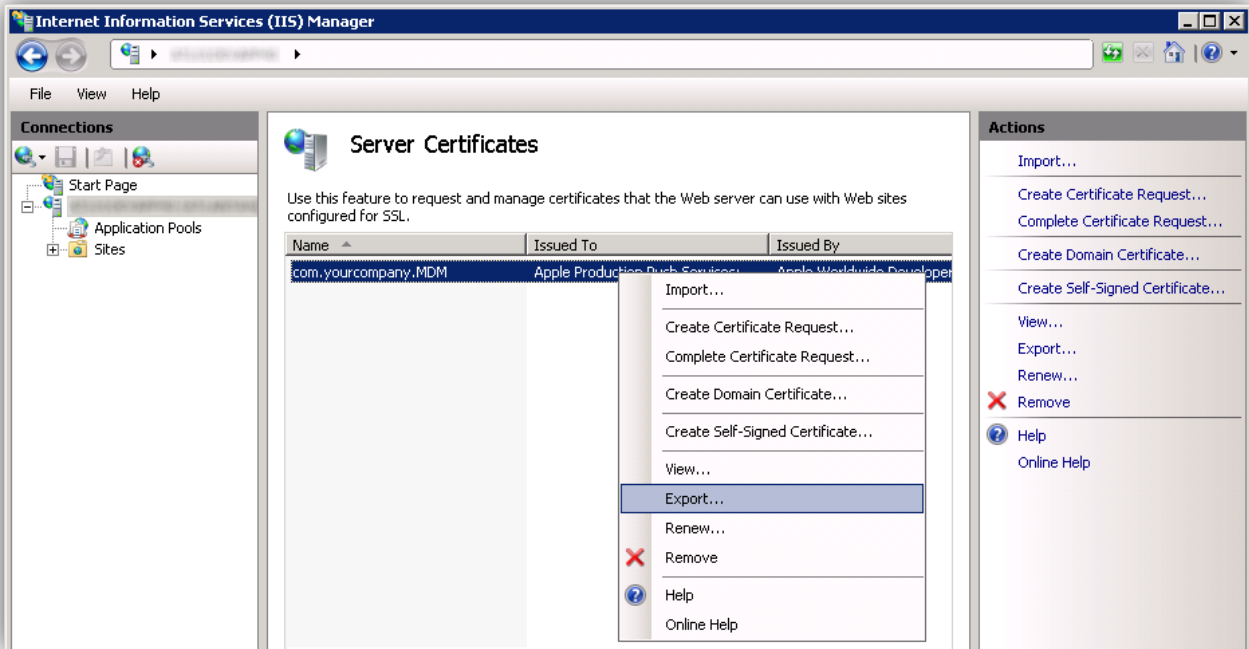
► Save the file to your Desktop in the **.pfx** format. When exporting the certificate you are required to set a password. Please take note of this as you will need it when uploading the certificate to AirWatch.

► *If you only have the option to save as a **.cer** file rather than a **.pfx** you are not correctly exporting the certificate. Ensure you screen looks exactly as pictured above and you are selecting the correct certificate to export.
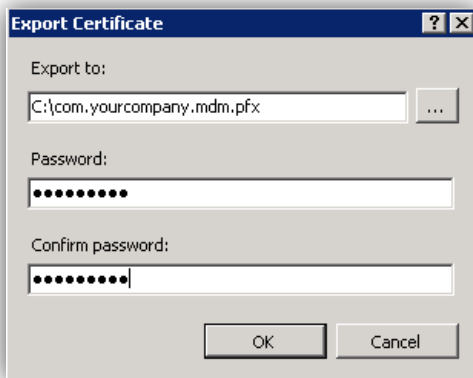
► You now have an APNs certificate. Upon completing this step you should have the following

- APNs certificate (**.pfx** format not .cer)

- The **password** you set when exporting the certificate

You are now ready to upload your certificate to AirWatch.

Uploading an APNs Certificate to AirWatch

You should now have your APNs certificate and are ready for uploading to AirWatch. This section will explain how to upload you APNs certificate to AirWatch so you can start managing your iOS devices.

Before you begin please ensure you have the following

☑ APNs certificate file (**.pfx** or **.p12** format not .cer)

☑ The **password** you set when exporting the certificate

☑ AirWatch web console URL, username and password

If you do not have any Web Console credentials, please contact support@air-watch.com

▶ Using your browser, navigate to your AirWatch environment. **Login** with your assigned username and password.

- *Your URL and login information was provided to you via activation email or from your AirWatch representative.

▶ From the top navigation select **Menu→Configure→System Settings**
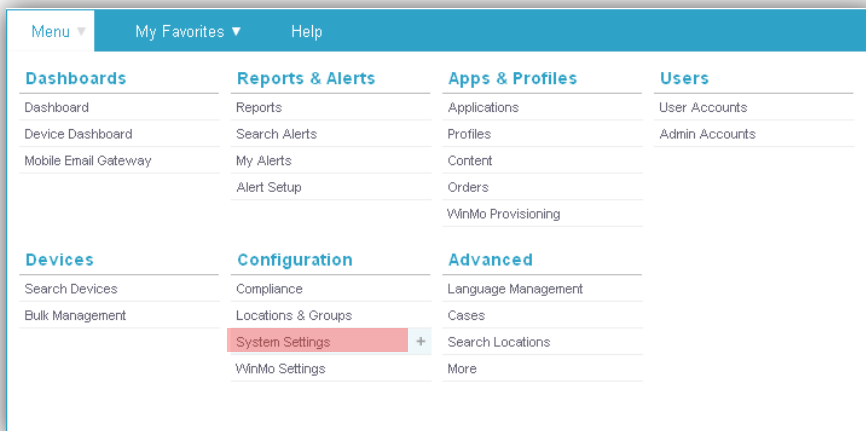
▶ Select your **top** Location Group (may only be one)
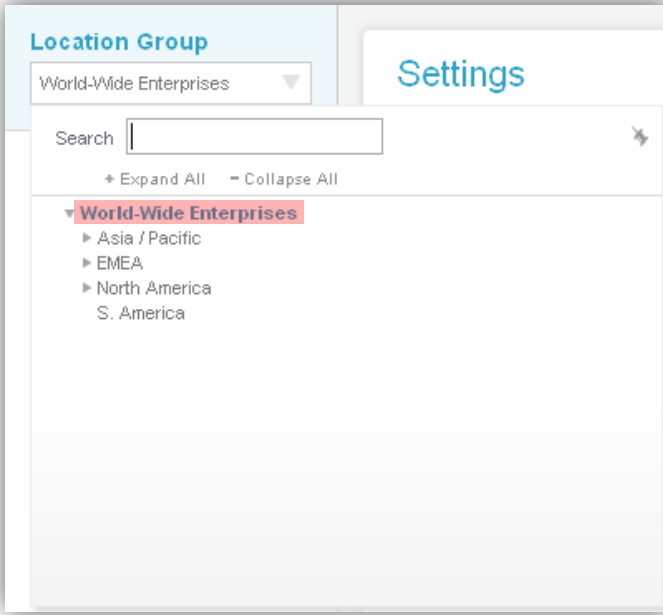
▶ Select **Device→iOS→APNS For MDM** from the left menu

▶ From the APNS settings page, check the **Enabled** combo box and select **Override** if not already selected
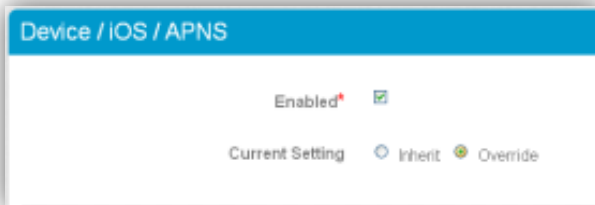
▶ Click the **Upload** button and select your new certificate file
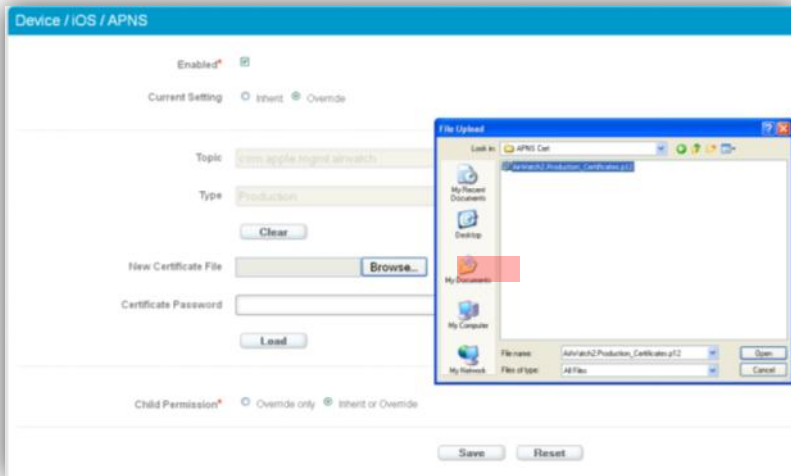
▶ Type in the **Certificate Password** you previously set for your APNs certificate when exporting it
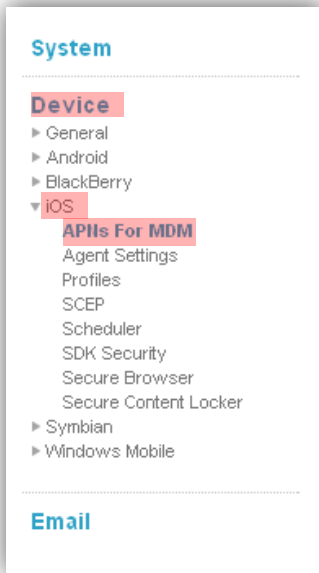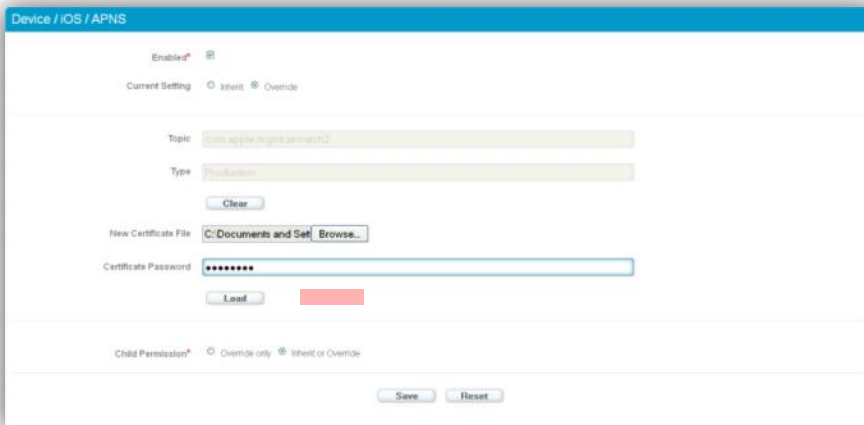

▶ Select **Load**. You will now see the Topic (Bundle ID) listed in the box below.
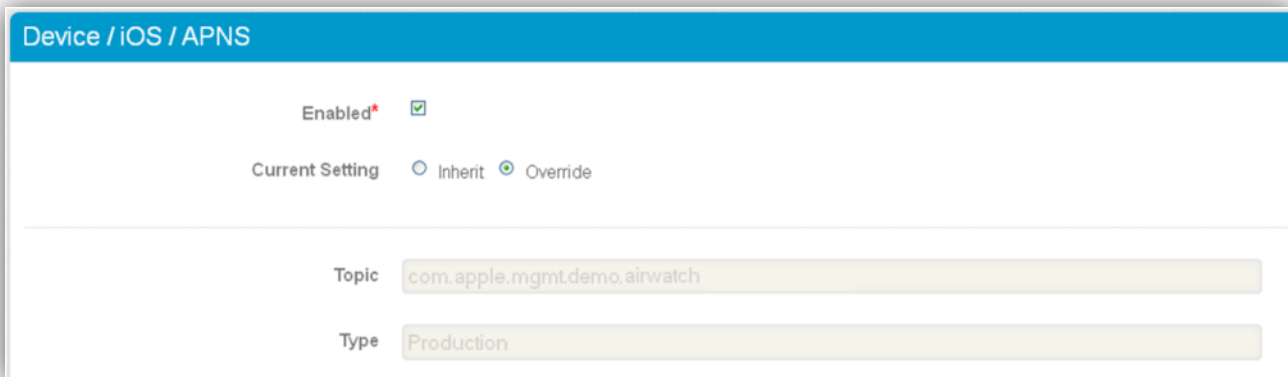
▶ Select **Save.**

Congratulations! You have successfully generated an APNs certificate and uploaded it to AirWatch. You can now continue proceed with managing your iOS devices.

FAQ

What are the allowed sources of the APNs certificate request?

The APNs certificate request can come from any server. The certificate request doesn't need to come only from the server that has AirWatch installed on it.

I cannot export a .p12 or .pfx file.

If you are trying to export your APNs certificate from your computer and it will only let you save as a .cer file you are not exporting the right file type. A .p12 or .pfx contains both the public and private key pair which is required by AirWatch to communicate with the APNs server. Is you are using a Mac, verify you have selected **Certificates** from the Categories list in the key chain. If you still have the problem repeat the process from scratch deleting all existing files and certificates.

AirWatch is failing to upload my APNs certificate.

If you are getting an error trying to upload your APNs certificate to AirWatch, please verify it is in the .p12 or .pfx format and you are typing the correct password set when exporting the certificate. If you still are having problems, verify the certificate is not corrupt by trying to install it on a Windows or Mac workstation by double-clicking the file. If the problem persists, contact AirWatch technical support at support@air-watch.com.

Why does AirWatch say my APNs Topic is invalid?

As of iOS 4.X Apple requires MDM providers to use topics in the notation "com.apple.mgmt.*" where the "*" is a wildcard that can be anything. This allows Apple to isolate APNs traffic from MDM messages and those to traditional iOS Apps. To prevent you from uploading a certificate with a non-compliant topic, AirWatch checks the certificate you upload and displays the "invalid" error if it doesn't match the Apple standards.

Why do you need an Apple APNs certificate?

Apple requires that each organization maintain their own certificate to ensure a secure mechanism for their corporate devices to communicate across Apple's push notification messaging network.

What if I want to use AirWatch's Software as a Service infrastructure?

The requirement is the same. Regardless of whether your organization deploys in AirWatch's SaaS environment, an appliance or in premise, your AirWatch MDM environment and all communication with your organization's devices will be validated based upon your organization's APNs certificate.

Do we need a certificate for a trial?

Yes. In order to manage any of your organization's devices, AirWatch is required to use your organization's specific APNs certificate. AirWatch does not have the ability to provide a "demo" or temporary certificate for testing.

airwatch™