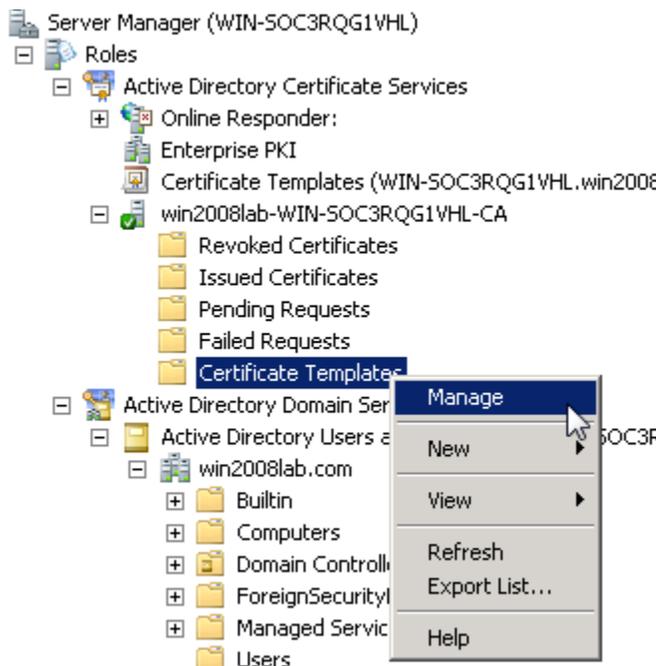


How to issue a certificate using Microsoft Windows 2008 certificate server for Aruba Instant

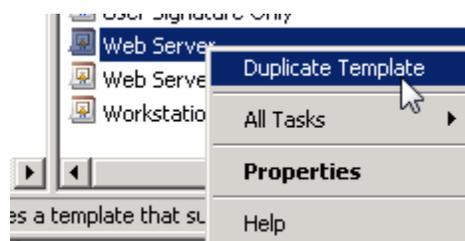
This document describes how to setup the Windows 2008 server with certificate services installed to issue certificate with exportable private key. The Aruba Instant does not support CSR generation and hence the certificate server must allow the private to be exported. The Aruba Instant version 6.1.2.3_2.0.0.0 is used for lab verification purpose. The certificate is required when setting up 802.1x with Radius server or Internal server.

Step 1: Create a new certificate template which allows the private key to be exported.

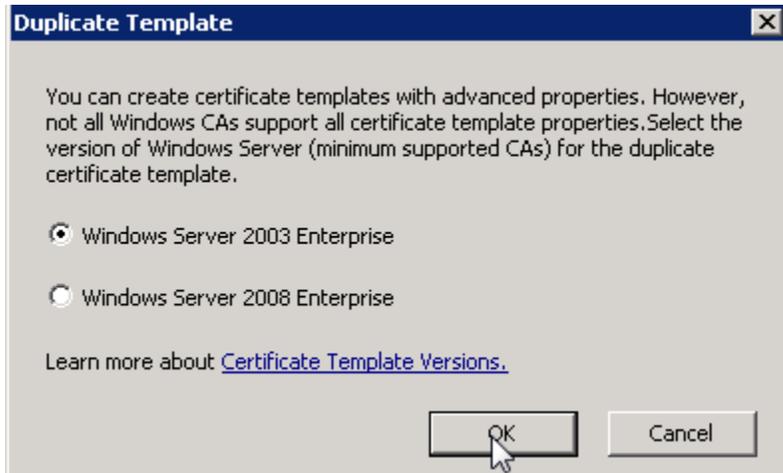
Open the Server Manager -> Roles -> Active Directory Certificate Services -> Click on the + next to the server name -> Certificate Templates -> Right click and select Manage



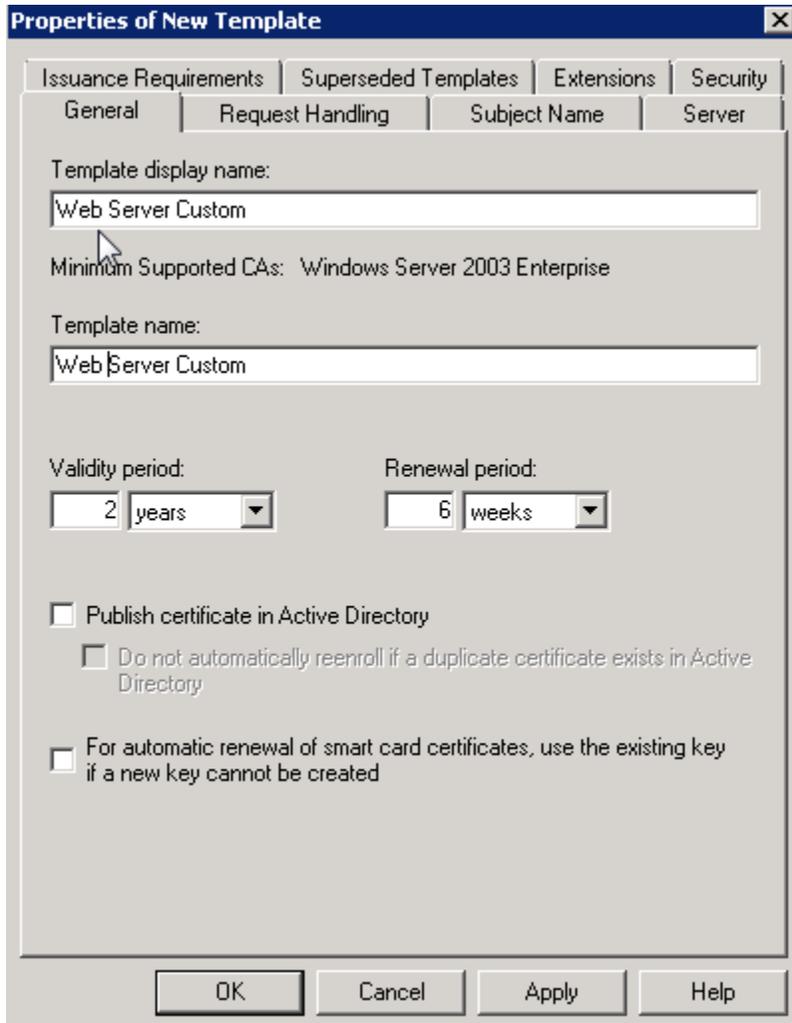
Step 2: Select the Web Server default template and click on Duplicate Template



Step 3: Click OK



Step 4: Type the Template Name



The screenshot shows the 'Properties of New Template' dialog box with the 'General' tab selected. The 'Template display name' and 'Template name' fields both contain 'Web Server Custom'. The 'Validity period' is set to 2 years and the 'Renewal period' is set to 6 weeks. There are three unchecked checkboxes: 'Publish certificate in Active Directory', 'Do not automatically reenroll if a duplicate certificate exists in Active Directory', and 'For automatic renewal of smart card certificates, use the existing key if a new key cannot be created'. The dialog has 'OK', 'Cancel', 'Apply', and 'Help' buttons at the bottom.

Properties of New Template [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name | Server

Template display name:
Web Server Custom

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name:
Web Server Custom

Validity period: 2 years [v]
Renewal period: 6 weeks [v]

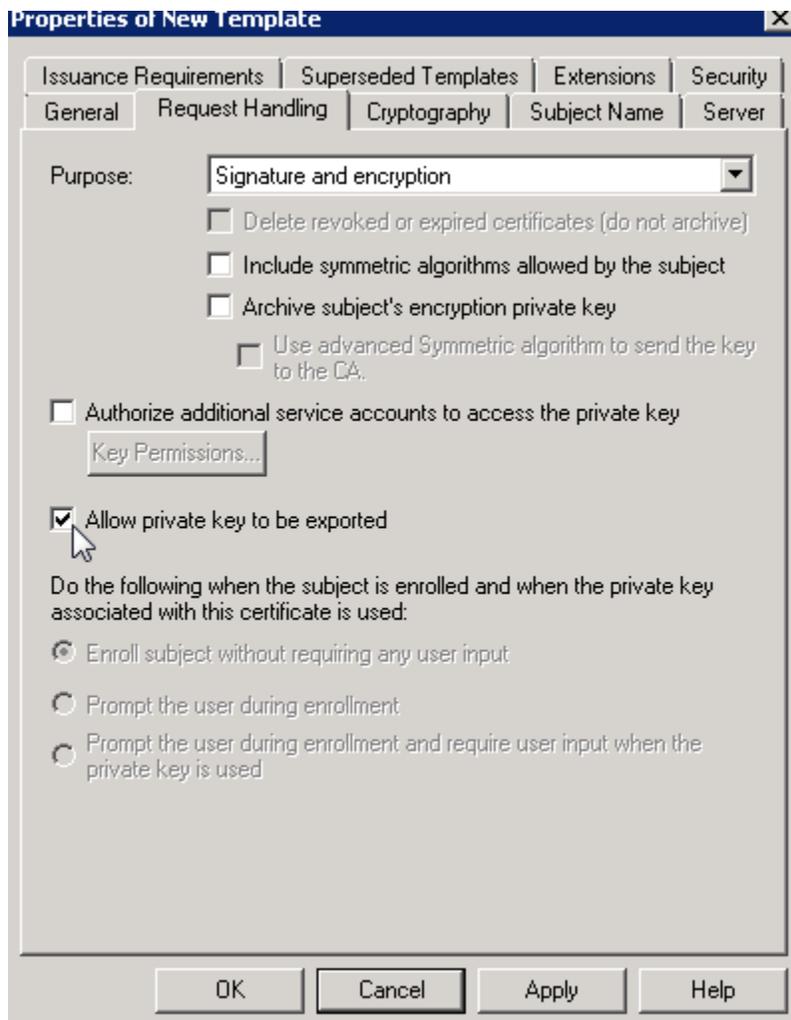
Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

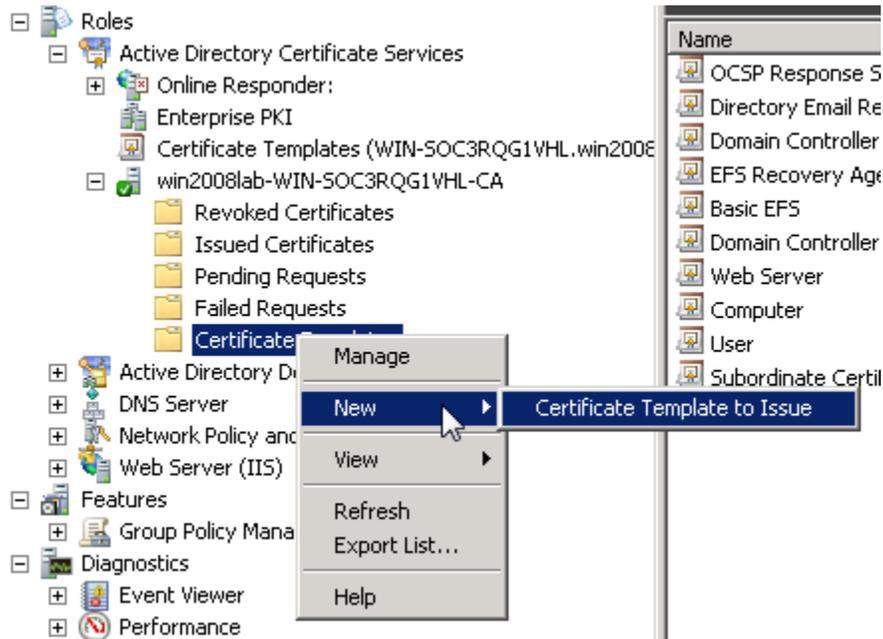
OK Cancel Apply Help

Step 5: Click on Request Handling and click on Allow private key to be exported

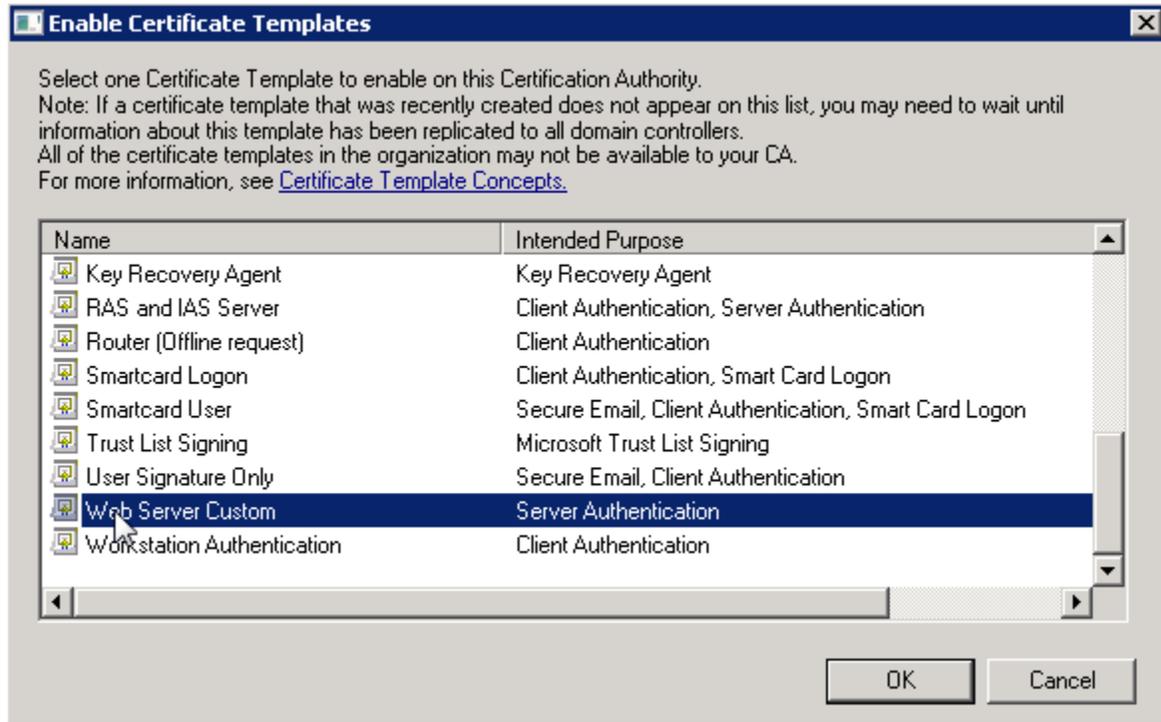


Step 6: Need to enable the template.

Select certificate template -> Right click -> Select New -> Certificate Template to Issue

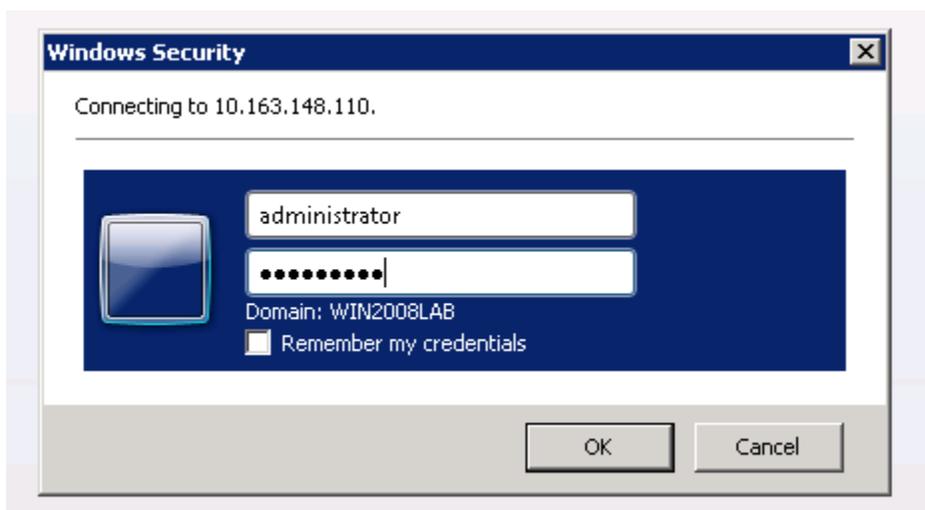


Step 7: Select the new template created and click OK



Step 8: Open the Browser and connect to the certificate server enrollment web page. You must login as administrator or equivalent in privileges in order to see the newly created template.

Example: <https://10.163.148.110/certsrv/>



Step 9: Click on Request a certificate

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Step 10: Click on advance certificate request

Request a Certificate

Select the certificate type:

[User Certificate](#)

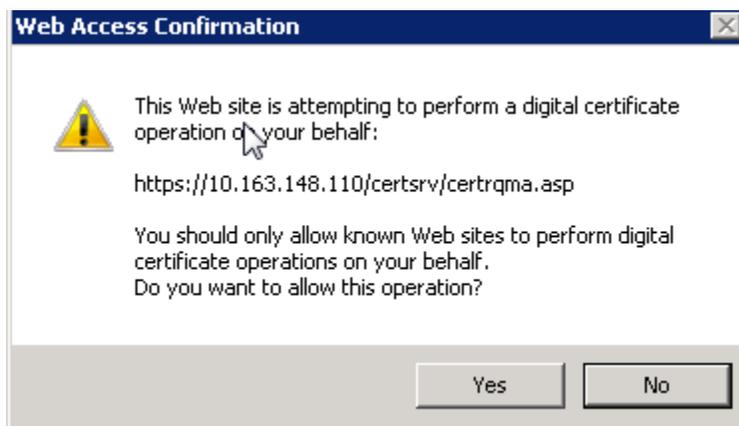
Or, submit an [advanced certificate request](#).

Step 11: Click on Create and Submit request to this CA. When prompted on Web Access Confirmation, click OK

Advanced Certificate Request

The policy of the CA determines the types of

[Create and submit a request to this CA.](#)



Step 12: On the Certificate Template drop down -> Select the newly created template -> Fill in all the required information -> Click Submit

Advanced Certificate Request

Certificate Template:

Web Server Custom

Identifying Information For Offline Template:

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Key Options:

Create new key set Use existing key set

CSP:

Key Usage: Exchange

Key Size: Min: 2048 Max: 16384 (common key sizes: [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name User specified key container name

Mark keys as exportable

Enable strong private key protection

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm:

Only used to sign request.

Save request

Attributes:

Friendly Name:

Step 13: Click Yes on Web Access Confirmation



Step 14: Click in Install this certificate

Certificate Issued

The certificate you requested was issued to you.

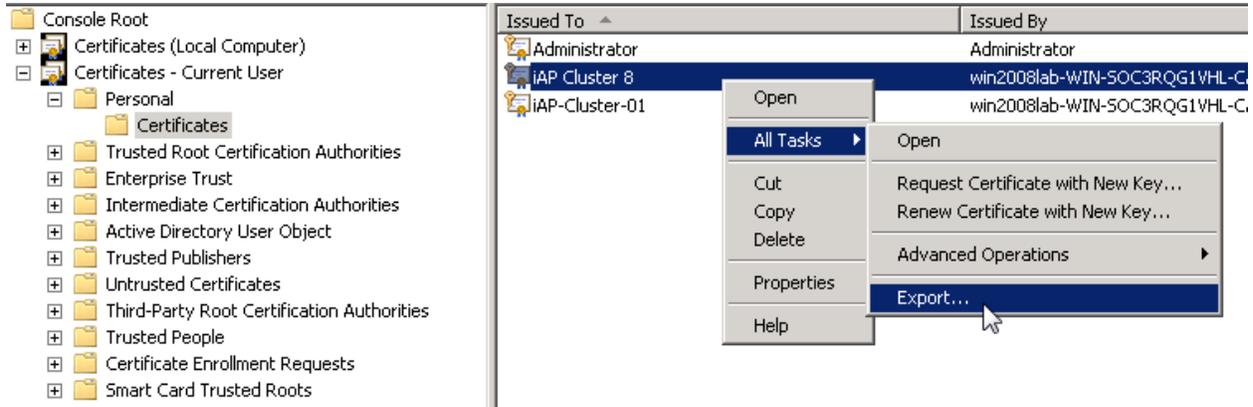


Step 15: The certificate is now install into your local certificate store.

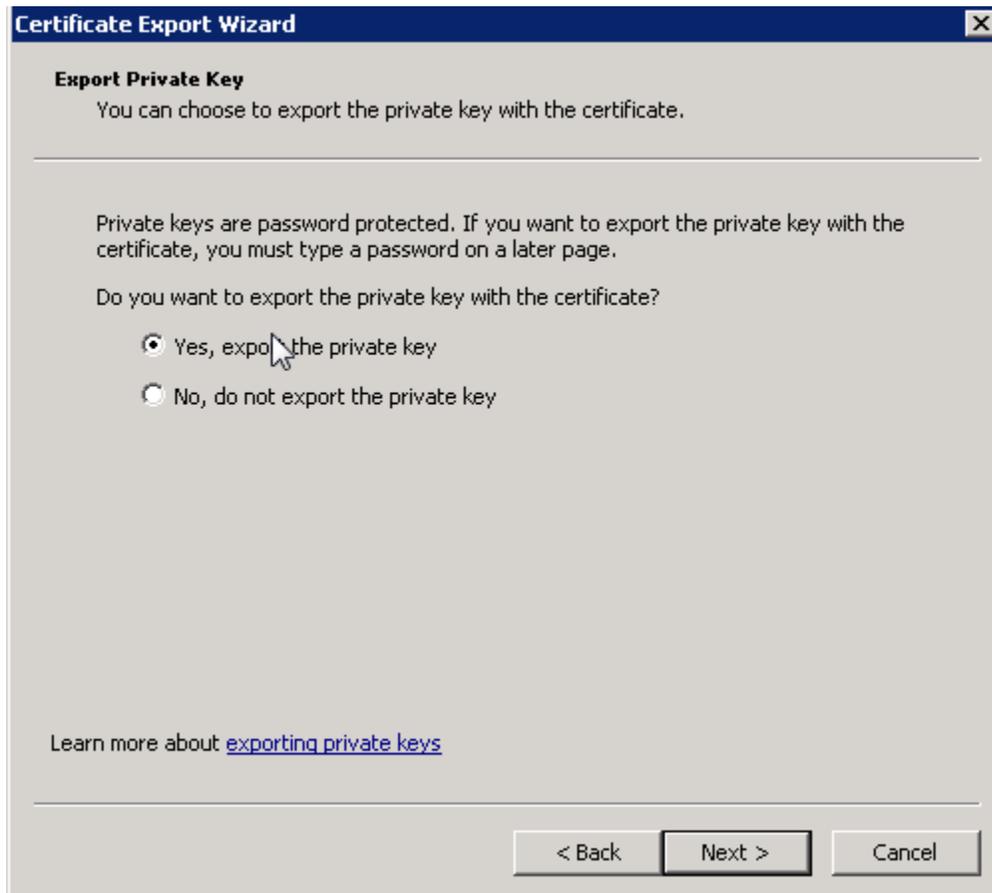
Certificate Installed

Your new certificate has been successfully installed.

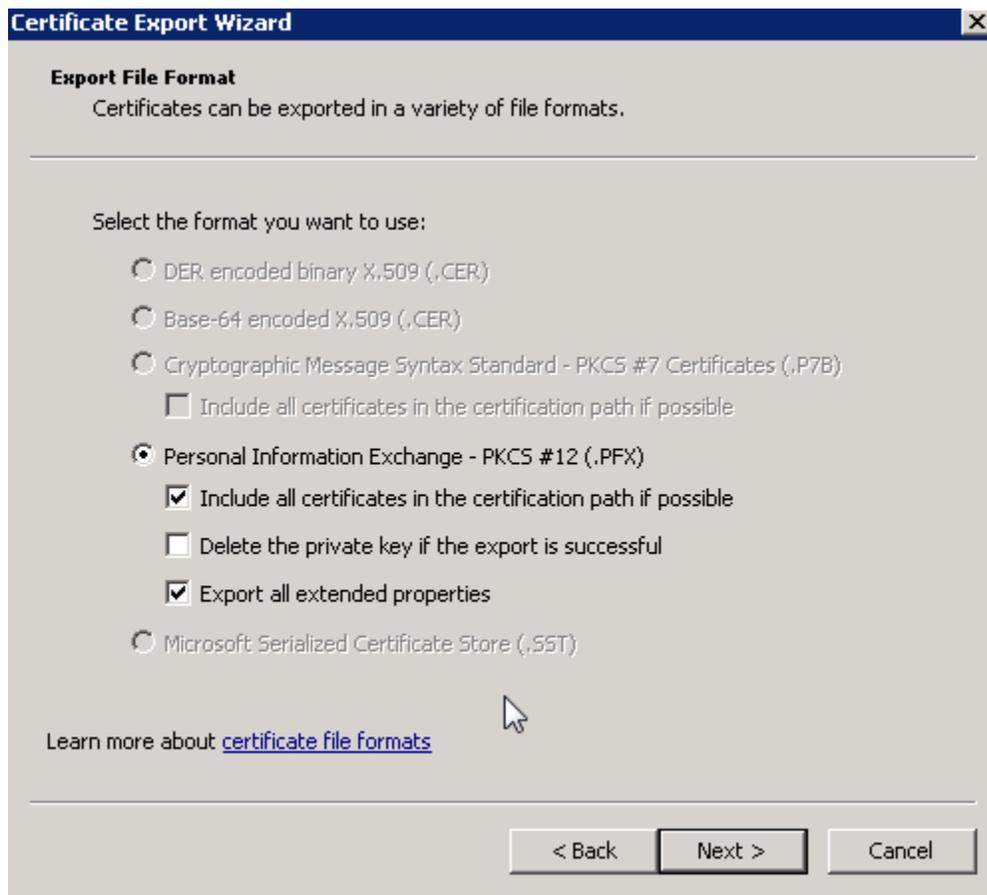
Step 16: Open the MMC -> Select Current User -> Personal ->Certificates -> Select the certificate name -> Right click -> All Tasks -> Export



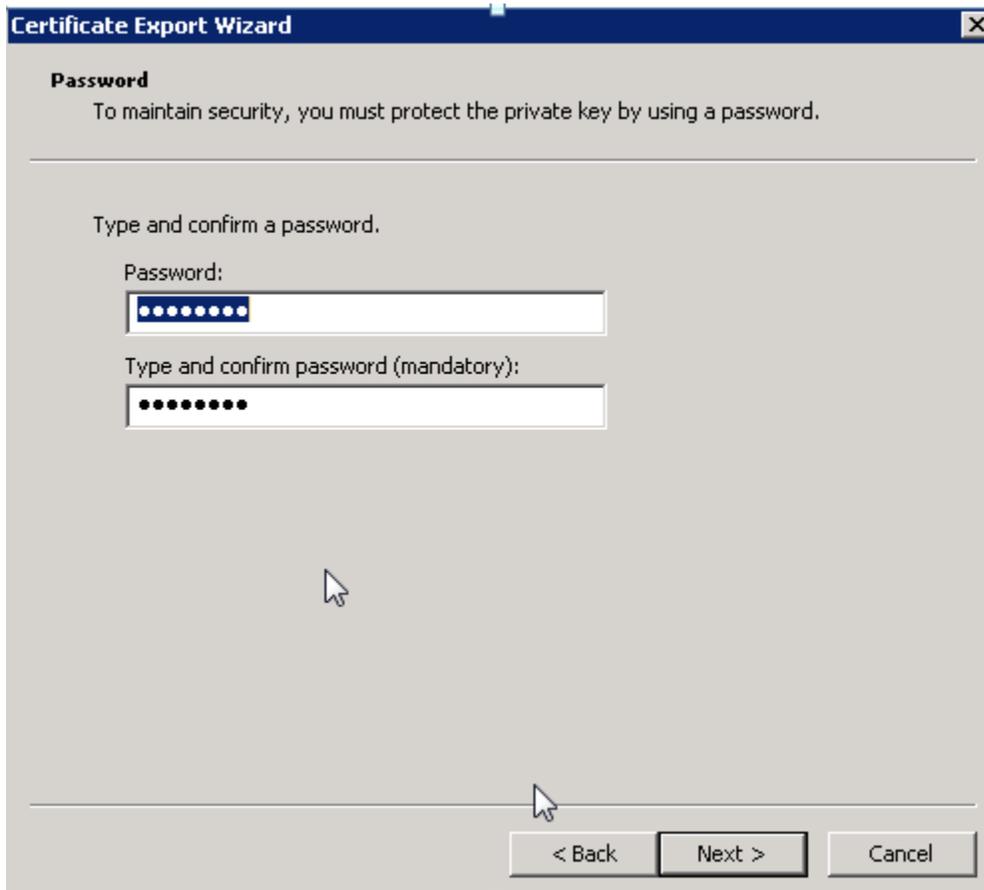
Step 17: Select Yes, export the private key and click Next



Step 18: Click Next



Step 19: Enter the Password and click Next



Certificate Export Wizard [X]

Password
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

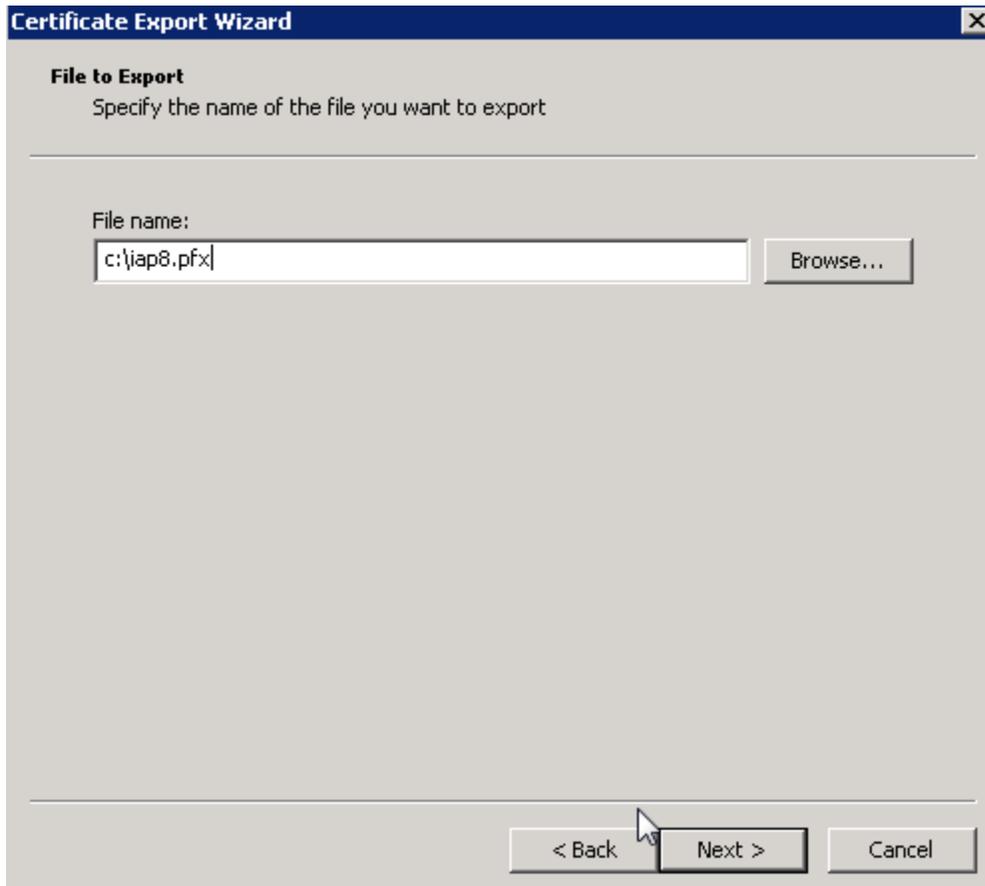
Password:

Type and confirm password (mandatory):

< Back Next > Cancel

The image shows a Windows-style dialog box titled "Certificate Export Wizard" with a close button (X) in the top right corner. The main heading is "Password". Below it, a message states: "To maintain security, you must protect the private key by using a password." A horizontal line separates this message from the input area. The input area contains the instruction "Type and confirm a password." followed by two text boxes. The first text box is labeled "Password:" and contains ten black dots. The second text box is labeled "Type and confirm password (mandatory):" and also contains ten black dots. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". A mouse cursor is visible over the "Next >" button.

Step 20: Enter the filename and click Next



Step 21: Click Finish

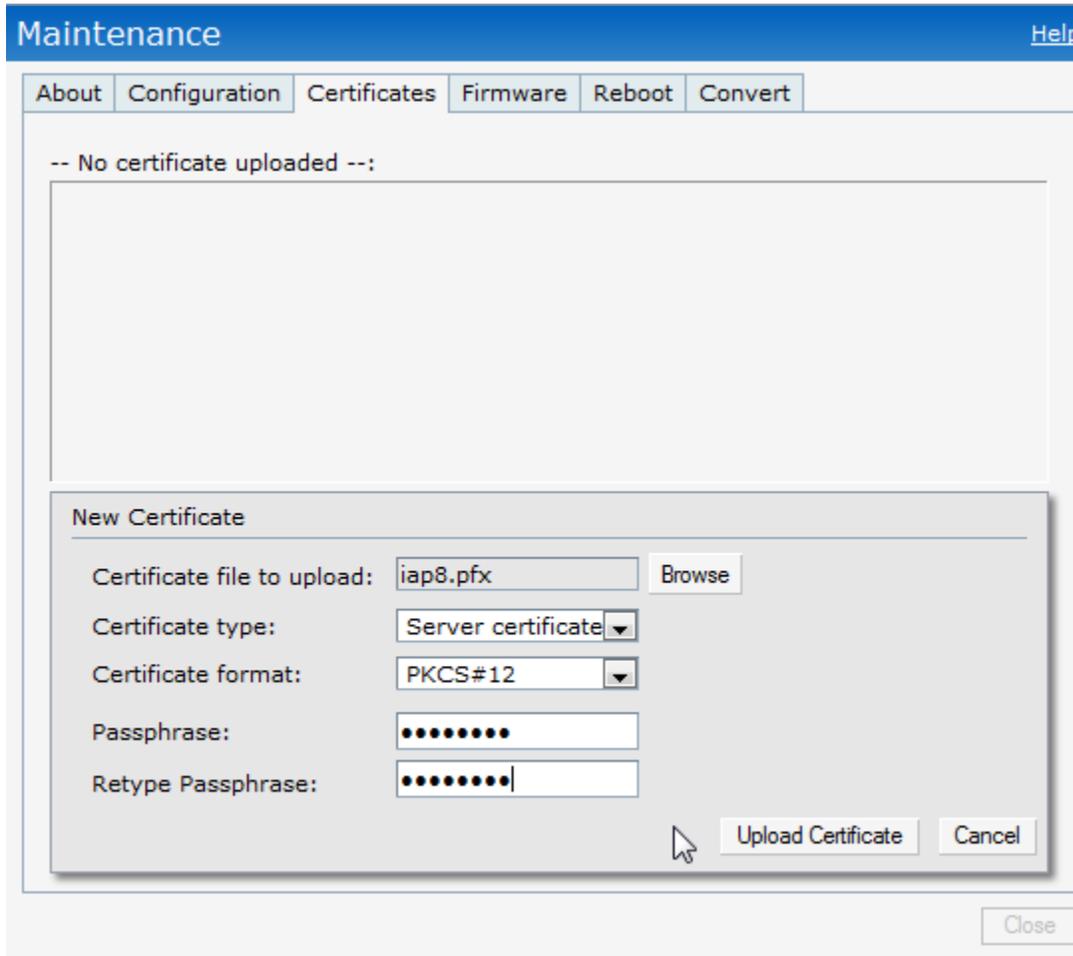


Step 22: Click OK



Step 23: Login to the Aruba Instant Cluster -> Maintenance -> Certificates -> Upload New Certificate -> Select the exported certificate, enter the password -> Upload Certificate

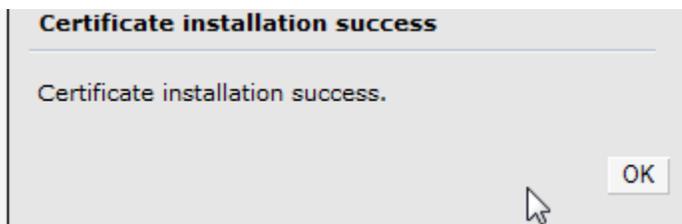
You will need to upload the CA certificate when using EAP-TLS.



The screenshot shows the 'Maintenance' interface with a blue header and a navigation bar containing 'About', 'Configuration', 'Certificates', 'Firmware', 'Reboot', and 'Convert'. The main content area displays '-- No certificate uploaded --:'. A 'New Certificate' dialog box is open, featuring the following fields and controls:

- Certificate file to upload:
- Certificate type: (dropdown)
- Certificate format: (dropdown)
- Passphrase:
- Retype Passphrase:
-

A 'Close' button is located at the bottom right of the main interface.



The screenshot shows a message box with the title 'Certificate installation success'. The text inside reads 'Certificate installation success.' and there is an 'OK' button at the bottom right.