

ATIPXpress

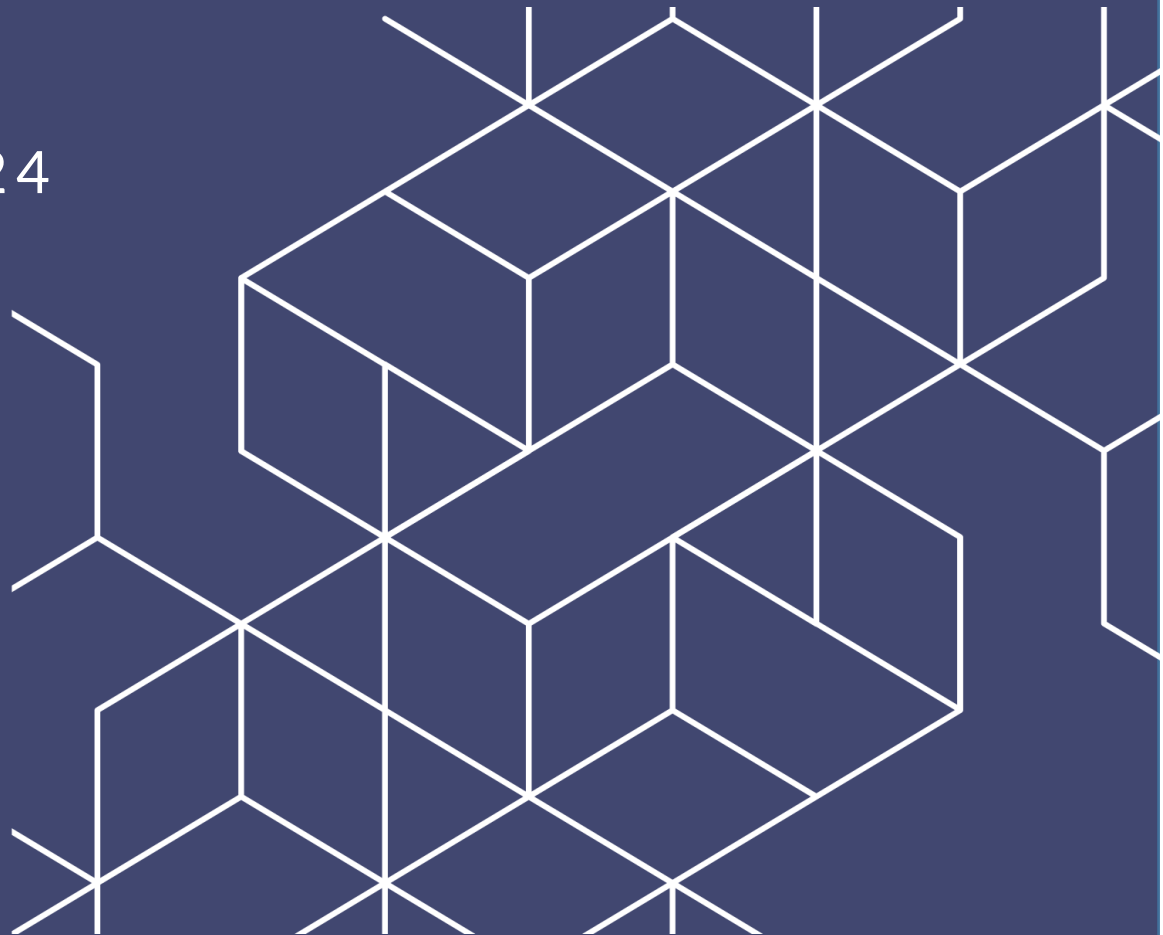


OPEXUS

Encryption Certificate Installation Manual

v11.7.0

May 2024



AX 11.7.0 Encryption Certificate Installation Manual

Notice of Rights

Copyright © 2024, AINS, LLC d/b/a OPEXUS. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publisher: AINS, LLC. For information on obtaining permission for reprints and excerpts, contact info@opexustech.com.

Additionally, all copyrights, confidential information, patents, design rights and all other intellectual property rights of whatsoever nature contained herein are, and shall remain, the sole and exclusive property of the publisher.

Notice of Liability

The information in this publication is believed to be accurate and reliable. However, the information is distributed by the publisher (AINS, LLC.) on an “As Is” basis without warranty for its use, or for any infringements of patents or other rights of third parties resulting from its use.

While every precaution has been taken in the preparation of this publication, neither the author (or authors) nor the publisher will have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused, directly or indirectly, by the information contained in this publication or by the computer software and hardware products described in it.

Notice of Trademarks

The publisher’s company name, company logo, company patents, and company proprietary products are trademarks or registered trademarks of the publisher: AINS, LLC. All other trademarks or registered trademarks are the property of their respective owners.

Non-Disclosure Statement

This document’s contents are confidential and proprietary to AINS, LLC. This document cannot be released publicly or outside the purchasing agency without prior written permission from AINS, LLC.

Images in this manual are used as examples and may contain data and versioning that may not be consistent with your version of the application or information in your environment.

Additional Notice

Information in this documentation is subject to change without notice and does not represent a commitment on the part of AINS, LLC.

Notwithstanding any of the foregoing, if this document was produced as a Deliverable or other work for hire under a contract on behalf of a U.S. Government end user, the terms and conditions of that contract shall apply in the event of a conflict.



Contents

- 1 Document/Correspondence Encryption Certificate Installation 4
 - 1.1 Generate Certificate..... 4
 - 1.2 Install Certificate 7
 - 1.3 Manage Certificates 12



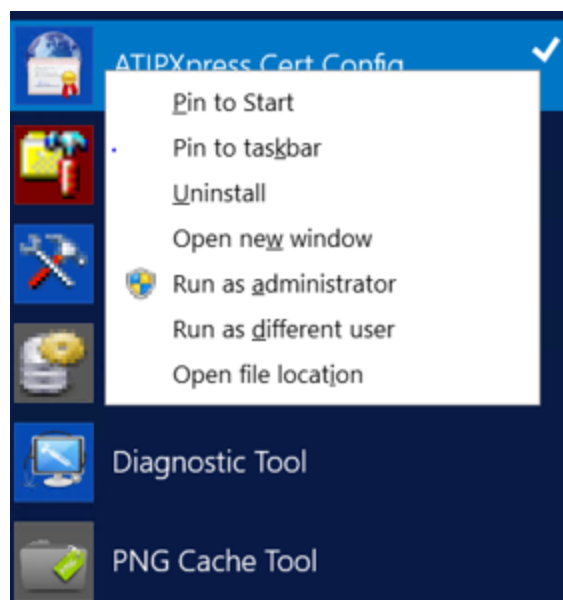
1 Document/Correspondence Encryption Certificate Installation

This manual provides instructions to install an encryption certificate for Documents/Correspondence on your ATIPXpress server.

1.1 Generate Certificate

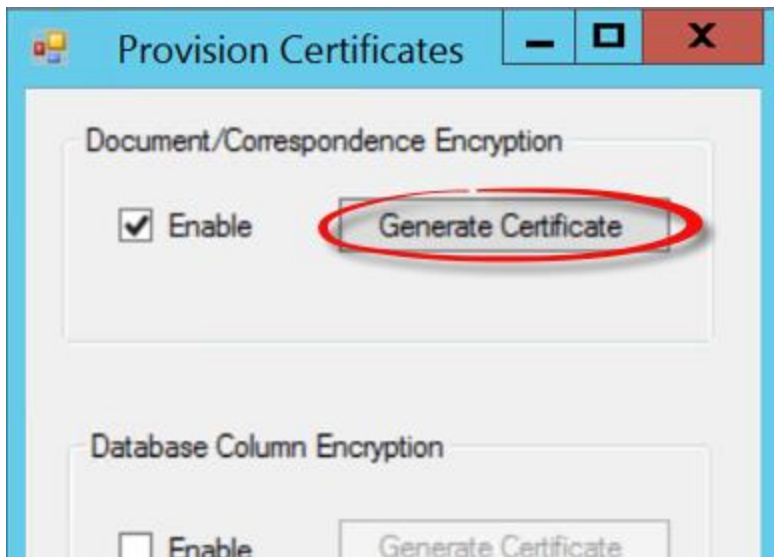
Follow the steps below to generate an encryption certificate:

1. Select **Server > ATIPXpress Cert Config.**

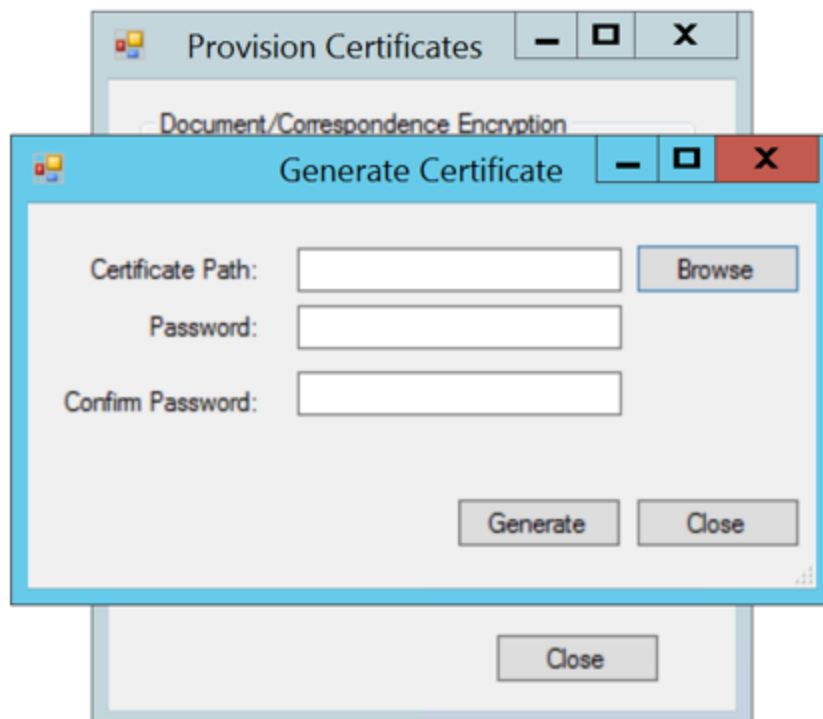


2. The *Provision Certificates* pop up window appears. Click the **Enable** checkbox and click **Generate Certificate**.

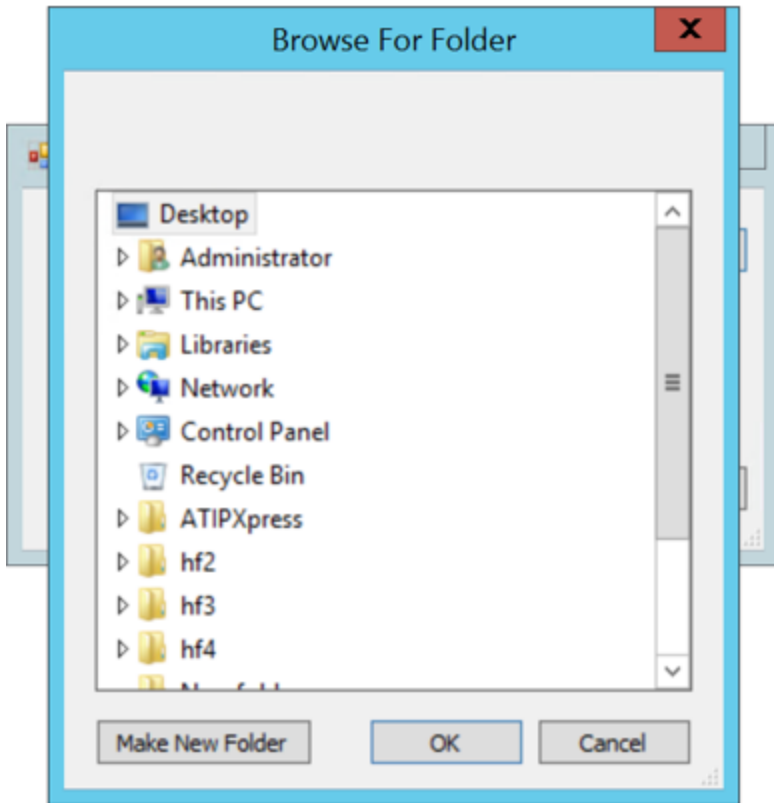




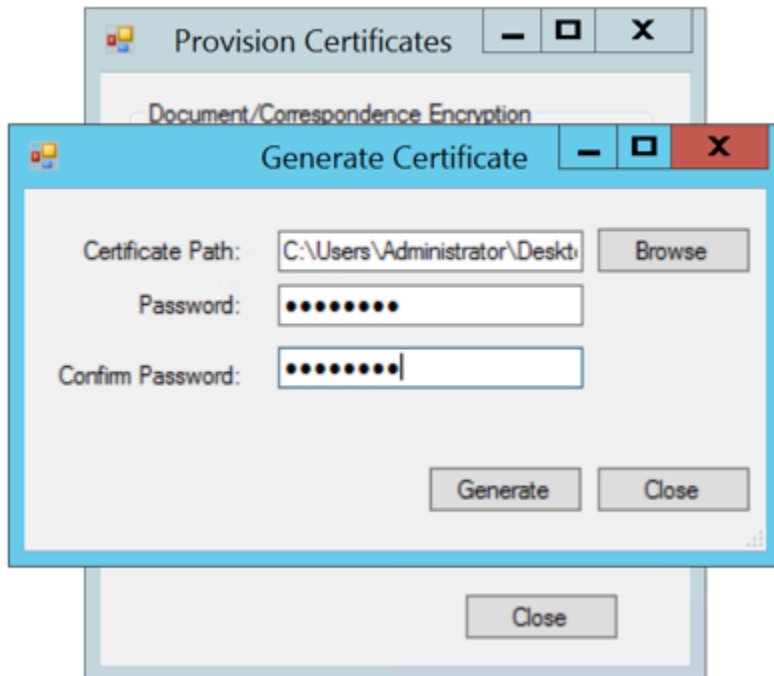
3. The *Generate Certificate* popup window appears. Enter a password for the certificate in the *Password* and *Confirm Password* fields.



4. Click **Browse**. The *Browse for Folder* window appears.

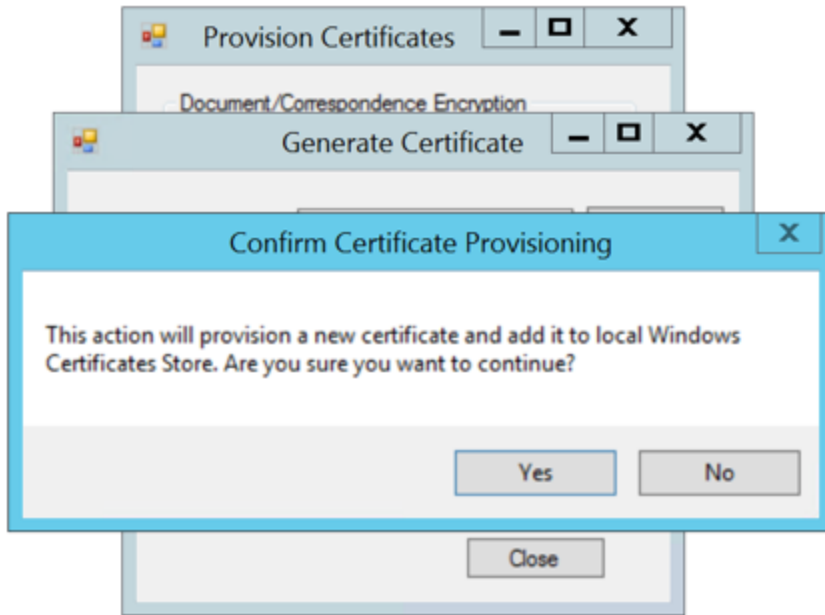


5. Select a destination folder for the certificate and click **OK**.

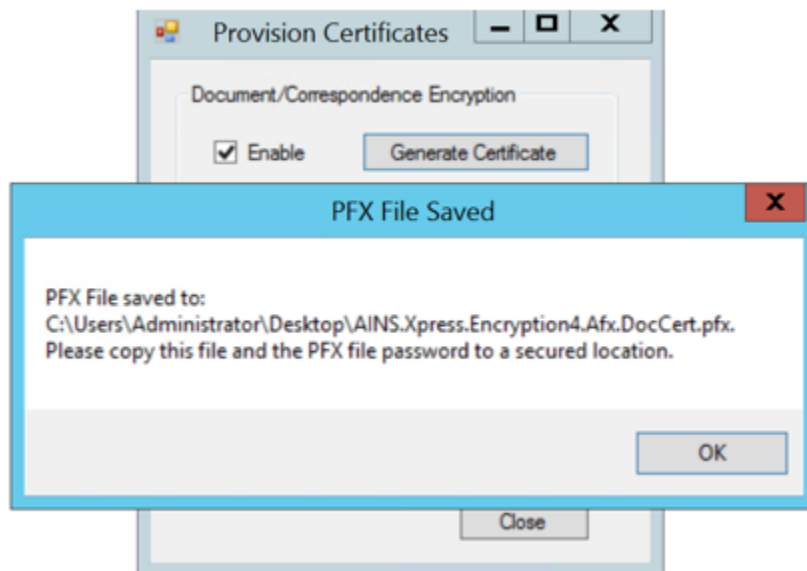


6. The selected folder path appears in the *Certificate Path* field. Click **Generate**. The *Confirm Certificate Provisioning* pop up window appears.
7. Click **Yes** to confirm certificate provisioning.





8. A confirmation window appears, highlighting the file path that the certificate has been saved to. Click **OK**.

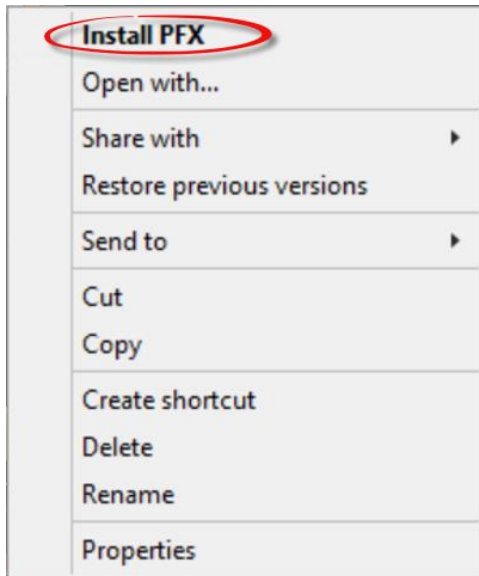


1.2 Install Certificate

Follow the steps below to install a certificate on the FX/AX server.

1. Navigate to a generated certificate (see step 8 in the previous section), then right click the certificate and select **Install** from the drop down list.

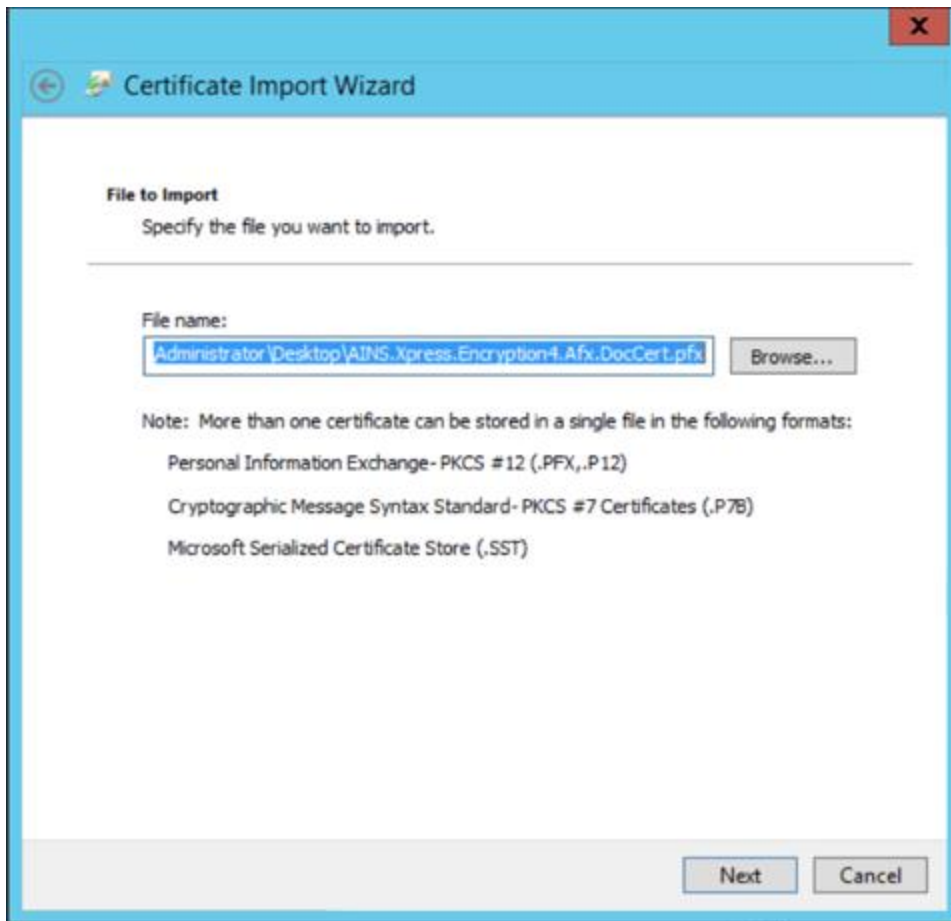




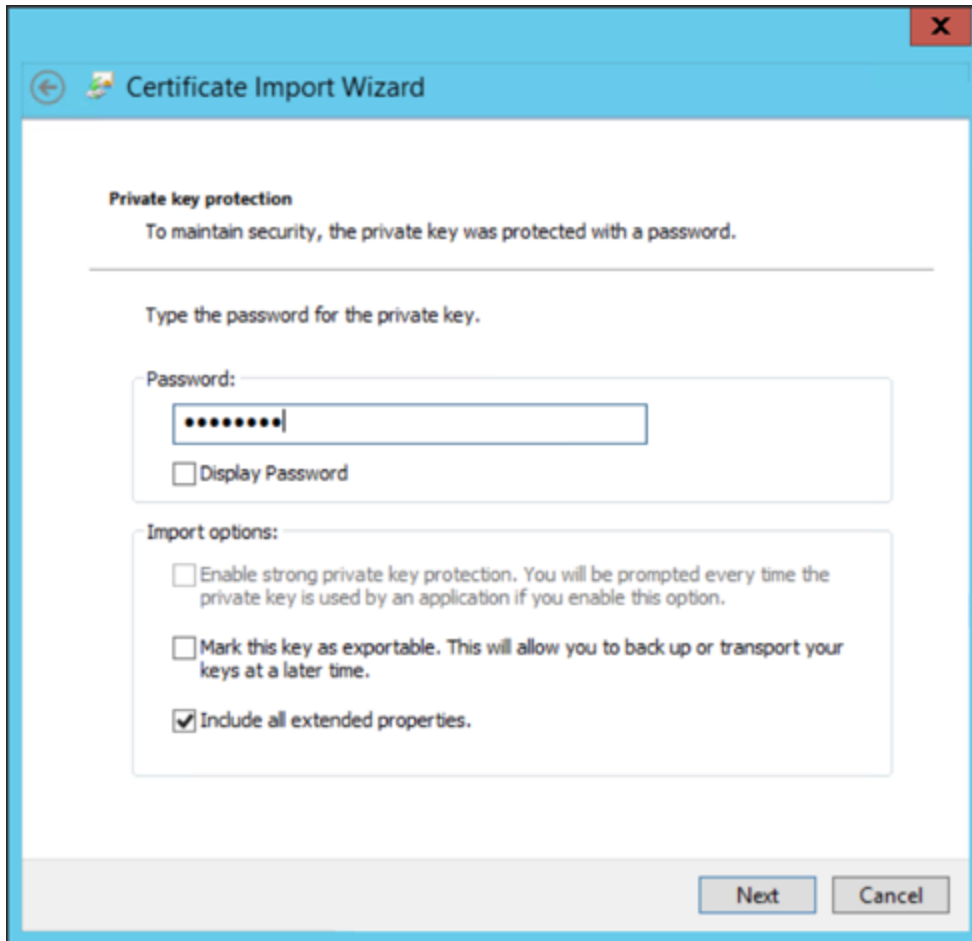
2. The *Certificate Import Wizard* window appears. Select the appropriate **Store Location** radio button and click **Next**.



3. Click **Browse** and select the desired certificate file.



4. Click **Next**.

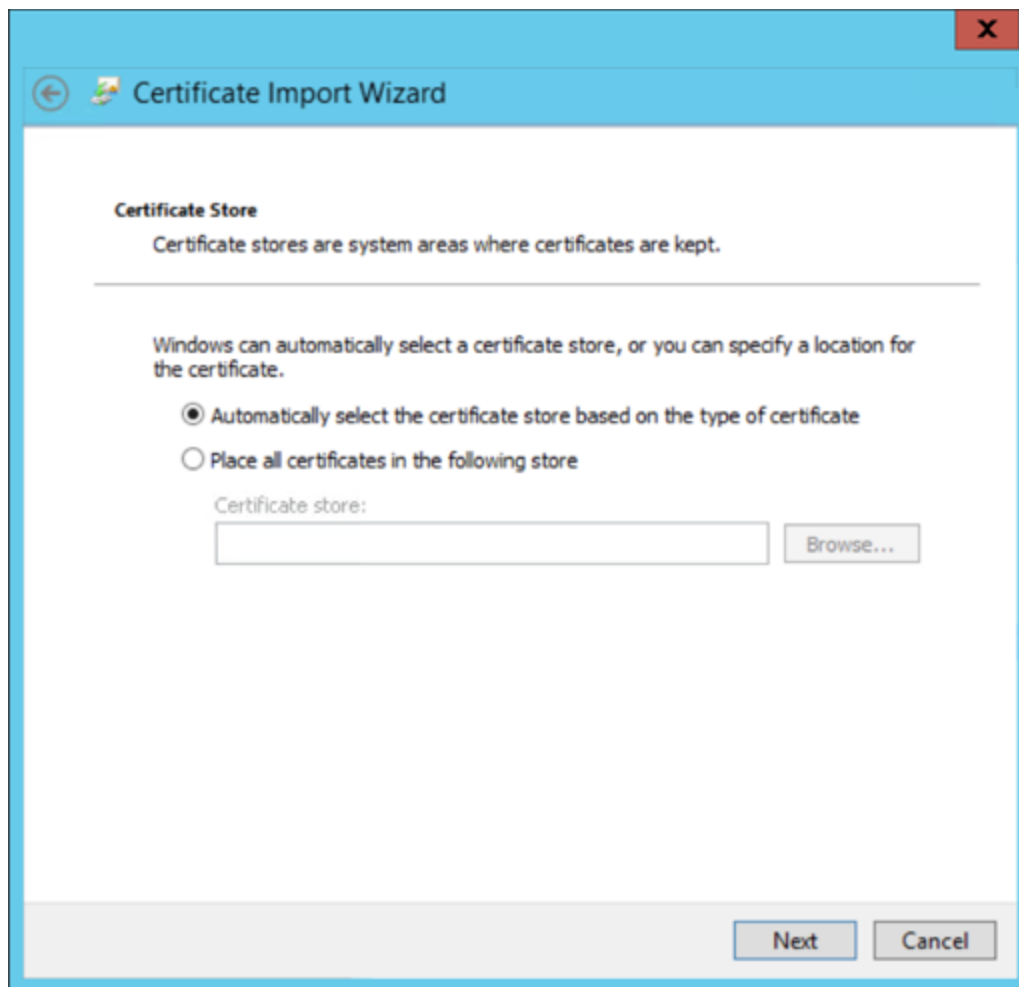


The image shows a Windows-style dialog box titled "Certificate Import Wizard". It has a blue header bar with a back arrow icon and a close button (X). The main content area is white and contains the following text and controls:

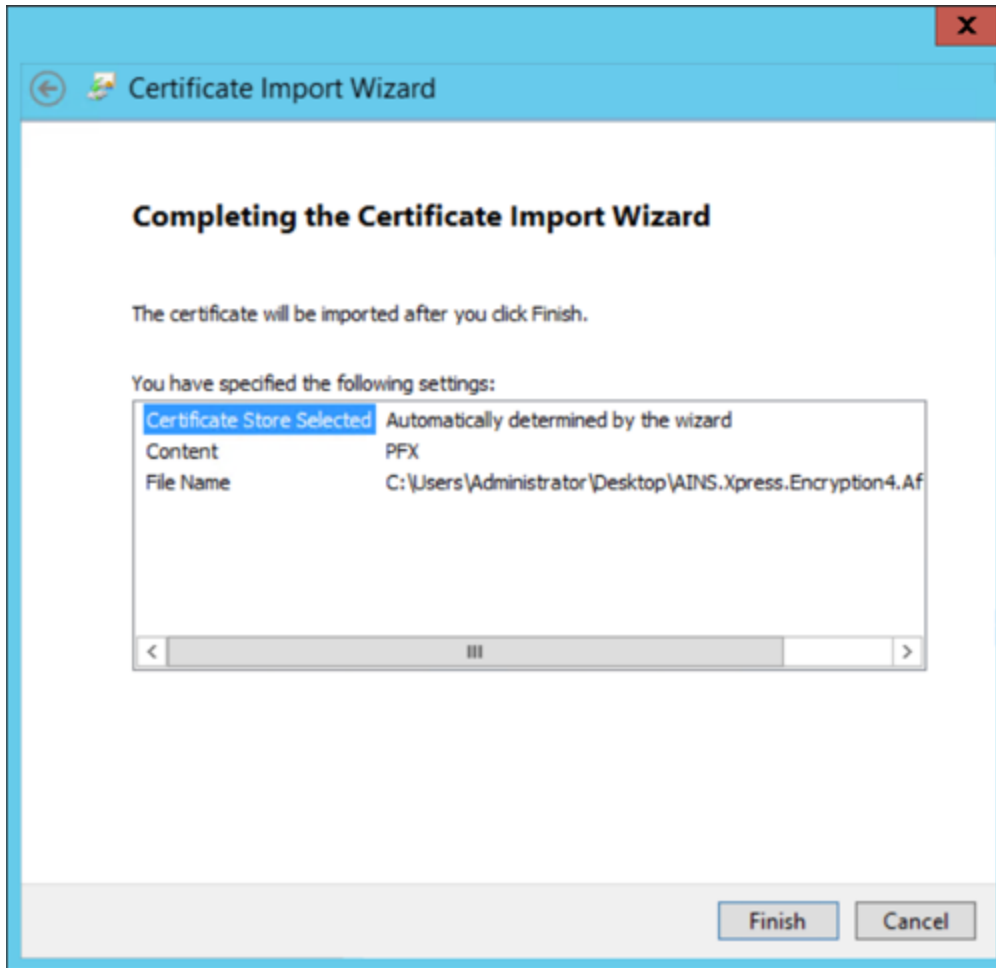
- Private key protection**
To maintain security, the private key was protected with a password.
- Type the password for the private key.
- Password:**
A text input field containing eight dots (••••••••). Below it is a checkbox labeled "Display Password".
- Import options:**
Three checkboxes:
 - ☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
 - ☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
 - ☒ Include all extended properties.

At the bottom right, there are two buttons: "Next" and "Cancel".

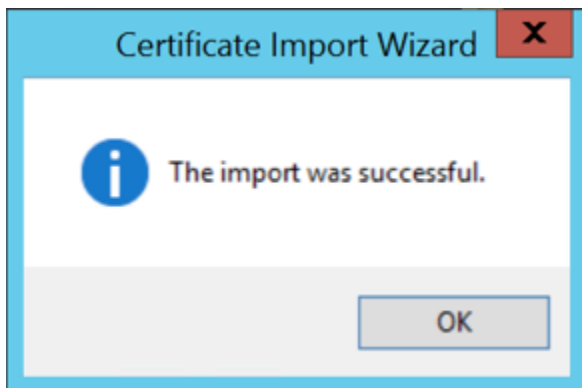
5. Enter the **Password** for the private key in the *Password* field (step 3 in section 1.1) and click **Next**.
6. Select a *Certificate Store* option. If selecting **Place all certificates in the following store**, also select a storage location. Click **Next**.



7. Click **Finish** to complete the certificate import.



8. A pop up window appears, indicating that the certificate import was successful. Click **OK**.



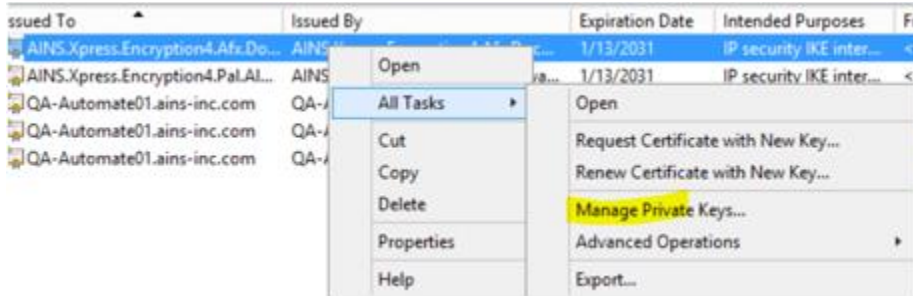
1.3 Manage Certificates

Follow the steps below to finish applying the certificate to the server.

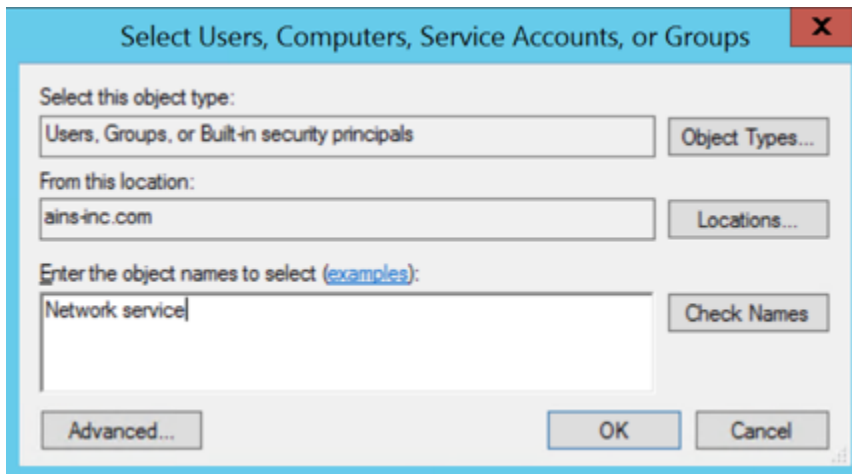
1. Click **Manage Certificates > Personal > Certificates**.



2. Double click on the desired certificate and select **Details**. The thumbprint should be same as in tblconfig > col
3. Right click the certificate, then select **All Tasks > Manage Private Keys** from the drop down list.



4. In the *Enter the object names to select* field, add **Network service** as shown below:



5. Click **Apply**, then click **OK** at the confirmation to complete the certificate configuration.