

# HP Device Manager 4.7

## FTPS Certificates Configuration



### Table of contents

- Overview..... 2
- Server certificate ..... 2
  - Configuring a server certificate on an IIS FTPS server ..... 2
    - Creating a certificate signed by a CA..... 4
    - Creating a self-signed certificate..... 7
  - Configuring a trusted-certificate list in HPDM ..... 8
    - Exporting a PEM-format certificate from a certificate..... 8
    - Creating the CTL ..... 10
    - Deploying the trusted-certificate list to HPDM..... 13
- Client certificate ..... 13
  - Configuring client-certificate authentication on an IIS FTPS server ..... 14
  - Configuring Active Directory mapping..... 14
    - Verifying the DC and CA configuration..... 15
    - Verify the IIS Server configuration..... 17
    - Requesting a client certificate from your CA..... 18
    - Mapping the client certificate to a user account in a domain..... 21
  - Verifying the client-certificate authentication ..... 24
  - Deploying a client certificate to HPDM ..... 24
    - Exporting a client certificate ..... 24
    - Preparing a client certificate and its private key for HPDM..... 27
    - Deploying a client certificate to HPDM components..... 27
- For more information ..... 28

## Overview

FTPS is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols. Certificates are an important factor of FTPS, and they are essential to creating a TLS/SSL connection. For FTPS, there are two types of certificates: server certificates and client certificates. A server certificate is necessary when setting up an FTPS server. This document introduces how to configure certificates on an IIS FTPS server and deploy those certificates to HPDM components.

### Note

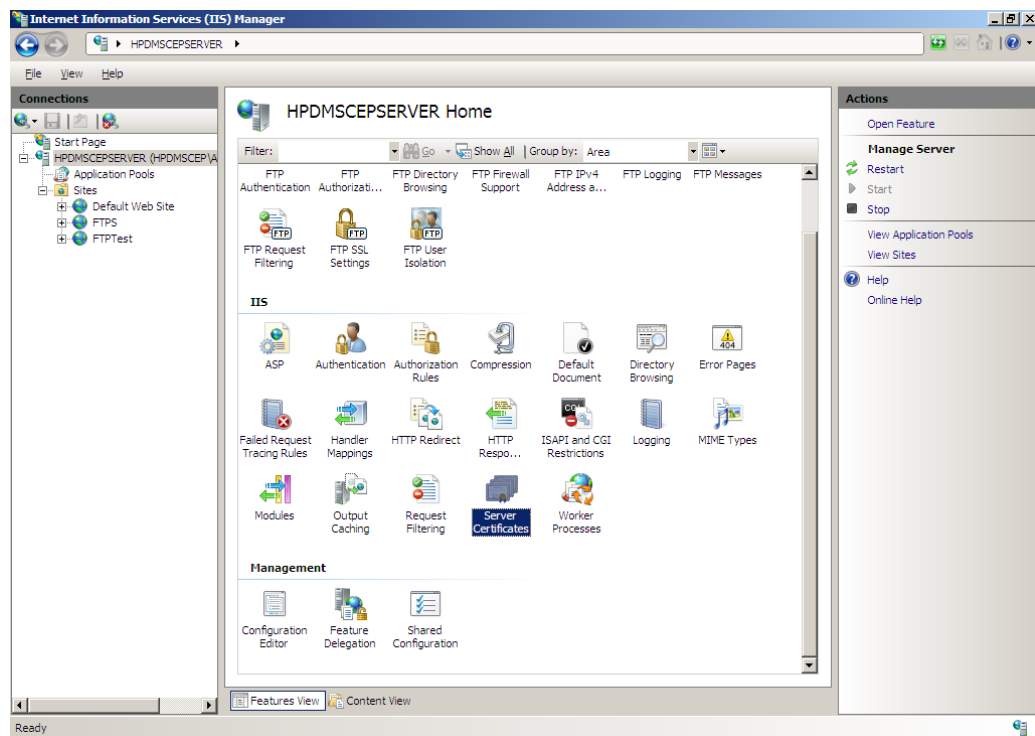
For instructions on setting up an FTPS site on an IIS server, see the *HP Device Manager 4.7 FTP Configuration* white paper.

## Server certificate

A server certificate is used to prove that the FTPS Server is a legitimate server. Most FTPS servers support for server certificate authentication. When you set up an FTPS Server, you must provide a certificate for it. When these certificates are signed by a trusted certificate authority (CA), you can be assured that your device is connected to the requested server, avoiding man-in-the-middle attacks. If the certificate is not signed by a trusted CA (that is, it is a self-signed certificate), the FTPS client might generate a warning stating that the certificate is not valid. You can choose to accept the certificate or reject the connection.

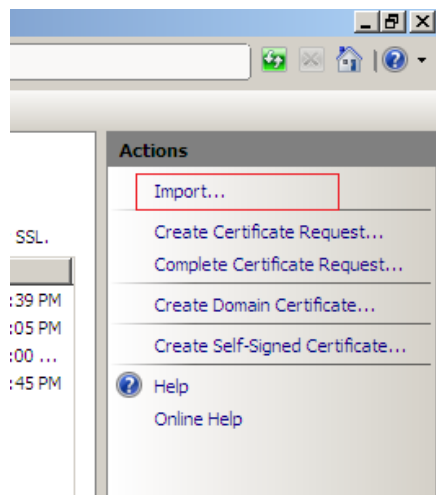
### Configuring a server certificate on an IIS FTPS server

1. On Windows Server 2008 R2, open **IIS Manager** (IIS 7.5).
2. In the Server Manager, select your server, and then double-click **Server Certificates**.

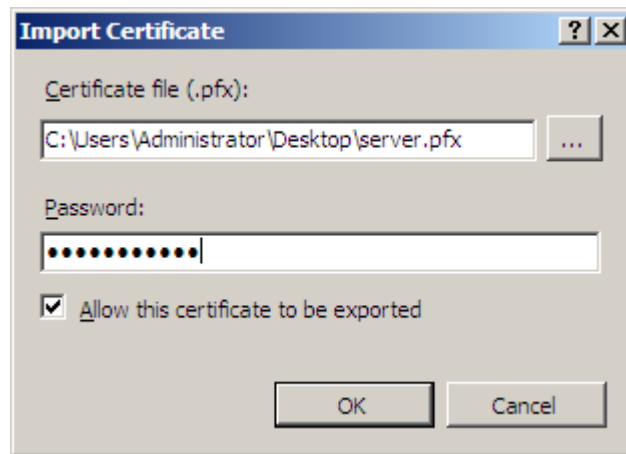


3. If necessary, create a certificate. See [Creating a certificate signed by a CA](#) or [Creating a self-signed certificate](#).

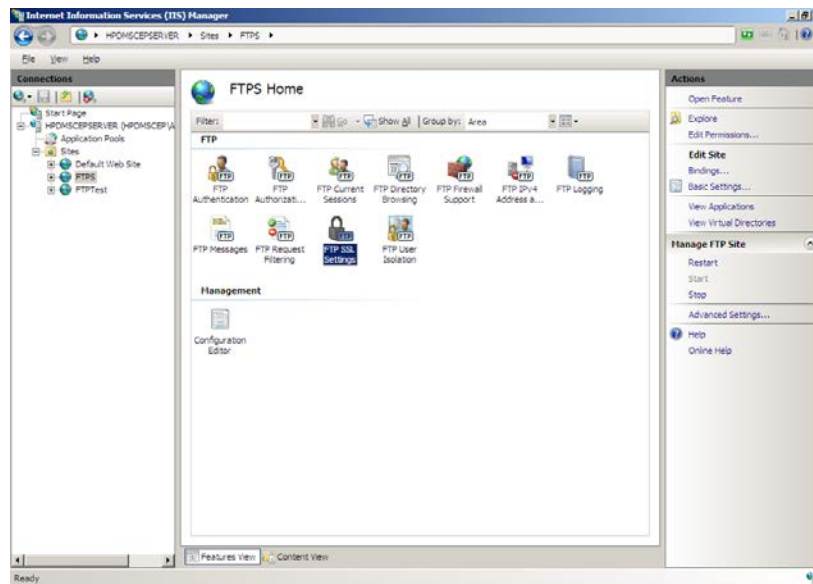
4. In the Server Certificates window, select **Import**.



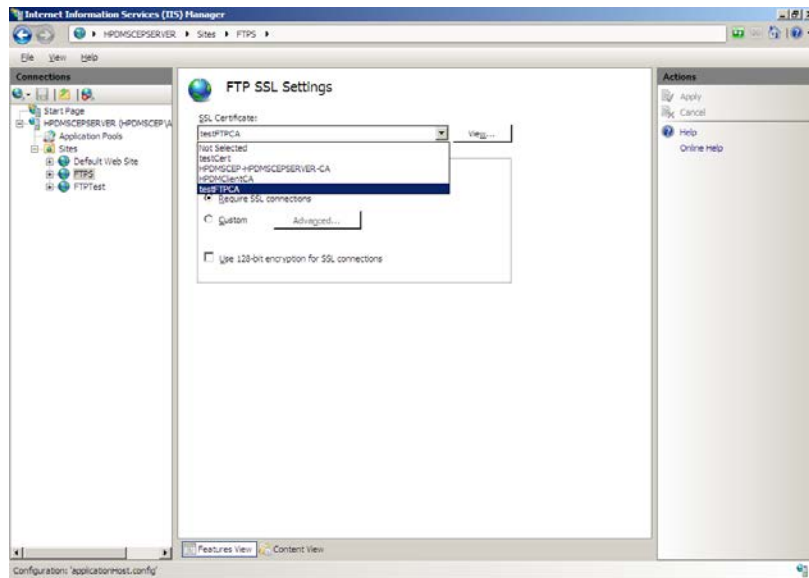
5. Browse to a certificate file (.pfx) that you requested from a trusted CA or created using tools such as OpenSSL and select it. Enter the password for this certificate, and then click **OK**.



6. In the Server Manager, select **<your server> > Sites > <your FTPS site>**, and then double-click **FTP SSL Settings**.

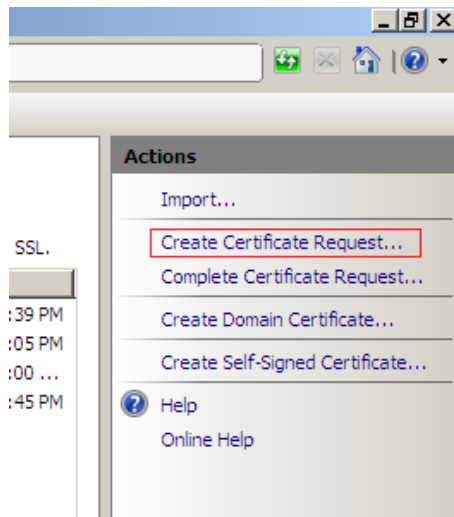


7. Select the certificate you imported in step 5, and then click **Apply**.

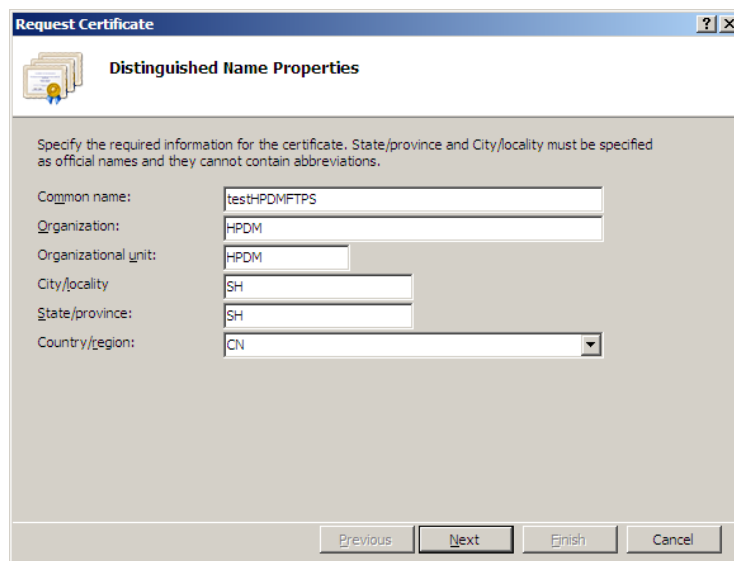


### Creating a certificate signed by a CA

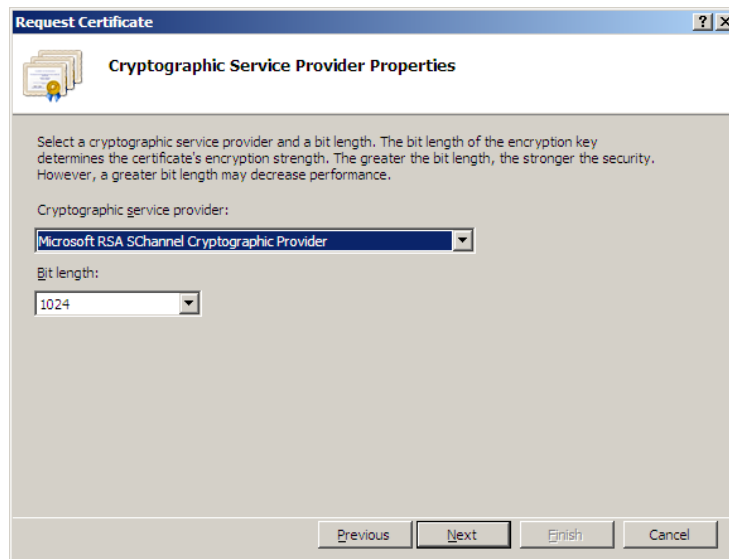
1. In the Server Certificates window, select **Create Certificate Request**.



2. Enter the Distinguished Name Properties information, and then click **Next**.

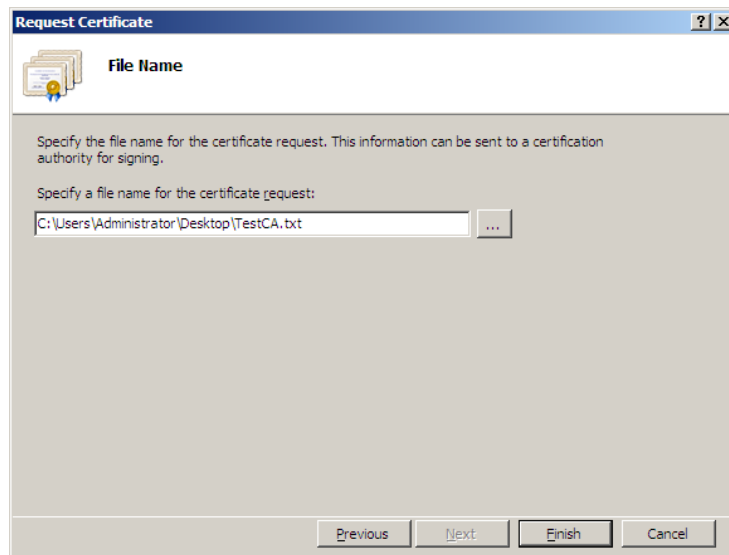


3. Select a **Cryptographic service provider** and **Bit length**, and then click **Next**.



The dialog box is titled "Request Certificate" and "Cryptographic Service Provider Properties". It contains a text box for "Cryptographic service provider" with "Microsoft RSA SChannel Cryptographic Provider" selected, and a "Bit length" dropdown menu set to "1024". At the bottom are "Previous", "Next", "Finish", and "Cancel" buttons.

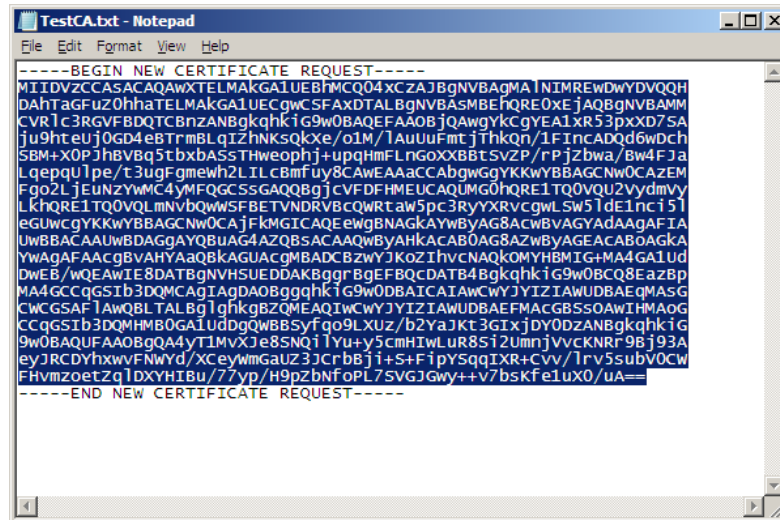
4. To save the certificate request, select a location for the file, and then enter a file name. Click **Finish**.



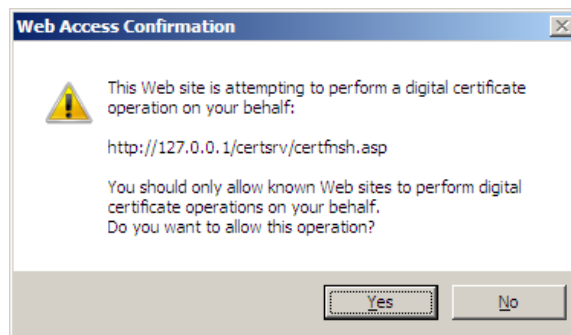
The dialog box is titled "Request Certificate" and "File Name". It contains a text box for "Specify a file name for the certificate request:" with the path "C:\Users\Administrator\Desktop\TestCA.txt" entered. At the bottom are "Previous", "Next", "Finish", and "Cancel" buttons.

5. In your browser, go to `http://<CA-address>/certsrv`.
6. Select **Request a certificate**.
7. Select **advance certificate request**.
8. Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.
9. Open the certificate request you saved in step 4.

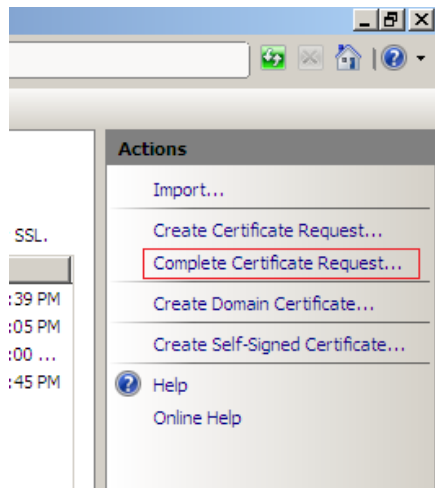
- Select the text between the lines ---BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----, and then copy it.



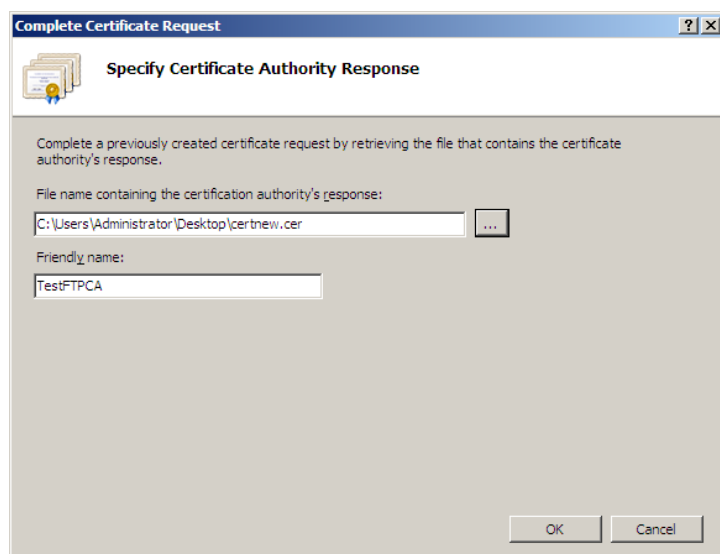
- Paste the text in **Saved Request**, and then click **Submit**.
- In the Web Access Confirmation Prompt, click **Yes**.



- Select **Base 64 encoded**, click **Download certificate**, and then save it.
- In IIS Manager, select **Server Certificates**.
- Select **Complete Certificate Request**.

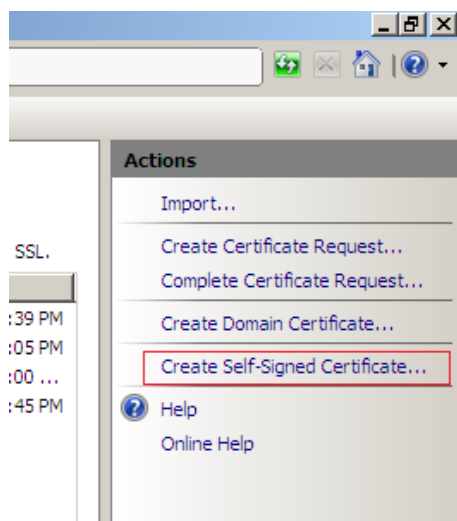


16. Select the file you saved in step 13. This file contains the CA response. Enter a name for this certificate, and then click **OK**.



### Creating a self-signed certificate

1. In the Server Certificates window, select **Create Self-Signed Certificate**.



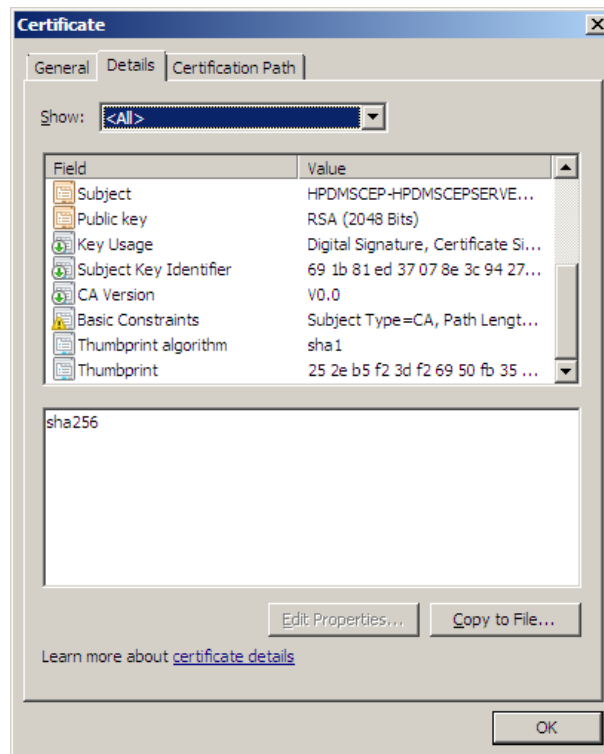
2. Enter a **Friendly Name** for this certificate, and then click **OK**.

## Configuring a trusted-certificate list in HPDM

By default, when connecting to an FTPS server, HPDM accepts the connection automatically and does not verify the server certificate. If you want to verify the server certificate when connecting to an FTPS server, create a certificate trust list (CTL) and deploy it to your HPDM components.

### Exporting a PEM-format certificate from a certificate

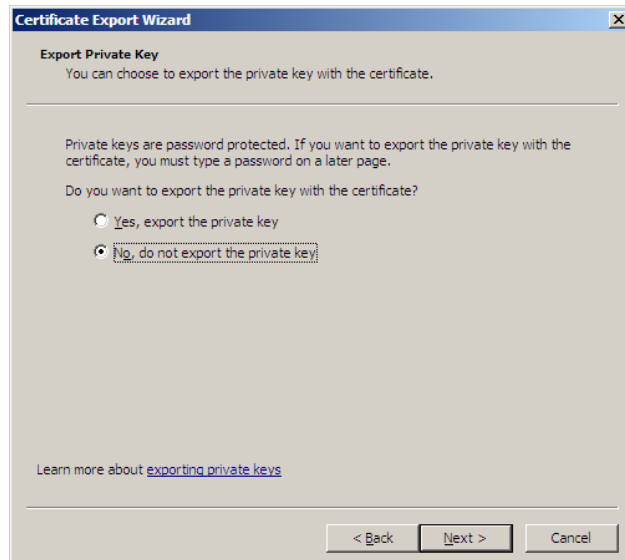
1. In the Details tab of the Certificate dialog, select **Copy to File**.



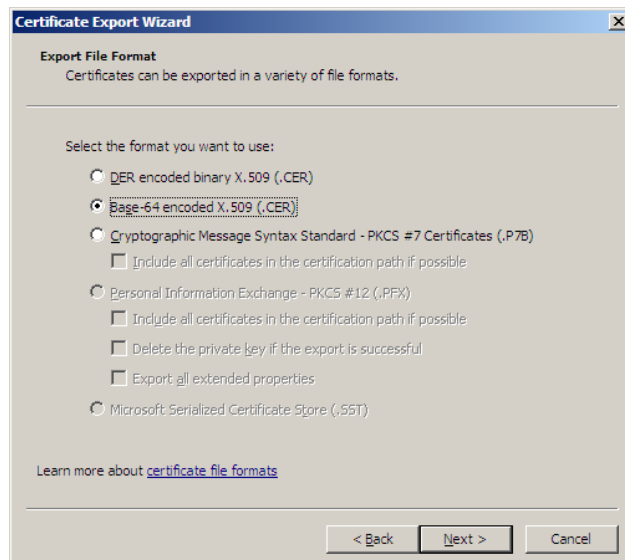
- 
2. In the dialog that appears, click **Next**.



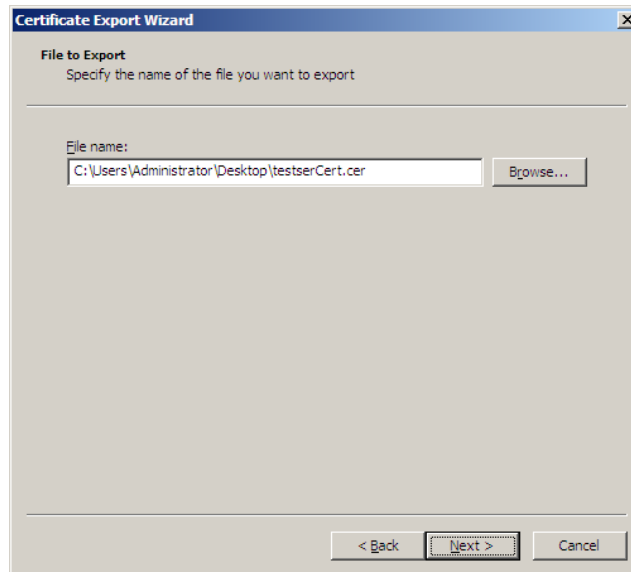
- 
- 
3. Select **No, do not export the private key**, and then click **Next**.



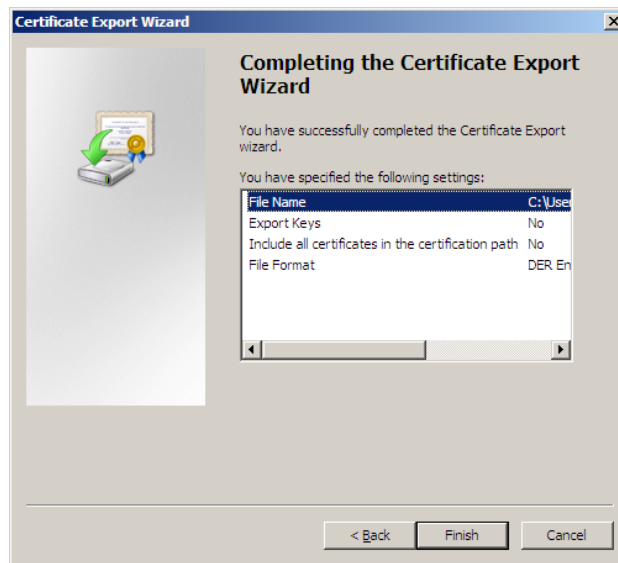
- 
- 
- 
4. Select **Base-64 encoded X.509 (.CER)**, and then click **Next**.



- Click **Browse**, select the file you want to export, and then click **Next**.



- Click **Finish**. You can open the exported PEM certificate in Notepad.



### Creating the CTL

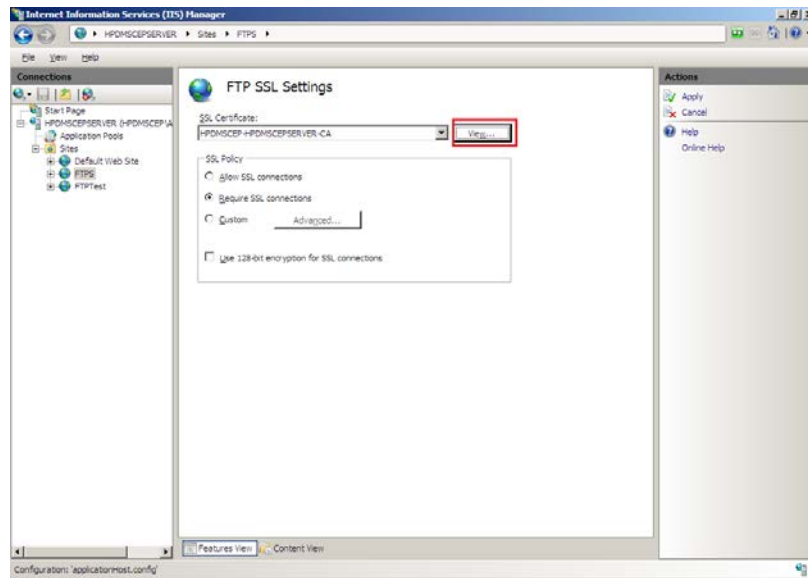
In HPDM, the CTL is a file containing trusted Privacy Enhanced Mail (PEM) format certificates. This file is used to verify server certificates. If you want your HPDM components to verify server certificates, you must create this file.

The name of this file is **ctl.pem** and cannot be changed. If the server certificate is a self-signed certificate, copy its PEM-format certificate content to **ctl.pem**. If the server certificate is available in a CA chain, copy all CA certificates on this CA chain to **ctl.pem**.

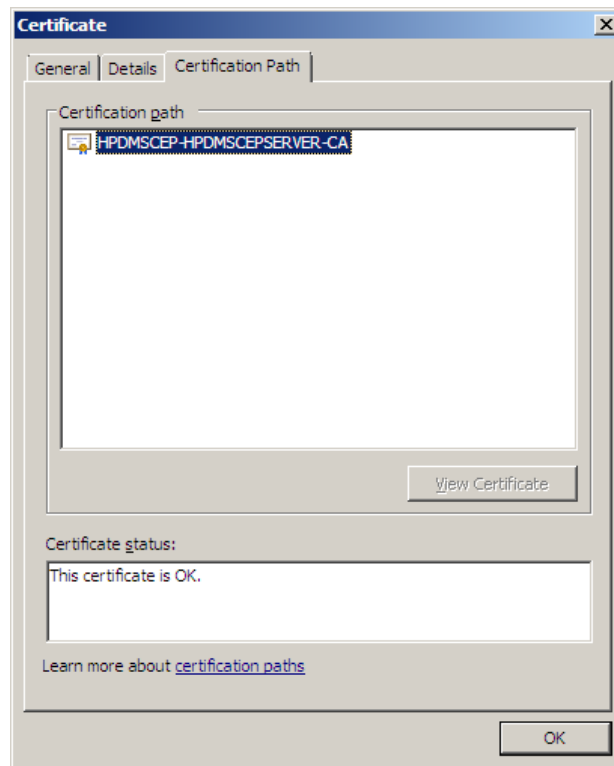
To create ctl.pem:

- On Windows Server 2008 R2, open **IIS Manager** (IIS 7.5).
- In the Server Manager, select **your server -> Sites -> your FTPS site**, and then double-click **FTP SSL Settings**.

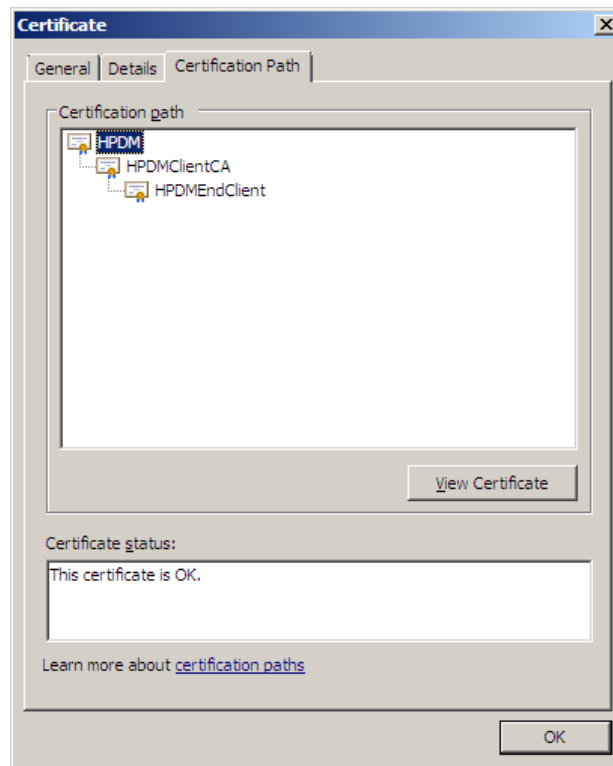
3. Click **View**.



4. In the dialog that appears, select the **Certification Path** tab and then export the certificate. If there is only one root node, it means that this is a self-signed certificate. Export it using the procedure in [Exporting a PEM-format certificate from a certificate](#).

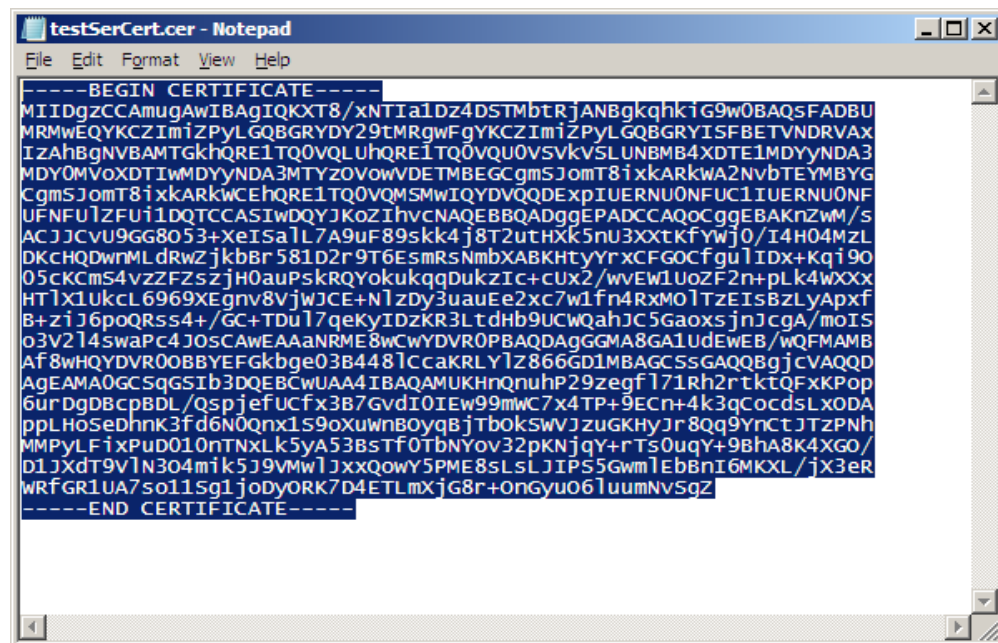


If there is more than one node, it means that this is a certificate from CA chain. See the following figure.



In this example, the name of the certificate is HPDMEndClient. HPDMClientCA is the root CA of HPDMEndClient and HPDM is the root CA of HPDMClientCA. In this scenario, you need to export both the HPDMClientCA and HPDM certificates; however, you do not need to export HPDMEndClient itself. Double-click the node **HPDMClientCA**, and then export it using the procedure in [Exporting a PEM-format certificate from a certificate](#). Export the **HPDM** certificate using the same procedure.

5. In Notepad, open the certificate files you exported in step 4. Select all content and copy it to the file named ctl.pem. If the file ctl.pem does not exist, create it first.



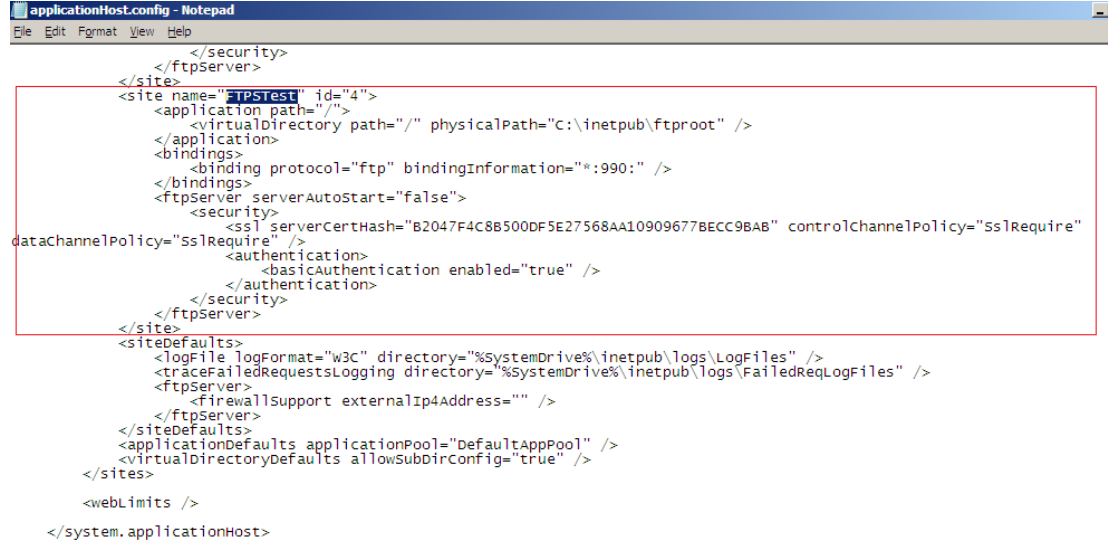


## Configuring client-certificate authentication on an IIS FTPS server

If you want the IIS FTPS server to authenticate the client certificate, you need to enable client-certificate authentication on the IIS FTPS server side first. There is no user interface for this option; however, you can configure it by modifying an IIS configuration file.

1. In Notepad, open the configuration file **ApplicationHost.config**. This is typically located in your %WinDir%\System32\Inetsrv\Config folder.

In the file, search for your FTPS site name. In the following example, the FTPS site name is **FTPSTest**.



```
applicationHost.config - Notepad
File Edit Format View Help

</security>
</ftpServer>
</site>
<site name="FTPSTest" id="4">
  <application path="/">
    <virtualDirectory path="/" physicalPath="C:\inetpub\ftproot" />
  </application>
  <bindings>
    <binding protocol="ftp" bindingInformation="*:990:" />
  </bindings>
  <ftpServer serverAutoStart="false">
    <security>
      <ssl serverCertHash="B2047F4C8B500DF5E27568AA10909677BECC9BAB" controlChannelPolicy="SslRequire" dataChannelPolicy="SslRequire" />
    </security>
    <authentication>
      <basicAuthentication enabled="true" />
    </authentication>
  </ftpServer>
</site>
<siteDefaults>
  <logFile logFormat="w3c" directory="%SystemDrive%\inetpub\logs\LogFiles" />
  <traceFailedRequestsLogging directory="%SystemDrive%\inetpub\logs\FailedReqLogFiles" />
  <ftpServer>
    <firewallSupport externalIp4Address="" />
  </ftpServer>
</siteDefaults>
<applicationDefaults applicationPool="DefaultAppPool" />
<virtualDirectoryDefaults allowSubDirConfig="true" />
</sites>

<webLimits />
</system.applicationHost>
```

2. Under the element <authentication>, clear the current content and enter the following.

```
<authentication>
  <anonymousAuthentication enabled="false" />
  <basicAuthentication enabled="false" />
  <clientCertAuthentication enabled="true" />
</authentication>
```

3. Under the element <security>, enter the following subelement <sslClientCertificates>.

```
<sslClientCertificates clientCertificatePolicy="CertRequire" useActiveDirectoryMapping="true" />
```

4. Save your updated ApplicationHost.config file.



```
<site name="FTPSTest" id="4">
  <application path="/">
    <virtualDirectory path="/" physicalPath="C:\inetpub\ftproot" />
  </application>
  <bindings>
    <binding protocol="ftp" bindingInformation="*:990:" />
  </bindings>
  <ftpServer serverAutoStart="true">
    <security>
      <ssl serverCertHash="B2047F4C8B500DF5E27568AA10909677BECC9BAB" controlChannelPolicy="SslRequire" dataChannelPolicy="SslRequire" />
      <authentication>
        <anonymousAuthentication enabled="false" />
        <basicAuthentication enabled="false" />
        <clientCertAuthentication enabled="true" />
      </authentication>
      <sslClientCertificates clientCertificatePolicy="CertRequire" useActiveDirectoryMapping="true" />
    </security>
  </ftpServer>
</site>
```

For more details about client-certificate authentication, go to

<http://www.iis.net/configreference/system.applicationhost/sites/site/ftpserver/security/authentication/clientcertauthentication>.




## Configuring Active Directory mapping

In an IIS server, client-certificate authentication uses Active Directory to map client certificates against a user account in a domain. There must be a Domain Controller (DC) and a CA in your environment, and they must be installed on the same device. For instructions on setting up a CA, see the *HP Device Manager 4.7 SCEP Tutorial* white paper.


### Verifying the DC and CA configuration

After setting up the DC and CA on a single device, verify that the components are configured correctly.













































1. Verify that the following roles are enabled:
  - Active Directory Certificate Services
  - Active Directory Domain Services
  - Web Server (IIS)
2. Verify that the Active Directory Certificate Services has the following Role Services installed:

Role Service	Status
 Certification Authority	Installed
 Certification Authority Web Enrollment	Installed
 Online Responder	Installed
Network Device Enrollment Service	Not installed
Certificate Enrollment Web Service	Not installed
Certificate Enrollment Policy Web Service	Not installed

3. Verify that the Active Directory Domain Services has the following Role Services installed:

















































Role Service	Status
 Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed
Password Synchronization	Not installed
Administration Tools	Not installed

4. In the DC, verify that the following IIS Role Services are installed:

Role Services: 24 installed	
Role Service	Status
 Web Server	Installed
 Common HTTP Features	Installed
 Static Content	Installed
 Default Document	Installed
 Directory Browsing	Installed
 HTTP Errors	Installed
 HTTP Redirection	Installed
 WebDAV Publishing	Not installed
 Application Development	Installed
 ASP.NET	Not installed
 .NET Extensibility	Not installed
 ASP	Installed
 CGI	Not installed
 ISAPI Extensions	Installed
 ISAPI Filters	Not installed
 Server Side Includes	Not installed
 Health and Diagnostics	Installed
 HTTP Logging	Installed
 Logging Tools	Installed
 Request Monitor	Installed
 Tracing	Installed
 Custom Logging	Not installed
 ODBC Logging	Not installed
 Security	Installed
 Basic Authentication	Not installed
 Windows Authentication	Installed
 Digest Authentication	Not installed
 Client Certificate Mapping Authentication	Not installed
 IIS Client Certificate Mapping Authentication	Not installed
 URL Authorization	Not installed
 Request Filtering	Installed
 IP and Domain Restrictions	Not installed
 Performance	Installed
 Static Content Compression	Installed
 Dynamic Content Compression	Not installed
 Management Tools	Installed
 IIS Management Console	Installed
 IIS Management Scripts and Tools	Not installed
 Management Service	Not installed
 IIS 6 Management Compatibility	Installed
 IIS 6 Metabase Compatibility	Installed
 IIS 6 WMI Compatibility	Not installed
 IIS 6 Scripting Tools	Not installed
 IIS 6 Management Console	Not installed
FTP Server	Not installed
FTP Service	Not installed
FTP Extensibility	Not installed
IIS Hostable Web Core	Not installed

### Verify the IIS Server configuration

1. Verify that the IIS Server is located on the same domain as the DC and CA.  
If the IIS Server is not installed on the same device as the DC and CA, you must ensure that the device it is installed on joins the same domain as the DC and CA device.
2. Verify that the Web Server (IIS) role is enabled
3. Verify that the following IIS Role Services are installed:

Role Services: 26 installed	
Role Service	Status
 Web Server	Installed
 Common HTTP Features	Installed
 Static Content	Installed
 Default Document	Installed
 Directory Browsing	Installed
 HTTP Errors	Installed
 HTTP Redirection	Not installed
 WebDAV Publishing	Not installed
 Application Development	Installed
 ASP.NET	Installed
 .NET Extensibility	Installed
 ASP	Not installed
 CGI	Not installed
 ISAPI Extensions	Installed
 ISAPI Filters	Installed
 Server Side Includes	Not installed
 Health and Diagnostics	Installed
 HTTP Logging	Installed
 Logging Tools	Not installed
 Request Monitor	Installed
 Tracing	Installed
 Custom Logging	Not installed
 ODBC Logging	Not installed
 Security	Installed
 Basic Authentication	Installed
 Windows Authentication	Installed
 Digest Authentication	Not installed
 Client Certificate Mapping Authentication	Installed
 IIS Client Certificate Mapping Authentication	Not installed
 URL Authorization	Not installed
 Request Filtering	Installed
 IP and Domain Restrictions	Not installed
 Performance	Installed
 Static Content Compression	Installed
 Dynamic Content Compression	Not installed
 Management Tools	Installed
 IIS Management Console	Installed
 IIS Management Scripts and Tools	Not installed
 Management Service	Not installed
 IIS 6 Management Compatibility	Not installed
 IIS 6 Metabase Compatibility	Not installed
 IIS 6 WMI Compatibility	Not installed
 IIS 6 Scripting Tools	Not installed
 IIS 6 Management Console	Not installed
 FTP Server	Installed
 FTP Service	Installed
 FTP Extensibility	Not installed
 IIS Hostable Web Core	Not installed

## Requesting a client certificate from your CA

1. To request a client certificate, go to <http://<CA-address>/certsrv>. The CA address is the address of the device where the DC and CA installed.
2. Click **Request a Certificate**.
3. Click **advance certificate request**.
4. Click **Create and submit a request to this CA**.
5. If a Web Access Confirmation prompt appears, click **Yes**.
6. Enter your **Identifying Information**.

Microsoft Active Directory Certificate Services - HPDMSCEP-HPDMSCEP-CA

### Advanced Certificate Request

**Identifying Information:**

Name: HPDMDemo  
E-Mail: xiaolu.zhang@hp.com  
Company: HP  
Department: HPDMD  
City: Shanghai  
State: SH  
Country/Region: CN

**Type of Certificate Needed:**  
Client Authentication Certificate

**Key Options:**

☒ Create new key set ☐ Use existing key set  
CSP: Microsoft RSA SChannel Cryptographic Provider  
Key Usage: ☒ Exchange  
Key Size: 1024 (Min: 384, Max: 16384, common key sizes: 512 1024 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: sha1  
Only used to sign request.  
☐ Save request  
Attributes:

7. Under Type of Certificate Needed, select **Client Authentication Certificate**.

Microsoft Active Directory Certificate Services - HPDMSCEP-HPDMSCEP-CA

### Advanced Certificate Request

**Identifying Information:**

Name: HPDMDemo  
E-Mail: xiaolu.zhang@hp.com  
Company: HP  
Department: HPDMD  
City: Shanghai  
State: SH  
Country/Region: CN

**Type of Certificate Needed:**  
Client Authentication Certificate

**Key Options:**

☒ Create new key set ☐ Use existing key set  
CSP: Microsoft RSA SChannel Cryptographic Provider  
Key Usage: ☒ Exchange  
Key Size: 1024 (Min: 384, Max: 16384, common key sizes: 512 1024 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: sha1  
Only used to sign request.  
☐ Save request  
Attributes:

8. Under Key Options, select **Mark key as exportable**. Do not change the other default options.

Microsoft Active Directory Certificate Services - HPDMSCEP-HPDMSCEP-CA

### Advanced Certificate Request

**Identifying Information:**

Name: HPDMDemo  
E-Mail: xiaolu.zhang@hp.com  
Company: HP  
Department: HPDM  
City: Shanghai  
State: SH  
Country/Region: CN

**Type of Certificate Needed:**  
Client Authentication Certificate

**Key Options:**

☒ Create new key set ☐ Use existing key set  
CSP: Microsoft RSA SChannel Cryptographic Provider  
Key Usage: ☒ Exchange  
Key Size: 1024 (Min: 384, Max: 16384, common key sizes: 512 1024 2048 4096 8192 16384)  
☒ Automatic key container name ☐ User specified key container name  
☒ Mark keys as exportable **This is very important, must to check.**  
☐ Enable strong private key protection

**Additional Options:**

Request Format: ☒ CMC ☐ PKCS10  
Hash Algorithm: sha1  
Only used to sign request.  
☐ Save request  
Attributes:

9. Enter a **Friendly Name** for this certificate, and then click **Submit**.

E-Mail: xiaolu.zhang@hp.com  
Company: HP  
Department: HPDM  
City: Shanghai  
State: SH  
Country/Region: CN

**Type of Certificate Needed:**  
Client Authentication Certificate

**Key Options:**

☒ Create new key set ☐ Use existing key set  
CSP: Microsoft RSA SChannel Cryptographic Provider  
Key Usage: ☒ Exchange  
Key Size: 1024 (Min: 384, Max: 16384, common key sizes: 512 1024 2048 4096 8192 16384)  
☒ Automatic key container name ☐ User specified key container name  
☒ Mark keys as exportable  
☐ Enable strong private key protection

**Additional Options:**

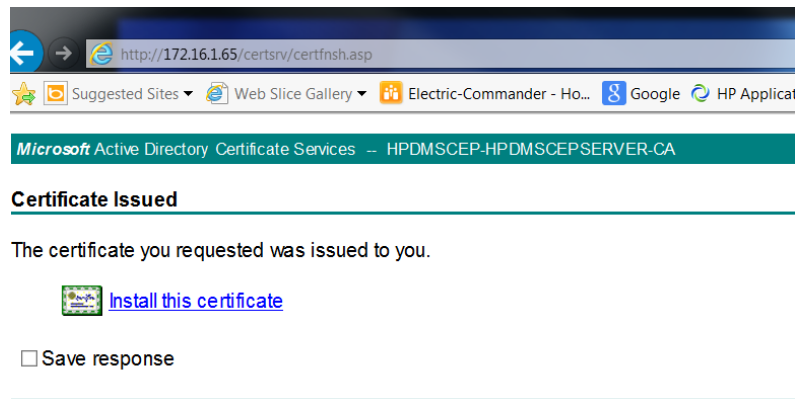
Request Format: ☒ CMC ☐ PKCS10  
Hash Algorithm: sha1  
Only used to sign request.  
☐ Save request  
Attributes:

**Friendly Name:** HPDMDClient

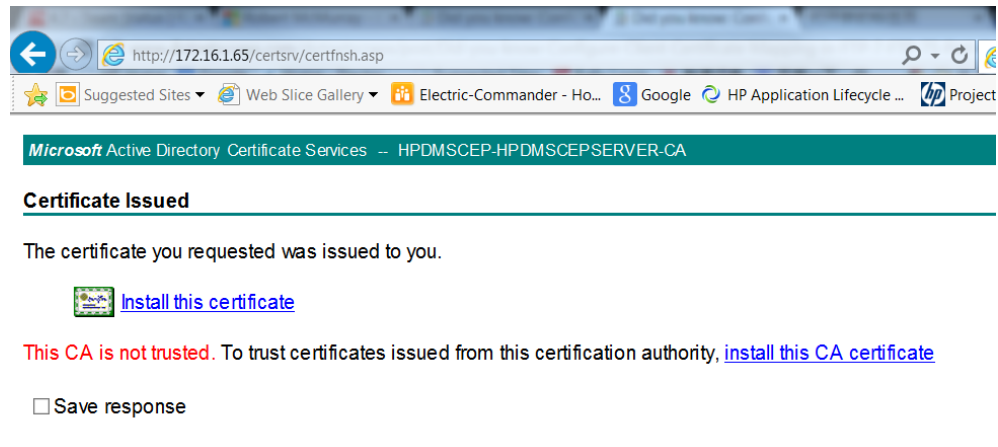
Submit >

10. If a Web Access Confirmation prompt appears, click **Yes**.

11. Click **Install this certificate**.

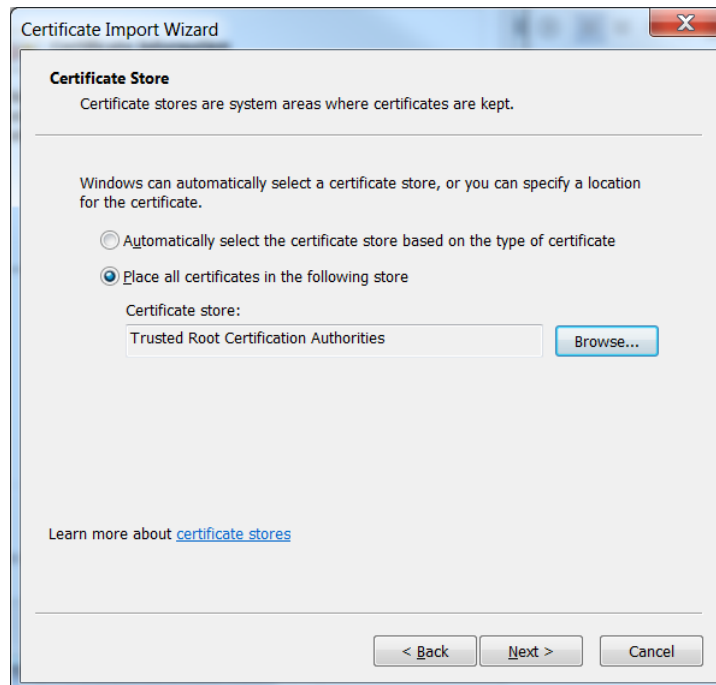


12. After you have clicked Install this certificate, if you see **This CA is not trusted**, click **install this CA certificate**. Otherwise, skip this step.

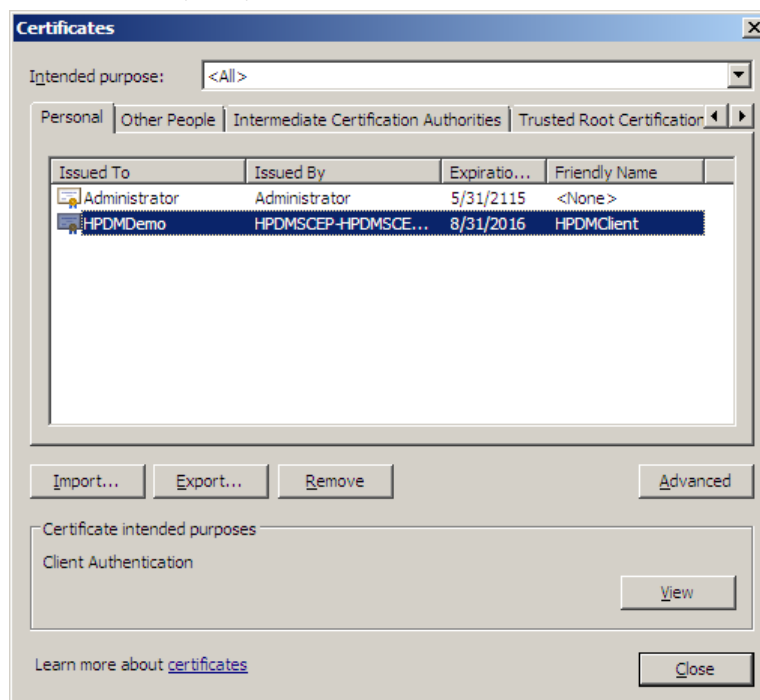


**Note:**

In the Certificate Import Wizard used to install the CA certificate, select **Place all certificates in the following store**, and then select **Trusted Root Certification Authorities** as the **Certificate store**.

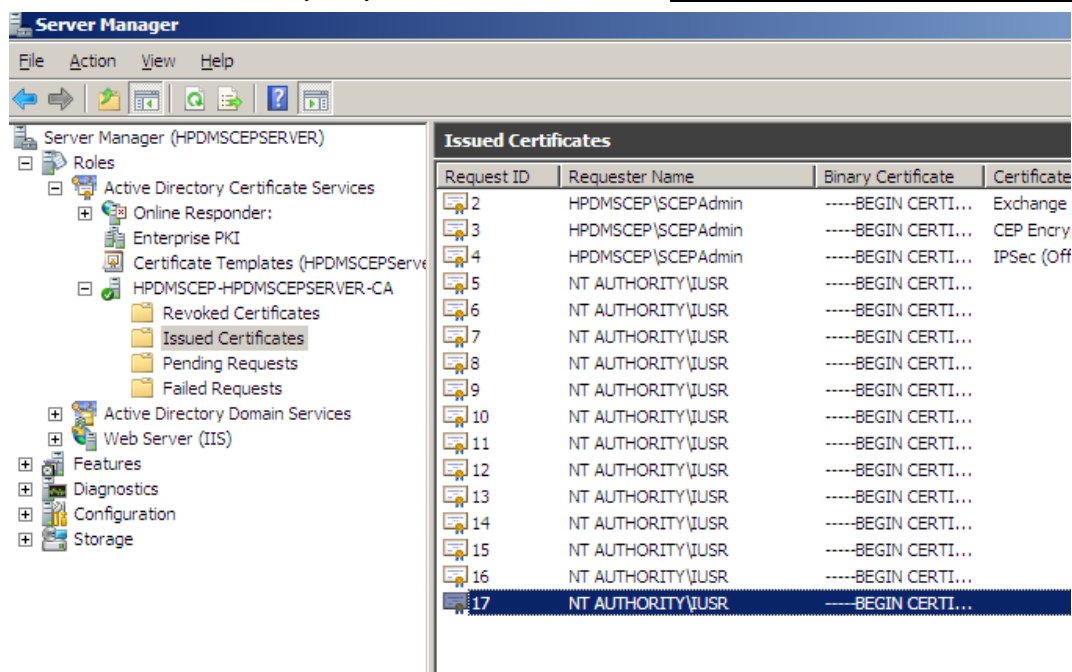


- There is a confirmation when your certificate has successfully installed. You can also confirm that the client certificate has been installed by selecting **Internet Explorer > Tools > Internet Options > Content > Certificates**. In the Personal tab, verify that your certificate is listed.



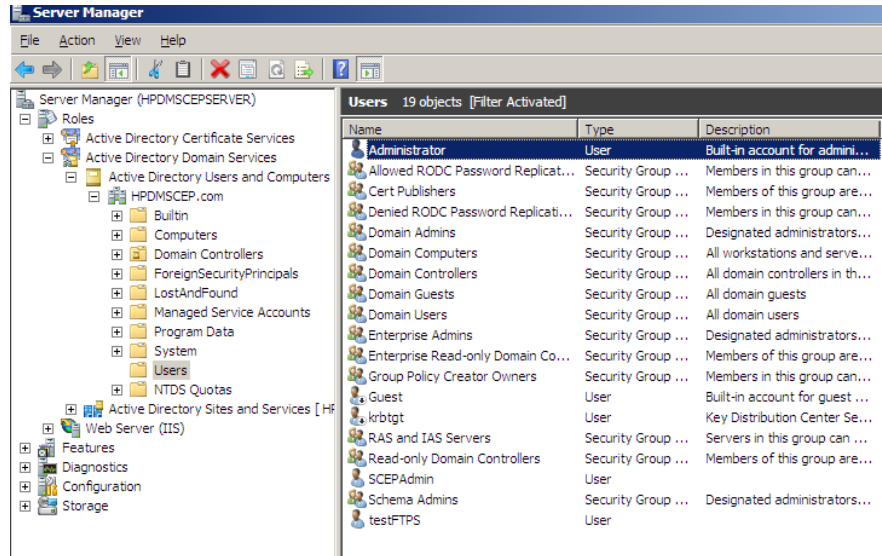
#### Mapping the client certificate to a user account in a domain

- Go to <http://<CA-address>/certsrv>. The CA address is the address of the device where the DC and CA installed.
- Select **Server Manager > Roles > Active Directory Certificate Services > <Your CA>**.
- Click **Issued Certificates**. Verify that you see the certificate issued in [Requesting a client certificate from your CA](#).

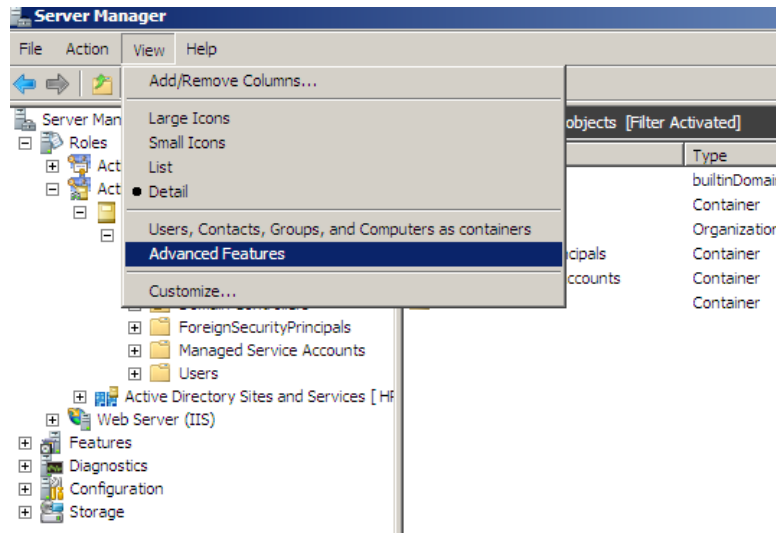


- Right click this certificate, and then click **Open**.
- Export this certificate using the procedure in [Exporting a PEM-format certificate from a certificate](#).
- Go to the DC Server.

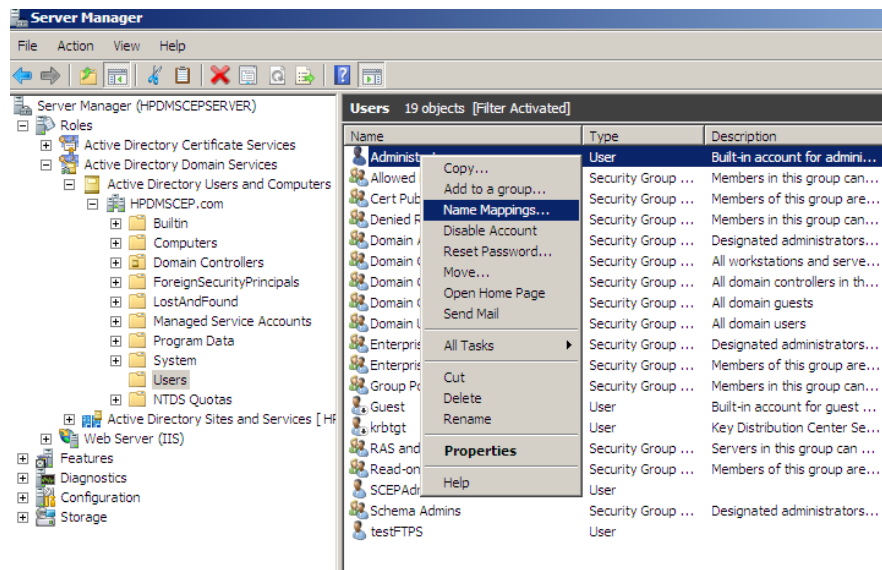
7. Select **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > <Your Domain>**.
8. Select **Users**.



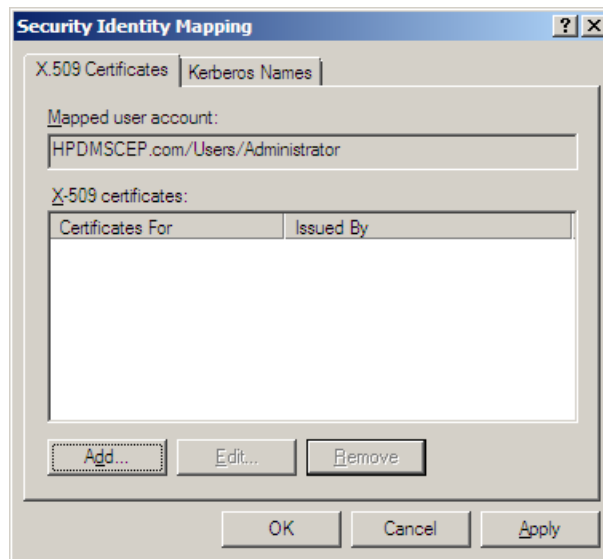
9. Click **View > Advanced Features**.



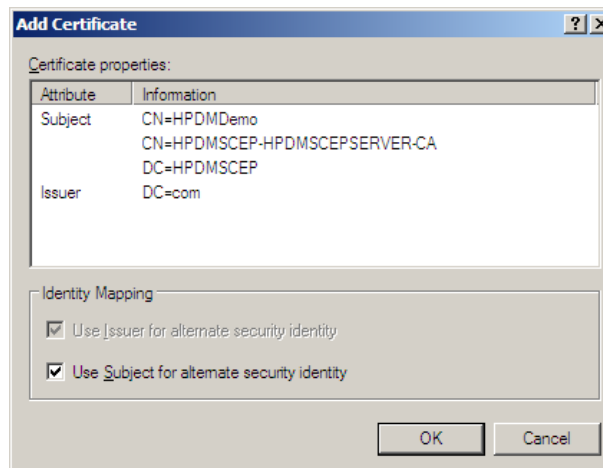
10. Right-click the user name (in this example, **Administrator**), and then click **Name Mappings**.



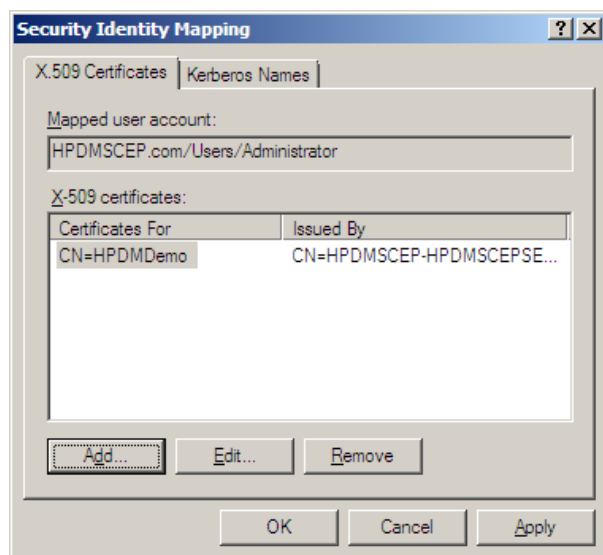
11. In the Security Identity Mapping dialog that appears, select the **X.509 Certificates** tab, and then select **Add**.



12. Select **Browse**, select the location where you saved the user certificate when you exported it in step 5, and then click **Open**.
13. Click **OK**.



14. Click **OK**.

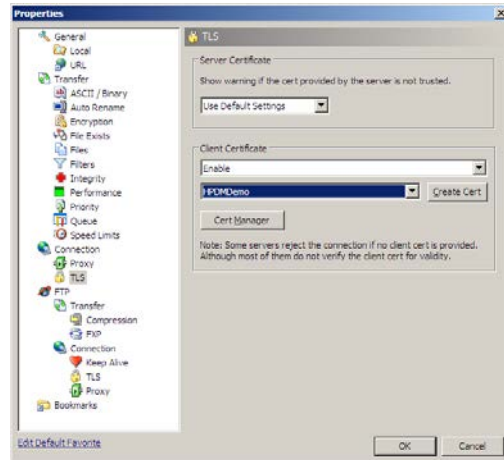


The client certificate is now mapped against the user account.

## Verifying the client-certificate authentication

After enabling client-certificate authentication and mapping the client certificate against a user account in your domain, the configuration of client certificate authentication on the IIS Server is complete. Now, you can verify your configuration via an FTP client. Only a few FTP clients support for using a client certificate when connecting to FTPS server. The following procedure uses SmartFTP, a GUI-based FTP client that supports client-certificate authentication.

1. On the device where you installed the client certificate that you requested, install SmartFTP.
2. Enter your **FTPS Server Address**, user name, and port 990. You do not need a password to use client-certificate authentication.
3. Open the properties dialog of your connection. Under Client Certificate, select **Enable**, and then select the client certificate.



4. Click **OK**.
5. Connect to the FTPS server, and then upload and download a file. If you cannot complete any one of these three functions, verify your configuration step by step.

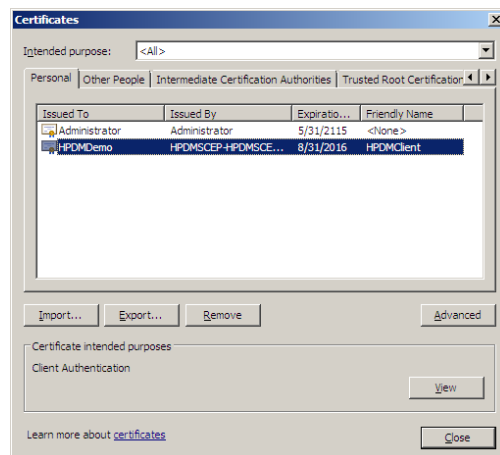
## Deploying a client certificate to HPDM

After you enable client-certificate authentication and configure the IIS FTPS server side, the FTP client must provide the correct client certificate information when connecting to your FTPS server. If there is no client certificate or if the client certificate fails to pass the authentication, the FTPS server refuses the connection. To connect your HPDM components to an FTPS server that has client-certificate authentication enabled, you must deploy your client certificates to all HPDM components.

### Exporting a client certificate

After you have completed the procedure in [Requesting a client certificate from your CA](#), a client certificate is installed on that device. If you want to deploy this client certificate to HPDM, you need to export it first.

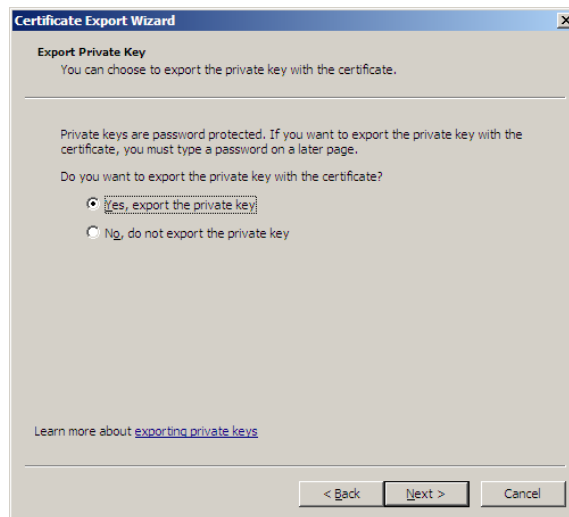
1. Select **Internet Explorer > Tools > Internet Options > Content > Certificates > Personal**, and then select the certificate that you requested.



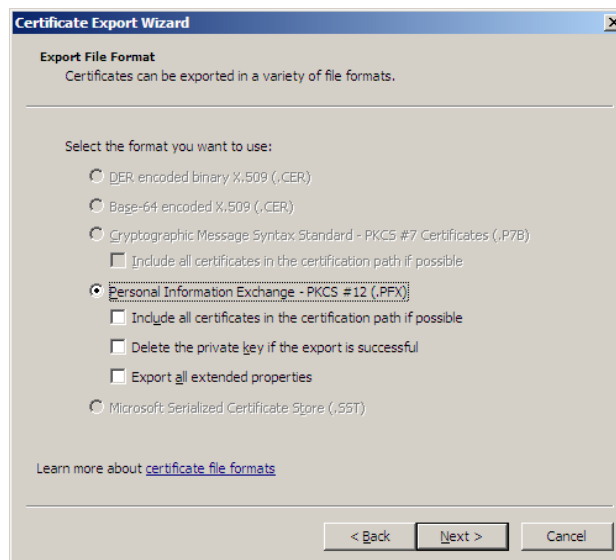
2. Click **Export**.
3. Click **Next**.



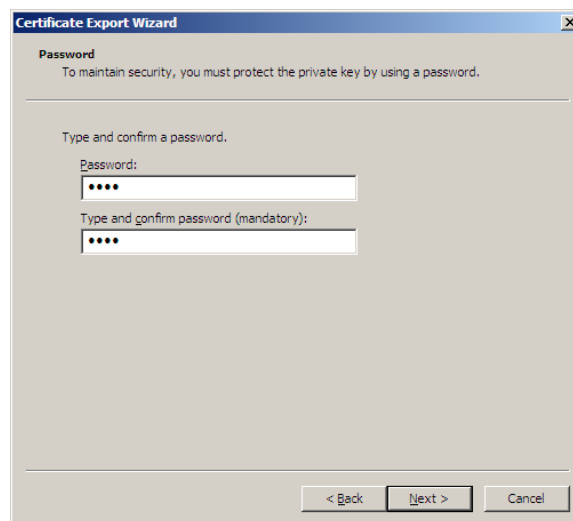
4. Select **Yes, export the private key**, and then click **Next**.



5. Select **Personal Information Exchange – PKCS #12 (.PFX)**, and then click **Next**.

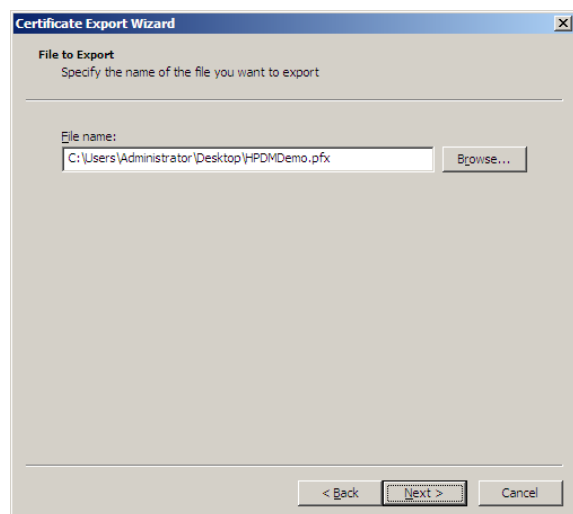


6. Enter a password for the private key.



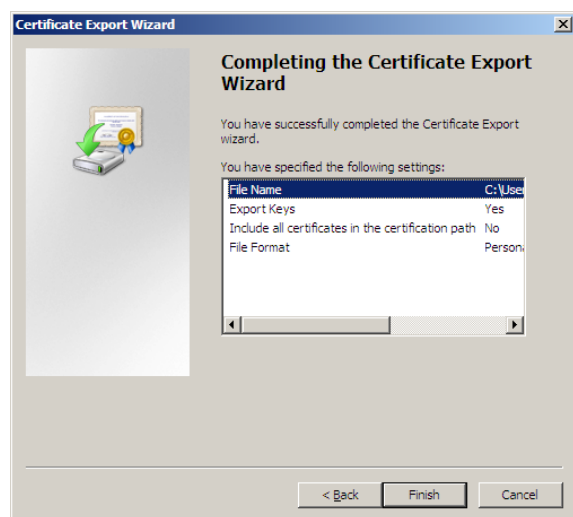
The 'Certificate Export Wizard' window is shown at the 'Password' step. It instructs the user to protect the private key with a password. There are two text input fields: 'Password:' and 'Type and confirm password (mandatory):', both containing four dots. Navigation buttons at the bottom include '< Back', 'Next >', and 'Cancel'.

7. Select **Browse**, select the file you want to export, and then click **Next**.



The 'Certificate Export Wizard' window is shown at the 'File to Export' step. It asks the user to specify the file name. The 'File name:' field contains 'C:\Users\Administrator\Desktop\HPDMDemo.pfx'. A 'Browse...' button is to the right of the field. Navigation buttons at the bottom include '< Back', 'Next >', and 'Cancel'.

8. Click **Finish**.



The 'Certificate Export Wizard' window is shown at the 'Completing the Certificate Export Wizard' step. It displays a success message and a summary of settings. On the left is an icon of a certificate with a green checkmark. The settings table is as follows:

You have specified the following settings:	
File Name	C:\Users\Administrator\Desktop\HPDMDemo.pfx
Export Keys	Yes
Include all certificates in the certification path	No
File Format	Personal

Navigation buttons at the bottom include '< Back', 'Finish', and 'Cancel'.

### Preparing a client certificate and its private key for HPDM

HPDM supports only PEM-format certificates and private keys. To use the PFX-format client certificate exported in [Exporting a client certificate](#), you must export the PEM-format certificate and its private key from the PFX file. HP recommends using OpenSSL. If you need the OpenSSL tool, contact HP Support.

- For HPDM, the file name of the client certificate is `client.pem` and it cannot be changed. In OpenSSL, use the following command to export the client certificate file.  

```
openssl pkcs12 -in yourclientcert.pfx -out client.pem -clcerts -nokeys
```
- For HPDM, the file name of the private key of the client certificate is `client.key` and it cannot be changed. In OpenSSL, use the following command to export the private file.  

```
openssl pkcs12 -in yourclientcert.pfx -out client.key -clcerts -nocerts
```
- When you export the certificate and private key, you must provide the password entered when you exported the PFX file, and then enter a new password for the private key.

### Deploying a client certificate to HPDM components

After preparing the `client.pem` file and the `client.key` file, you must deploy them to each HPDM component. If you do not, HPDM cannot connect to an FTPS server that has client-certificate authentication enabled.

To deploy the files to HPDM Console, HPDM Server, HPDM Gateway and Master Repository Controller:

1. Copy `client.pem` and `client.key` to the folder  
`%HPDMInstallPath%\Certificates\repos_certs\`.
2. To deploy the password for the client key, open a command prompt, change the current path to  
`%HPDMInstallPath%\Certificates\`, and then run the command `dmenc <password>` where `<password>` is the password you entered when you exported the PEM-format private key.  
For example, if the password is HPDM, run command `dmenc HPDM`.

To deploy the files to HPDM Agents running a Windows Embedded operating system:

1. Copy `client.pem` and `client.key` to the folder `c:\windows\xpeagent\repos_certs\`.
2. Deploy the password of the private key by sending the following script task to the devices via HPDM.  
`c:\windows\xpeagent\dmenc <password>`

To deploy the files to HPDM Agents running HP ThinPro:

1. Copy `client.pem` and `client.key` to the folder `/etc/hpdmagent/repos_certs/`.
2. Deploy the password of the private key by sending the following script task to the devices via HPDM.  
`/usr/sbin/dmenc <password>`

---

### Note

If you want each HPDM Agent to use a different client certificate, you must request each client certificate, map each client certificate to a user account, prepare `client.pem` and `client.key` files for each client certificate, and then deploy each client certificate to a different HPDM Agents, one at a time.

---

## For more information

To read more about HP Device Manager, go to [hp.com/go/hpdm](http://hp.com/go/hpdm).

### Sign up for updates

[hp.com/go/getupdated](http://hp.com/go/getupdated)

---

© Copyright 2015 HP Development Company, L.P.

ARM is a registered trademark of ARM Limited. Java is a registered trademark of Oracle and/or its affiliates. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Pentium is a trademark of Intel Corporation in the U.S. and other countries.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

First Edition: October 2015

