

Implement Security Certificates

4BzSoftware@gmail.com Common Support 011

Released on 2013-06-01, last updated on 2013-11-20

4BZSoftware

Table of Contents

1. Introduction	3
2. Prerequisites	4
3. Quick Guide	5
3.1 Configure Server running NAV Server Service	5
3.2 Configure Server running NAV Web Server Component	6
3.3 Configure NAV Client	7
4. How to	8
4.1 Open Certificates snap-in for MMC with Computer account	8
4.2 Import "NavServiceTRCA.cer" certificate file to TRCA group	12
4.3 Import "NavServiceTRCA.crl" certificate revocation file to TRCA	15
4.4 Import "NavServiceCert.pfx" file to Personal group	18
4.5 Grant access "NavServiceCert" certificate to service account	22
4.6 Configure NAV Server Service by NAV Administration Tool	24
4.7 Configure NAV Web Server - "web.config" file	25
4.8 Configure NAV Client - "ClientUserSettings.config" file	27
5. Troubleshoot	28
5.1 The client could not establish a connection to the Microsoft Dynamics NAV Server. FaultCode = 'InvalidSecurity' Reason = 'An error occurred when verifying security for the message.'	28
5.2 The service MicrosoftDynamicsNavServer\$DynamicsNAV70 failed to start... It is likely that certificate 'CN=NavServiceCert' may not have a private key that is capable of key exchange or the process may not have access rights for the private key	29
6. Version Control	30

1. Introduction

Document helps you implement Security Certificates Authentication for Navision 2013.

It is required by UserName and NavUserPassword credential types.

To make it easy, all certificates are generated and you just import them for using:

- Valid time: from 2013-01-01 to 2040-01-01.
- Password: "navservice".
- Thumbprint: "4c 69 ca bc 65 4d 07 d5 61 f1 43 61 21 55 44 00 bf 30 79 f5".

All needed material can be downloaded at SkyDrive link

<https://skydrive.live.com/?cid=1322D544FED91559&id=1322D544FED91559%21107>

We make every effort to ensure that there are no errors. However, no one is perfect, and mistakes do occur. If you find an error or have any idea, we would be very grateful for your feedback.

Reference:

- Walkthrough: Implementing Security Certificates in a Test Environment
[http://msdn.microsoft.com/en-us/library/gg502478\(v=nav.70\).aspx](http://msdn.microsoft.com/en-us/library/gg502478(v=nav.70).aspx)
- How to: Configure User Authentication for the Microsoft Dynamics NAV Web Client
[http://msdn.microsoft.com/en-us/library/jj551778\(v=nav.70\).aspx](http://msdn.microsoft.com/en-us/library/jj551778(v=nav.70).aspx)

2. Prerequisites

- The Certificates snap-in for Microsoft Management Console (MMC).
- "NavServiceTRCA.cer" file: Root Certification Authority for both Server and Client.
- "NavServiceTRCA.crl" file: Certificate Revocation for both Server and Client.
- "NavServiceCert.pfx" file: Personal Information Exchange Certificate for Server.

4BZSoftware

3. Quick Guide

3.1 Configure Server running NAV Server Service

1. [Open Certificates snap-in for MMC with Computer account.](#)
2. [Import "NavServiceTRCA.cer" certificate file to Trusted Root Certification Authorities group.](#)
3. [Import "NavServiceTRCA.crl" certificate revocation file to the same group.](#)
4. [Import "NavServiceCert.pfx" personal information exchange file to Personal group](#)
(Password is "navservice")
5. [Grant access "NavServiceCert" certificate to service account that starts NAV Server service.](#)
6. [Open Microsoft Dynamics NAV Administration Tool to edit desired instance.](#)
7. [Change ClientServicesCredentialType \(General tab\) to UserName or NavUserPassword.](#)
8. [Add thumbprint to CertificateThumbprint \(Client Services tab\)](#)
(Thumbprint is "4c 69 ca bc 65 4d 07 d5 61 f1 43 61 21 55 44 00 bf 30 79 f5")
9. [Save and restart the Microsoft Dynamics NAV Server instance.](#)
10. Check Windows Firewall.

If there is a problem, please refer to Troubleshoot or see Windows Event Viewer.

3.2 Configure Server running NAV Web Server Component

1. [Open Certificates snap-in for MMC with Computer account.](#)
2. [Import "NavServiceTRCA.cer" certificate file to Trusted Root Certification Authorities group.](#)
3. [Import "NavServiceTRCA.crl" certificate revocation file to the same group.](#)
4. [Edit "C:\Program Files\Microsoft Dynamics NAV\70\Web Client\web.config" file.](#)
5. [Switch <authentication mode="Windows" /> to <authentication mode="Forms">](#)
6. [Uncomment ClientServicesCredentialType key with UserName or NavUserPassword value.](#)
7. [Add "NavServiceCert" value to DnsIdentity key.](#)
8. [Save "C:\Program Files\Microsoft Dynamics NAV\70\Web Client\web.config" file.](#)
9. Check Windows Firewall.
10. Test with browsers on local and other computers.

If there is a problem, please refer to Troubleshoot or see Windows Event Viewer.

3.3 Configure NAV Client

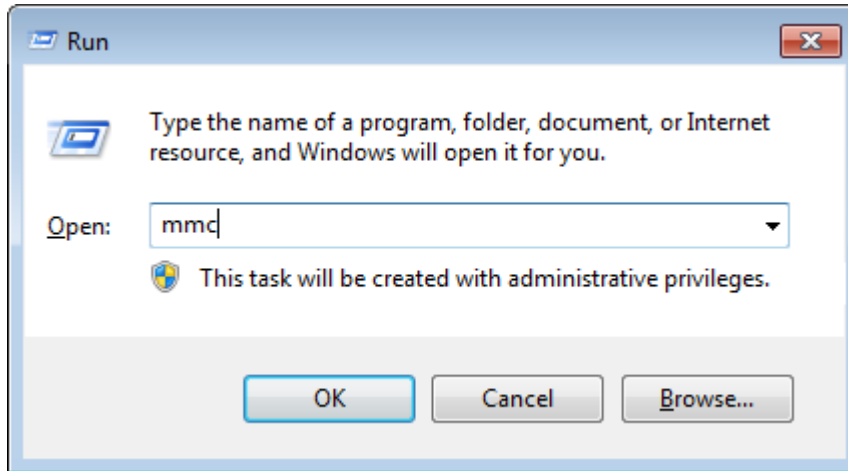
1. [Open Certificates snap-in for MMC with Computer account.](#)
2. [Import "NavServiceTRCA.cer" certificate file to Trusted Root Certification Authorities group.](#)
3. [Import "NavServiceTRCA.crl" certificate revocation file to the same group.](#)
4. [Edit "%AppData%\Microsoft\Microsoft Dynamics NAV\70\ClientUserSettings.config" file.](#)
5. [Change value of ClientServicesCredentialType key to UserName or NavUserPassword.](#)
6. [Add "NavServiceCert" value to DnsIdentity key.](#)
7. [Save "%AppData%\Microsoft\Microsoft Dynamics NAV\70\ClientUserSettings.config" file.](#)
8. Test with Microsoft Dynamics NAV Windows client (Role Tailored client).

If there is a problem, please refer to Troubleshoot or see Windows Event Viewer.

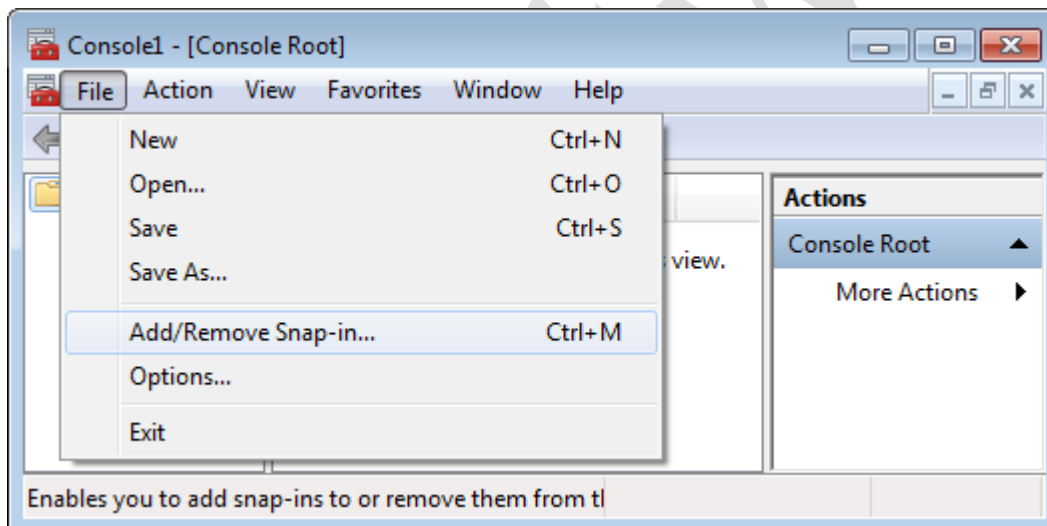
4. How to

4.1 Open Certificates snap-in for MMC with Computer account

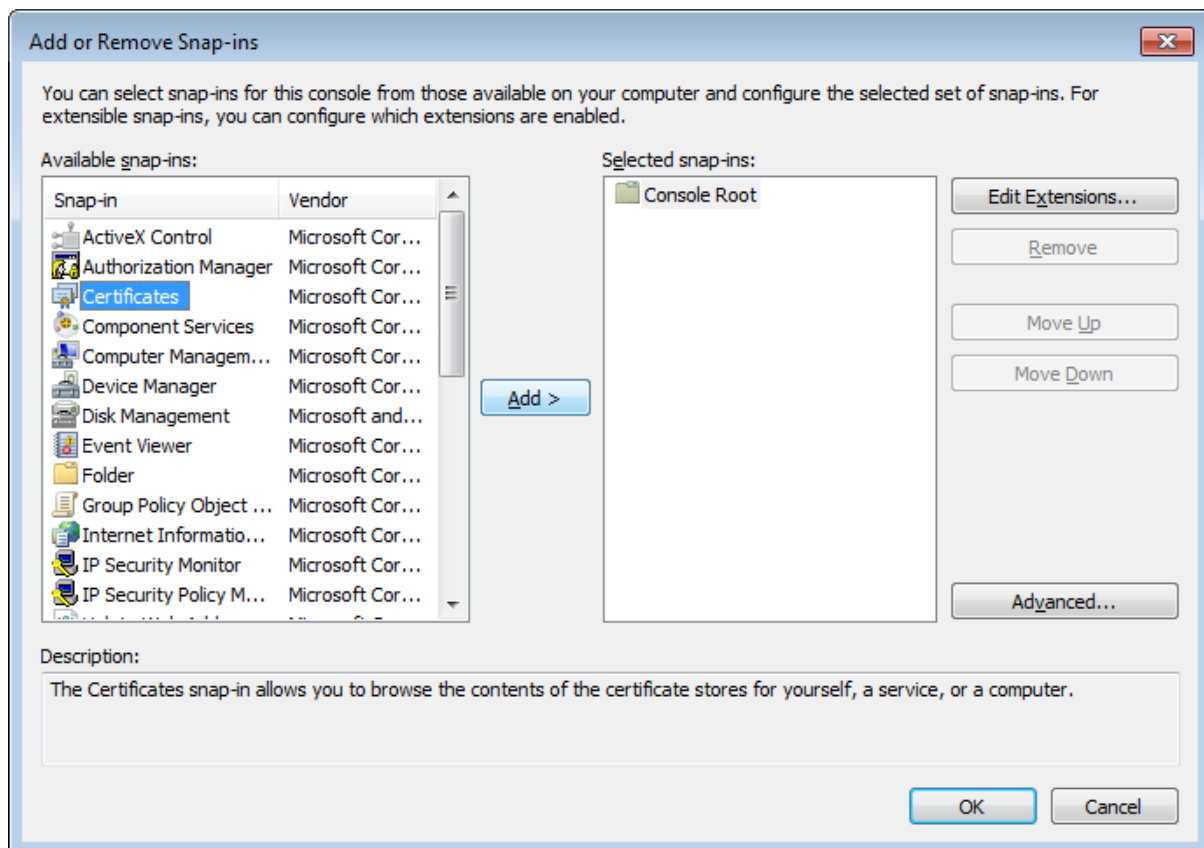
1. Press {Windows + R} and enter “mmc” to open Microsoft Management Console



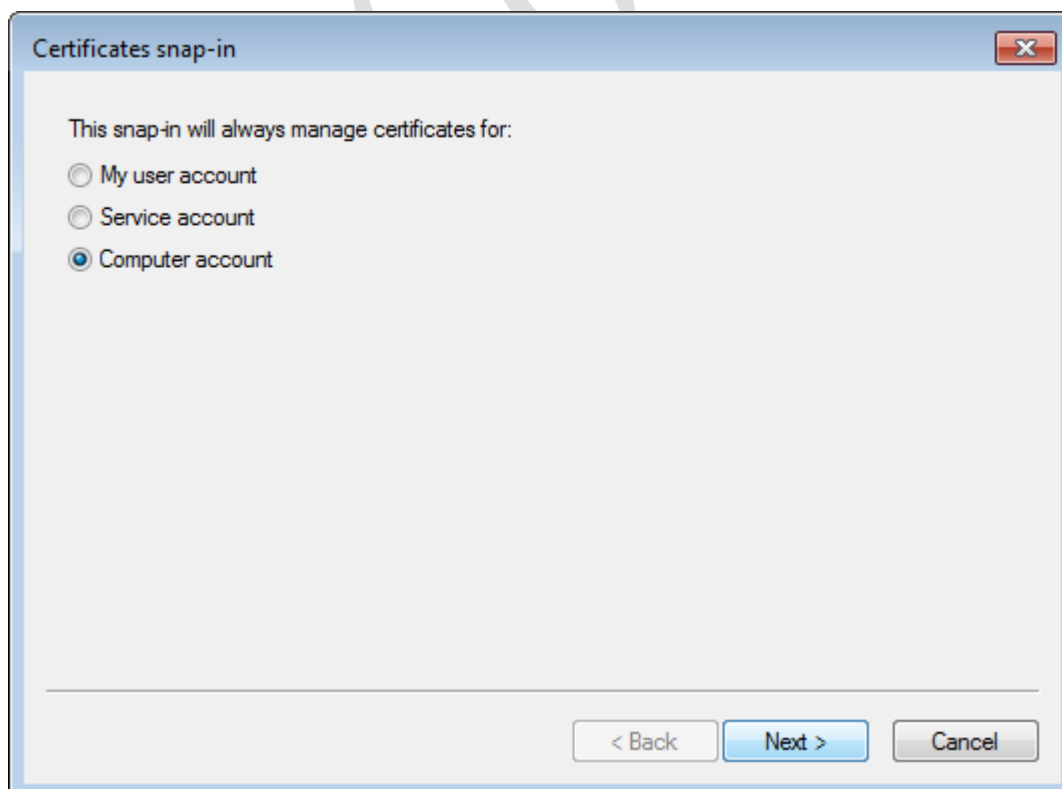
2. Press {Ctrl + M} or click File → Add/Remove Snap-in... to add or remove snap-ins

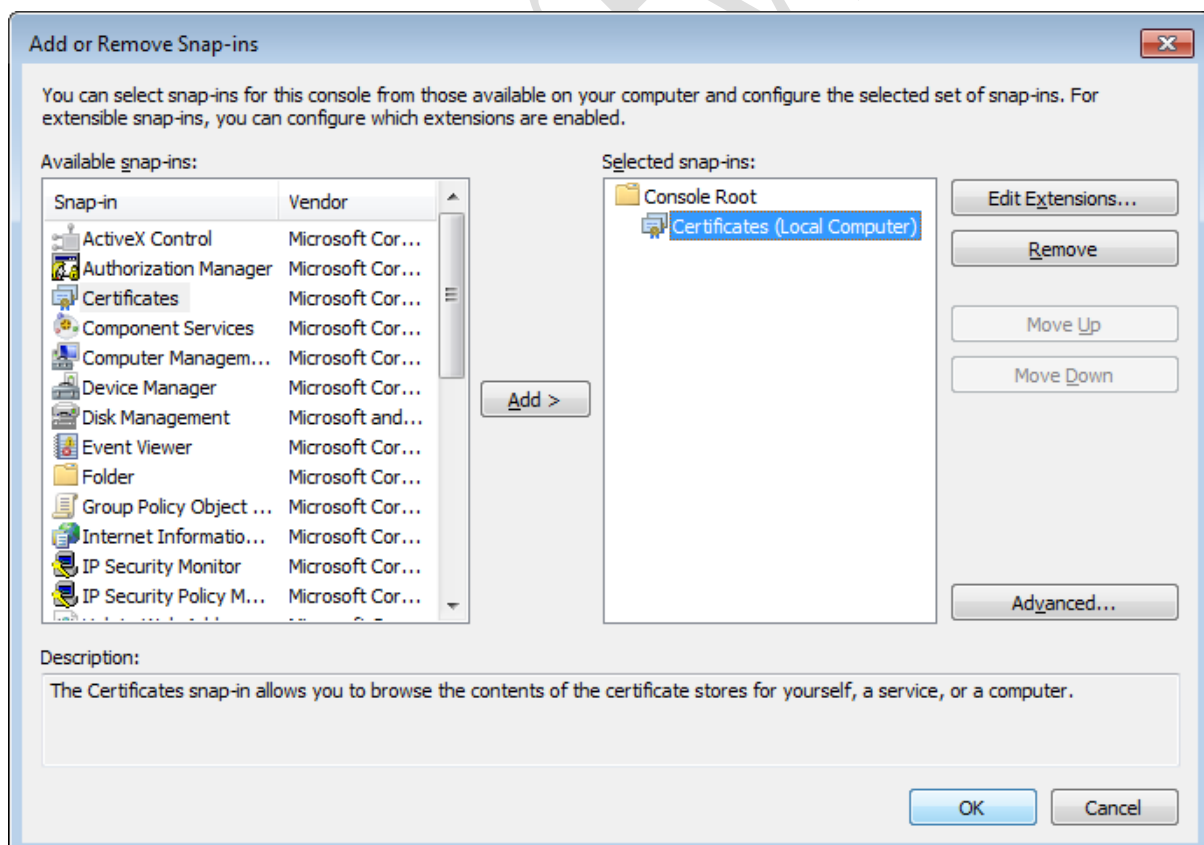
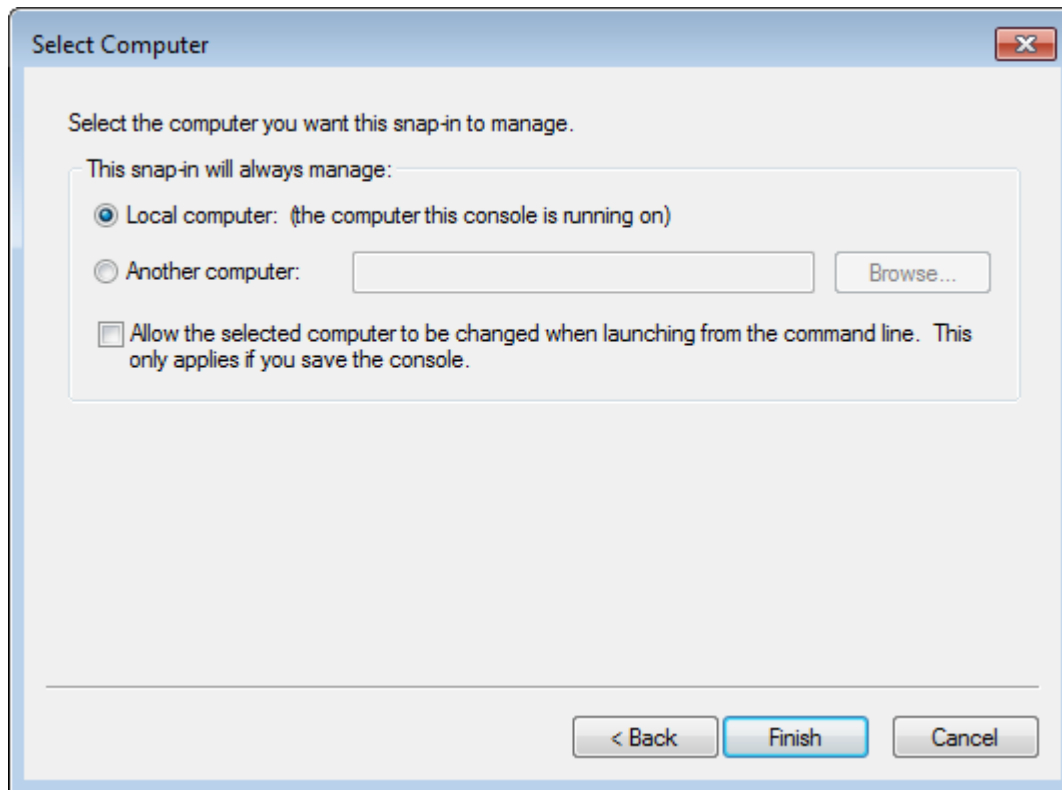


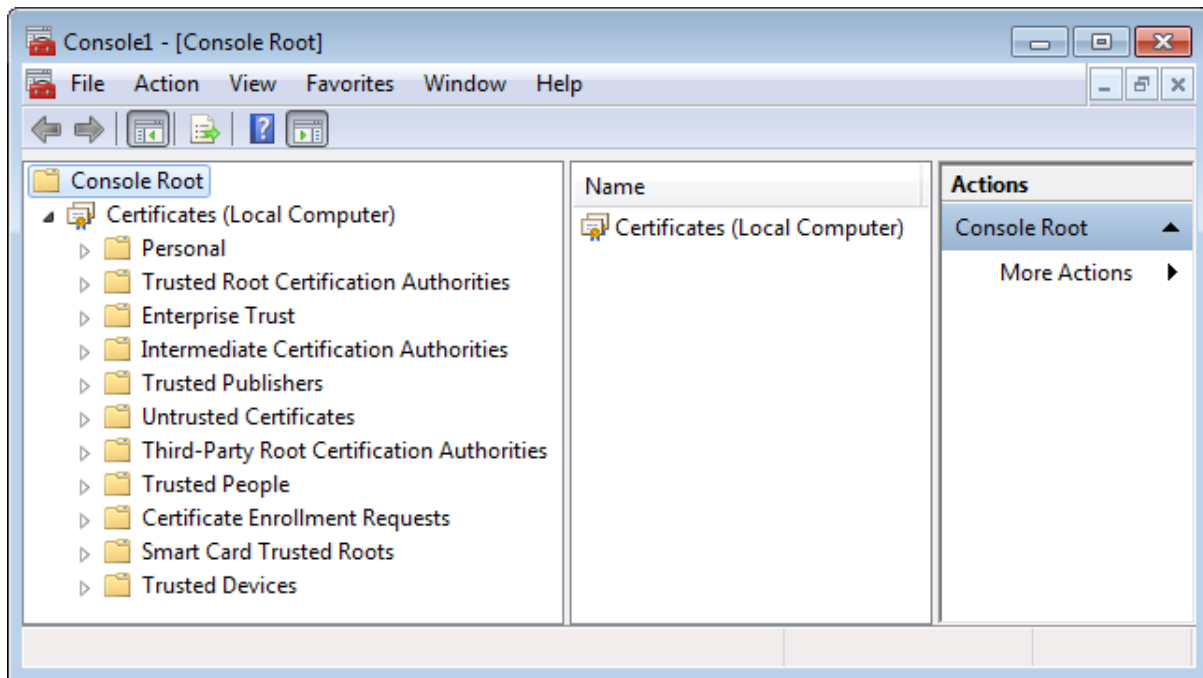
3. Select Certificates and click Add



4. Select Computer account and click Next → Finish → OK

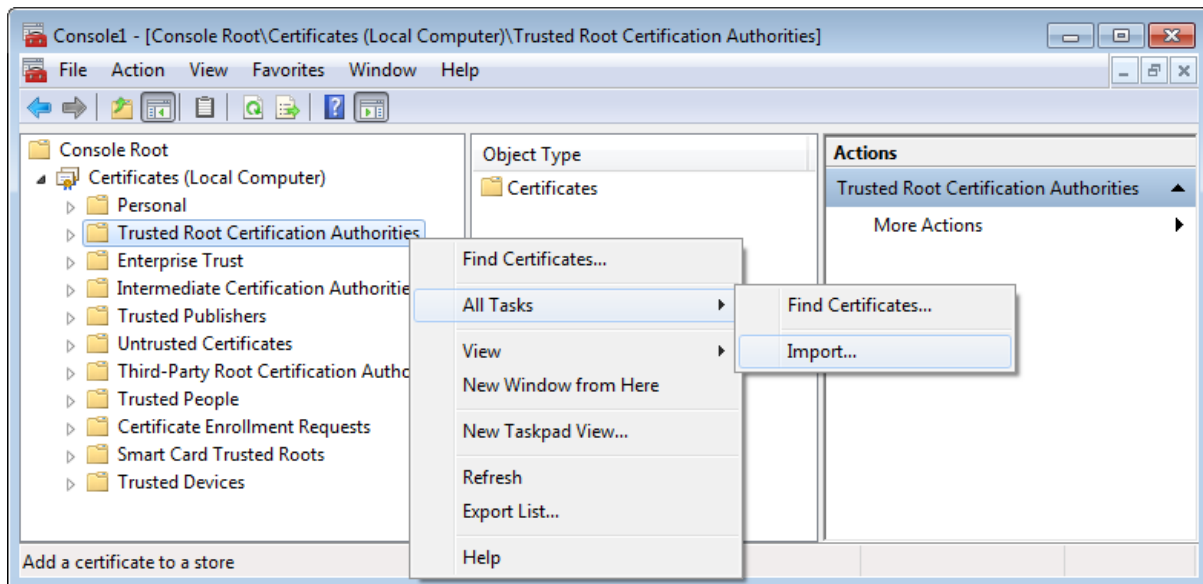






4.2 Import “NavServiceTRCA.cer” certificate file to TRCA group

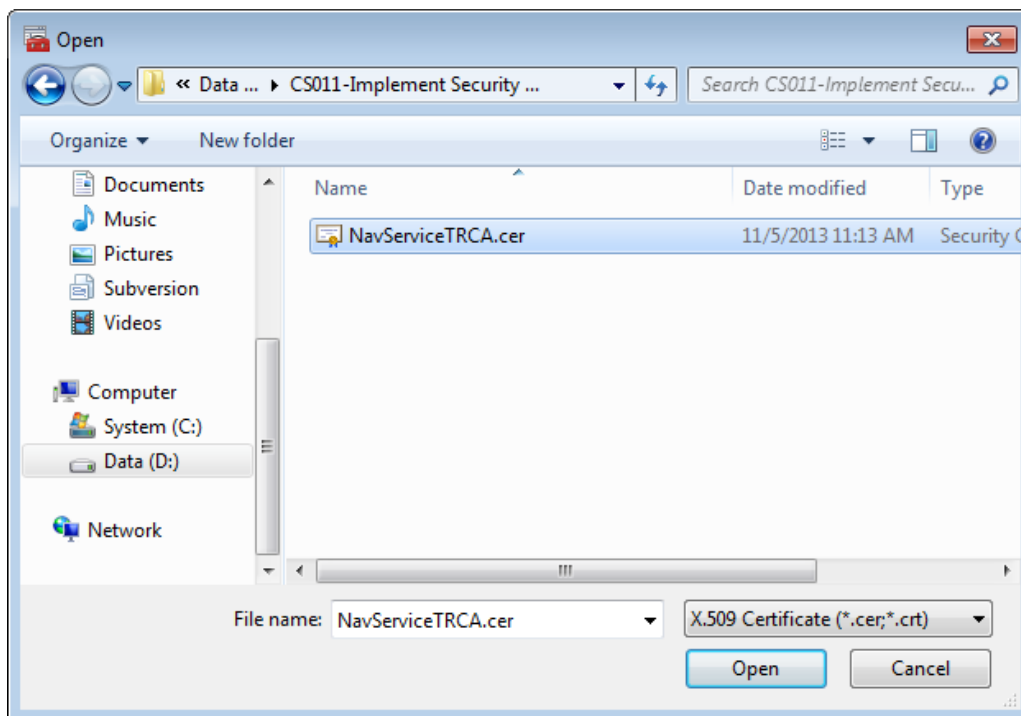
1. Right-click Trusted Root Certification Authorities → All Tasks → Import...



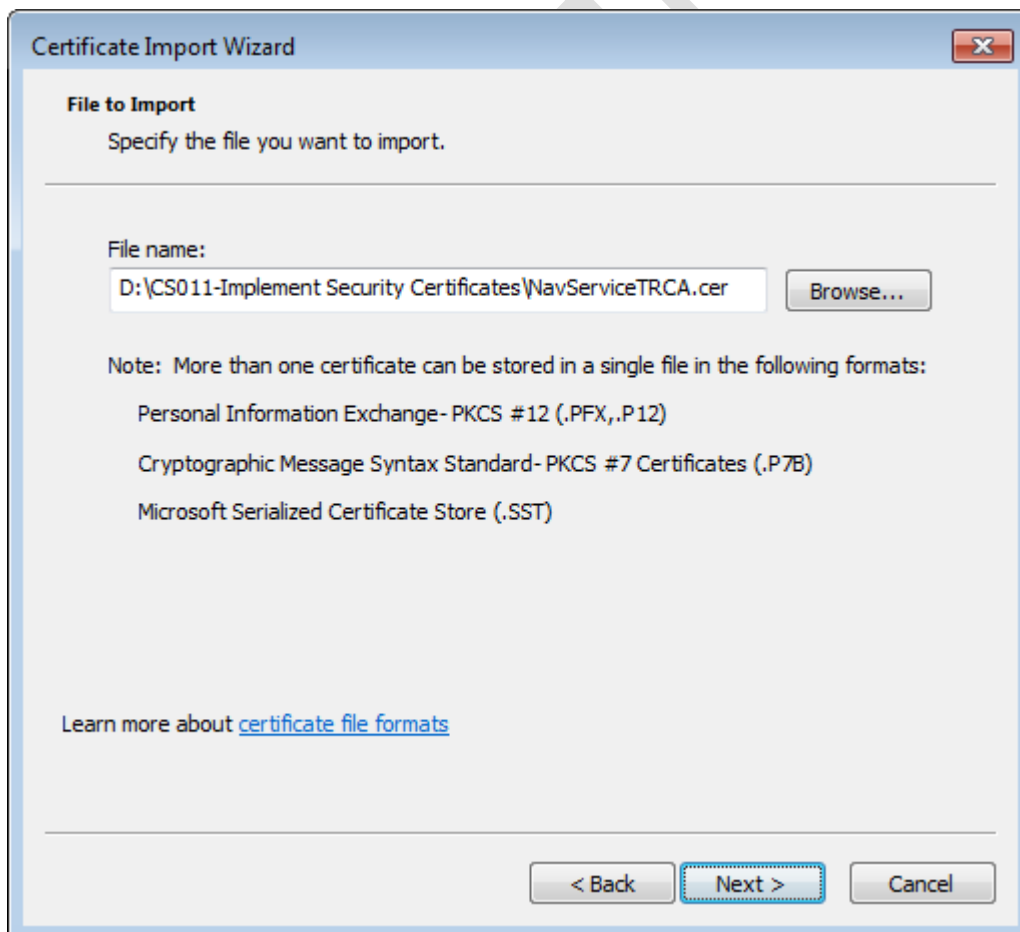
2. Click Next



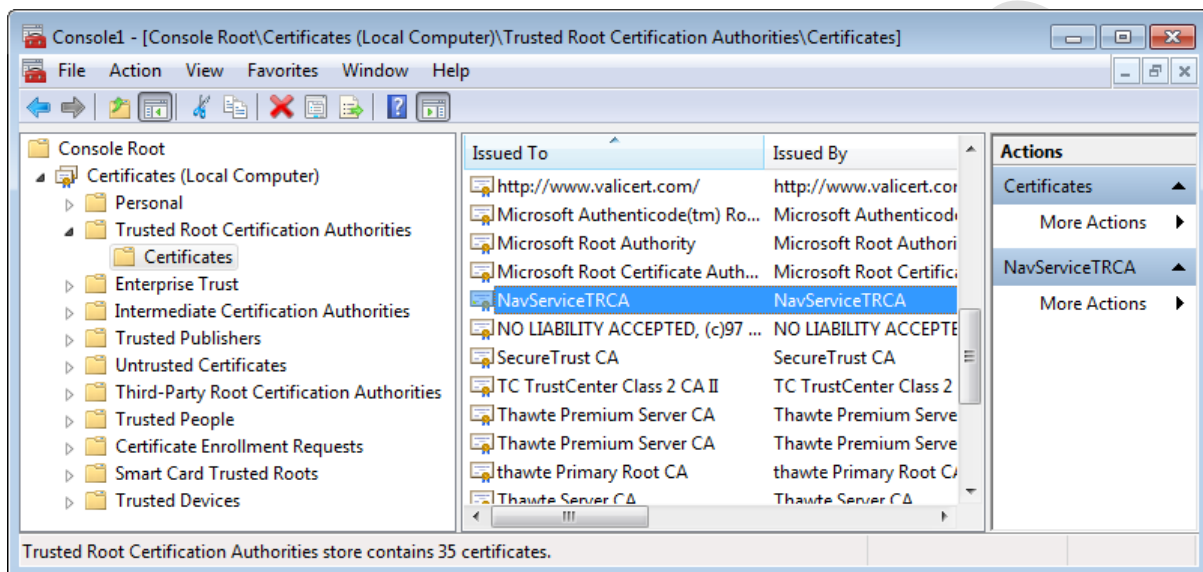
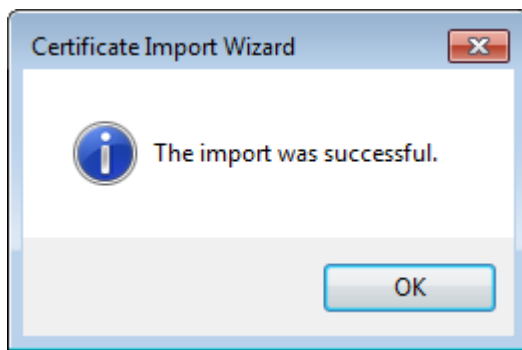
3. Browse "NavServiceTRCA.cer" file and click Open



4. Click Next

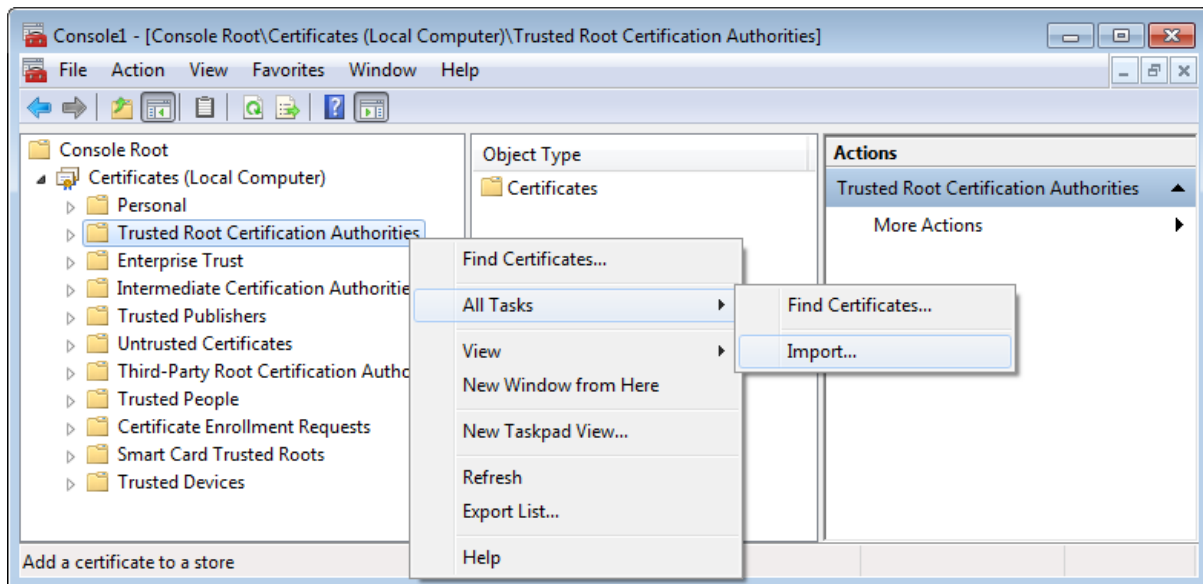


5. Click Next → Finish → OK



4.3 Import “NavServiceTRCA.crl” certificate revocation file to TRCA

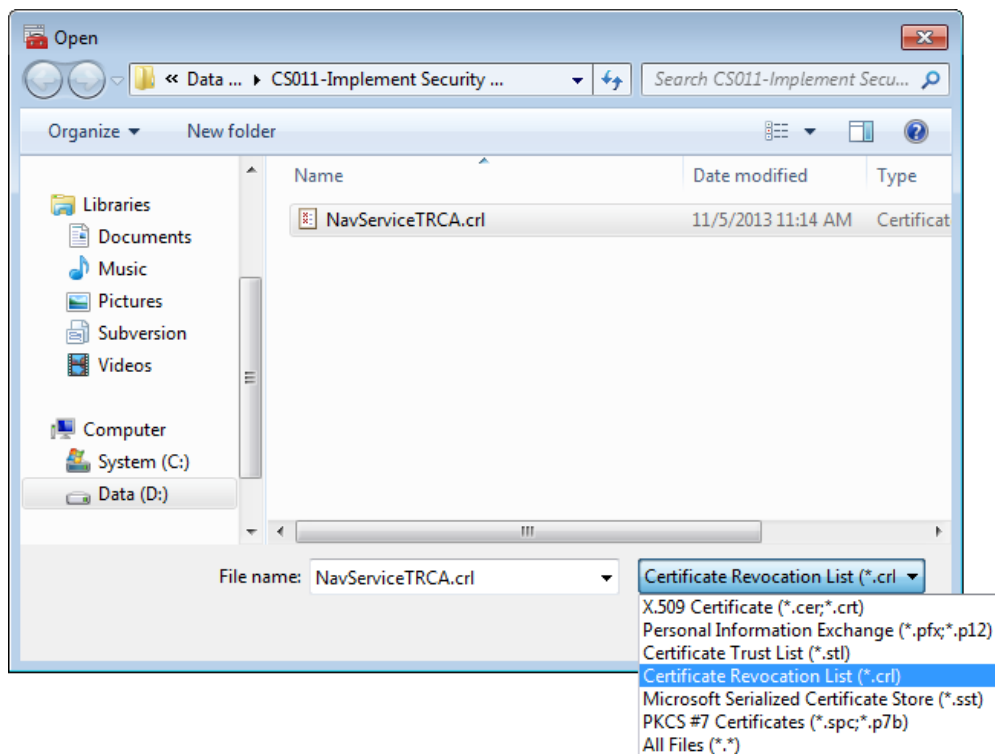
1. Right-click Trusted Root Certification Authorities → All Tasks → Import...



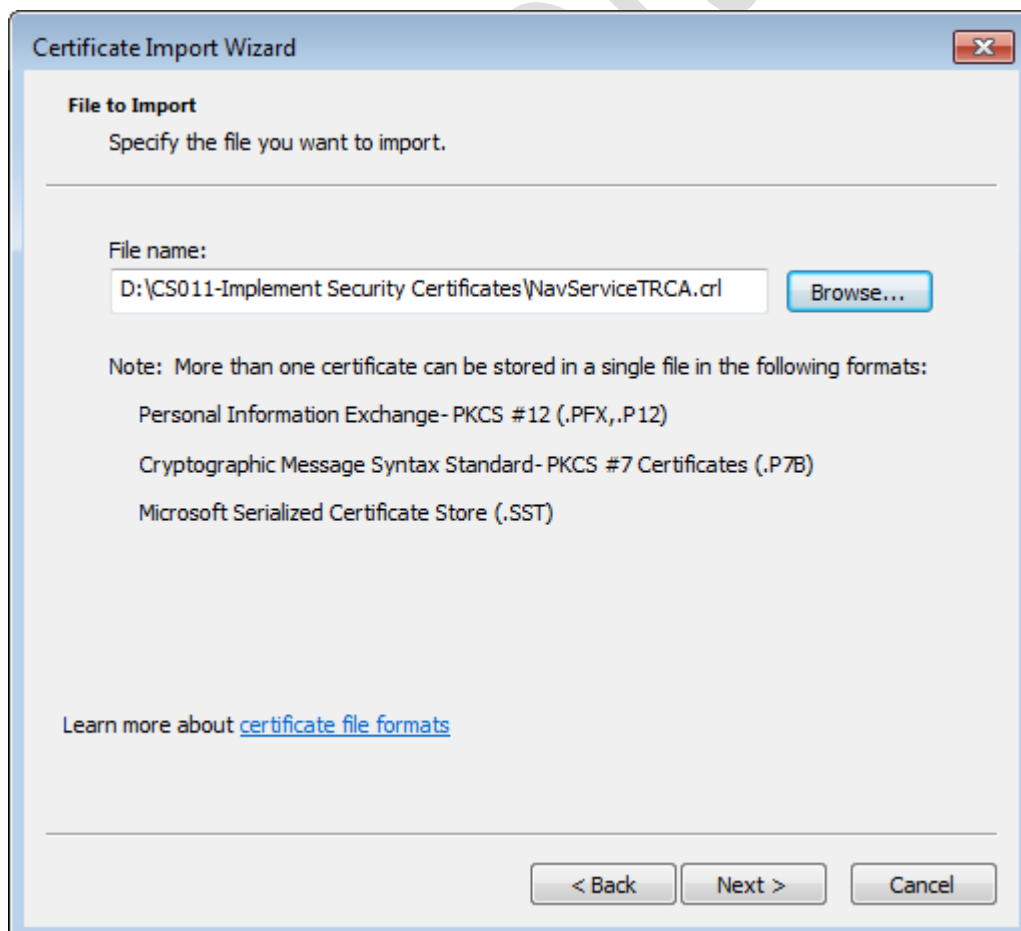
2. Click Next



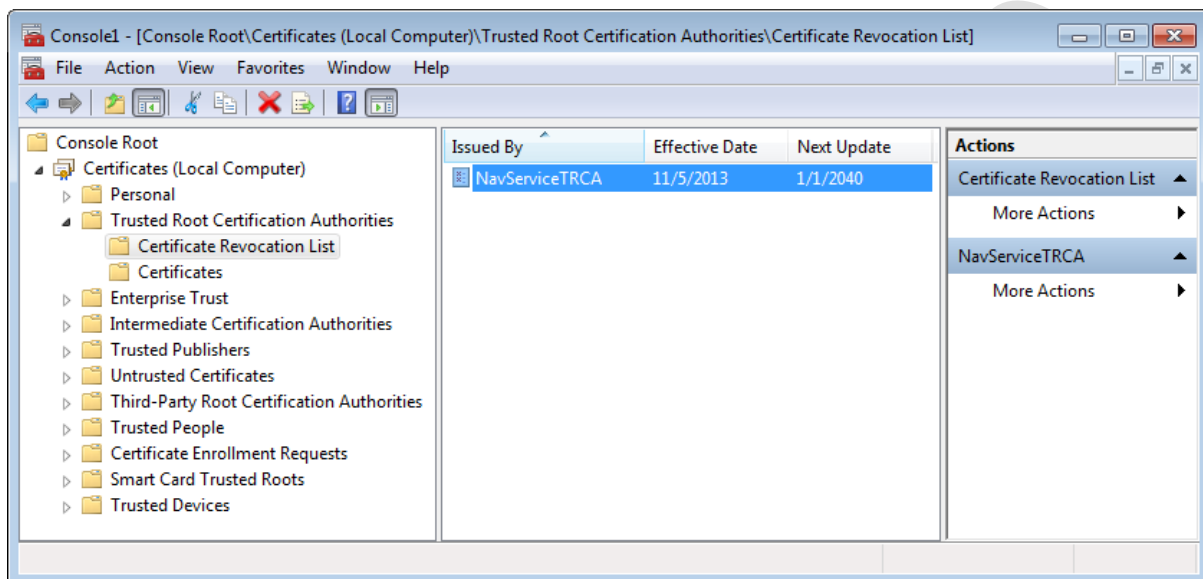
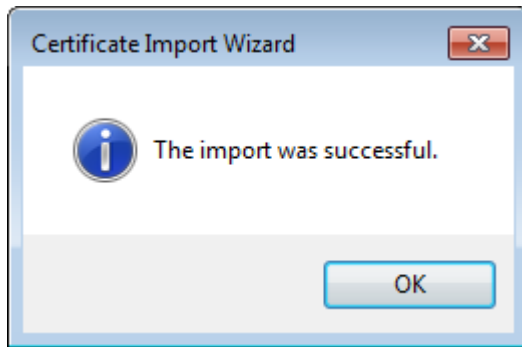
3. Browse “NavServiceTRCA.crl” file and click Open



4. Click Next

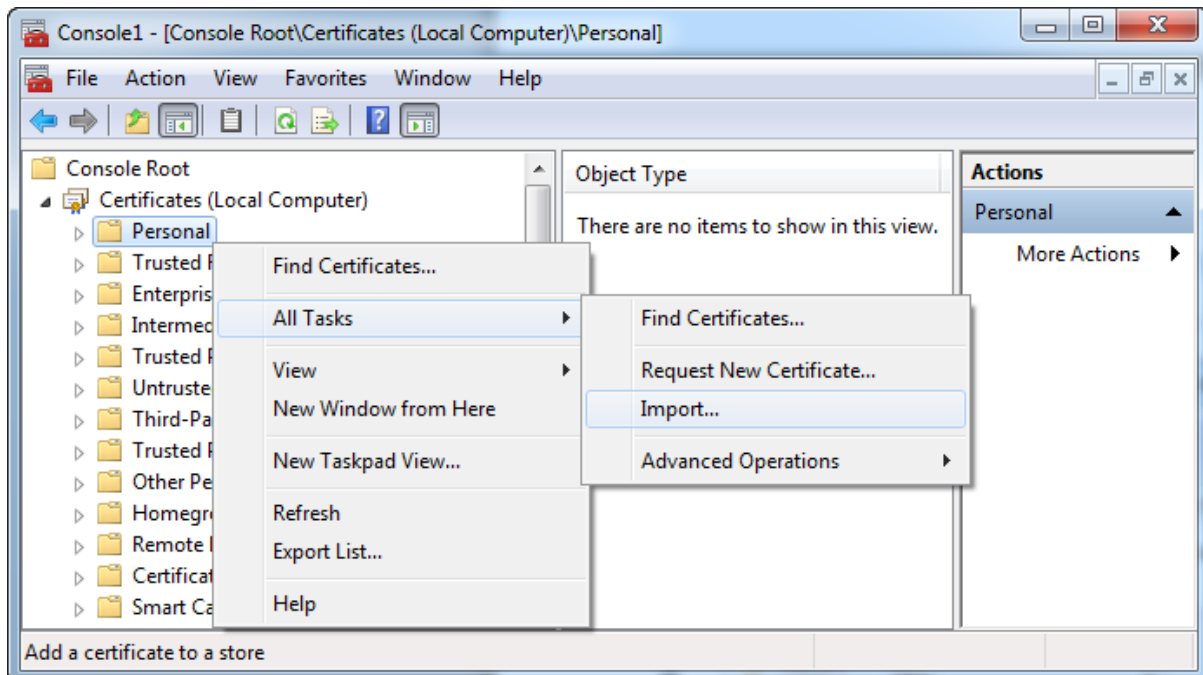


5. Click Next → Finish → OK



4.4 Import “NavServiceCert.pfx” file to Personal group

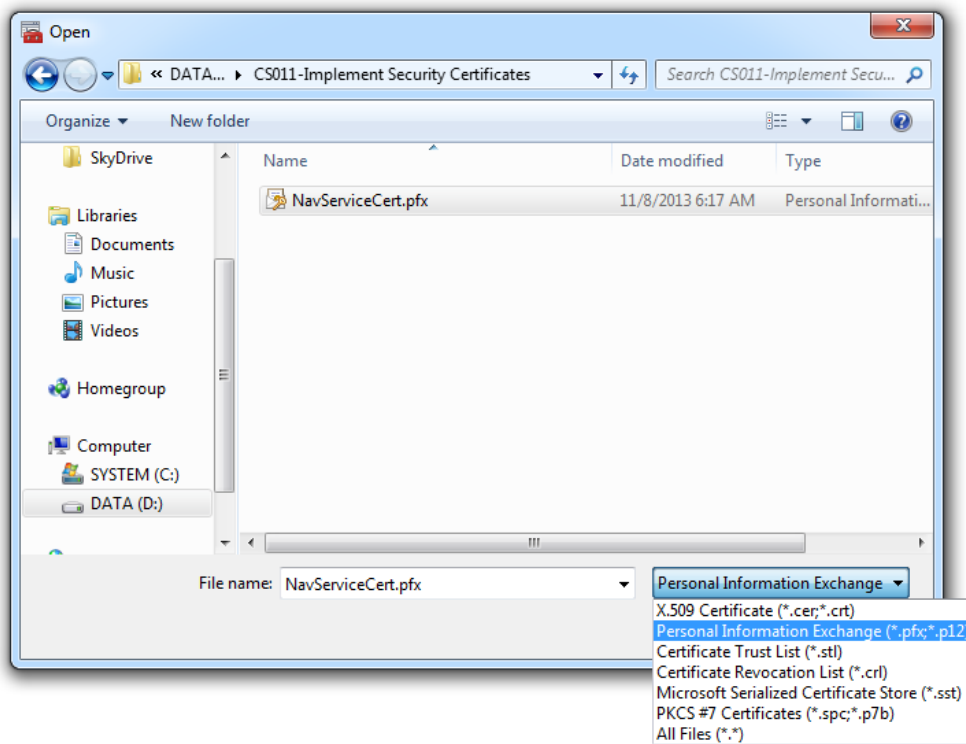
1. Right-click Personal → All Tasks → Import...



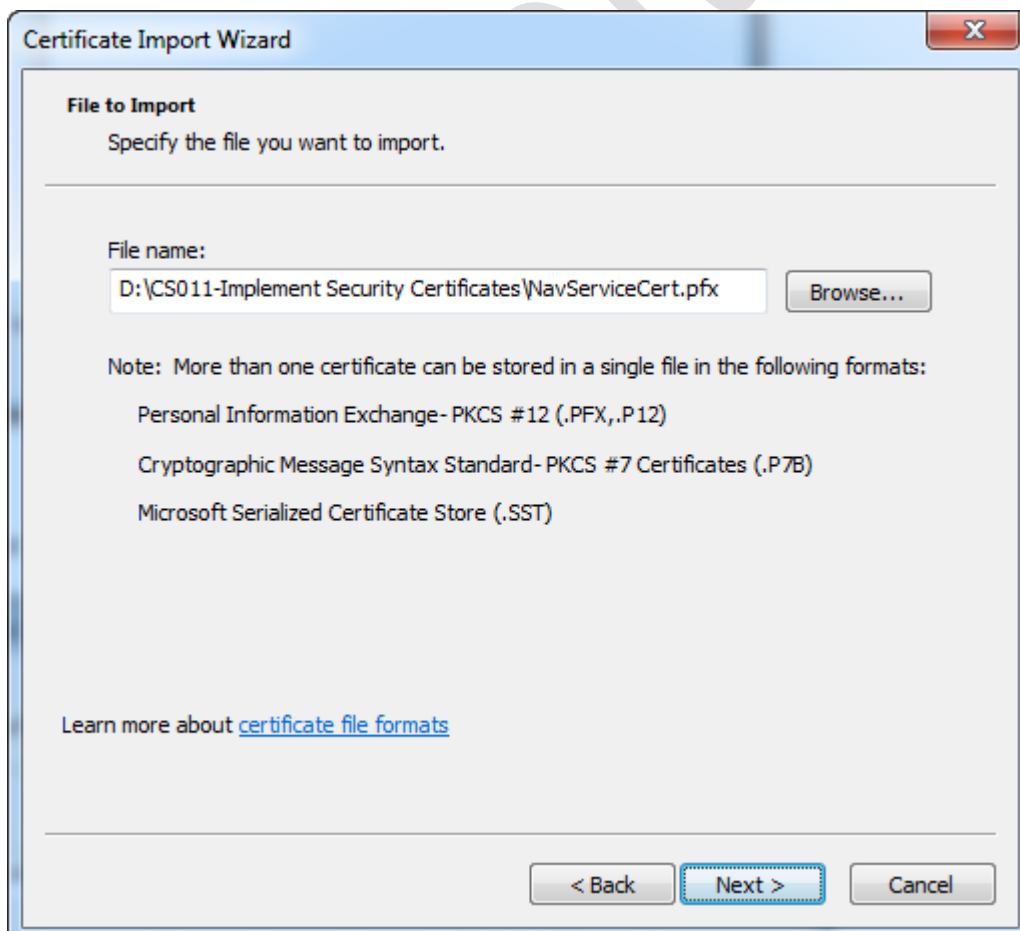
2. Click Next



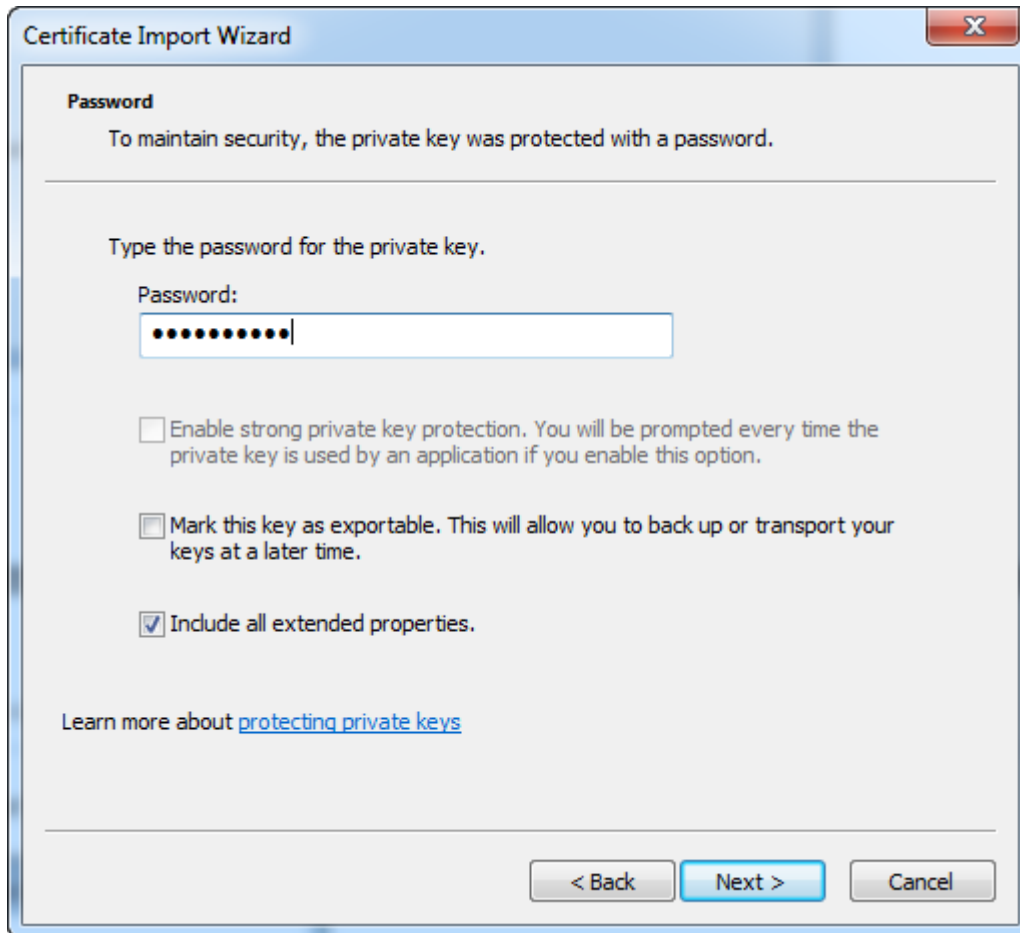
3. Browse "NavServiceCert.pfx" file and click Open



4. Click Next



5. Type password “navservice” and click Next



The image shows a Windows 'Certificate Import Wizard' dialog box. The title bar reads 'Certificate Import Wizard'. The main content area is titled 'Password' and contains the text: 'To maintain security, the private key was protected with a password.' Below this, it says 'Type the password for the private key.' There is a text input field labeled 'Password:' which contains ten dots, indicating a masked password. Below the input field are 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.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (unchecked), and 'Include all extended properties.' (checked). At the bottom left, there is a link: 'Learn more about [protecting private keys](#)'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

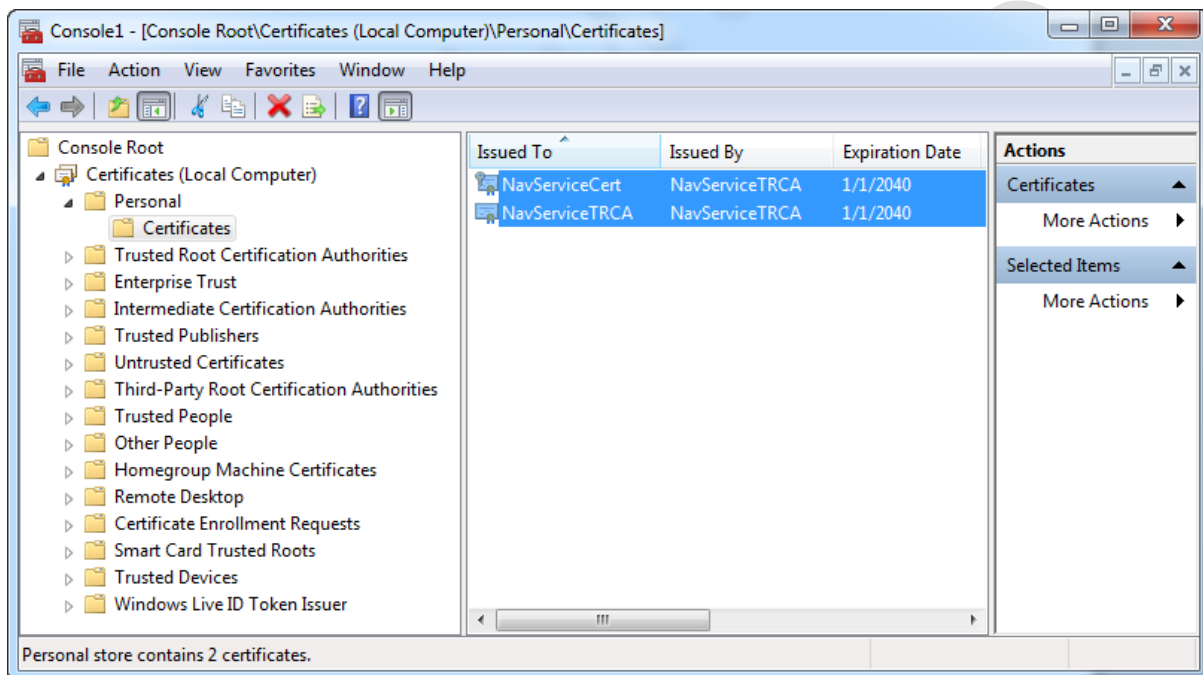
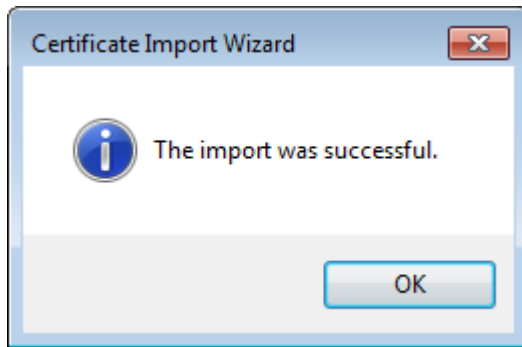
☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☒ Include all extended properties.

Learn more about [protecting private keys](#)

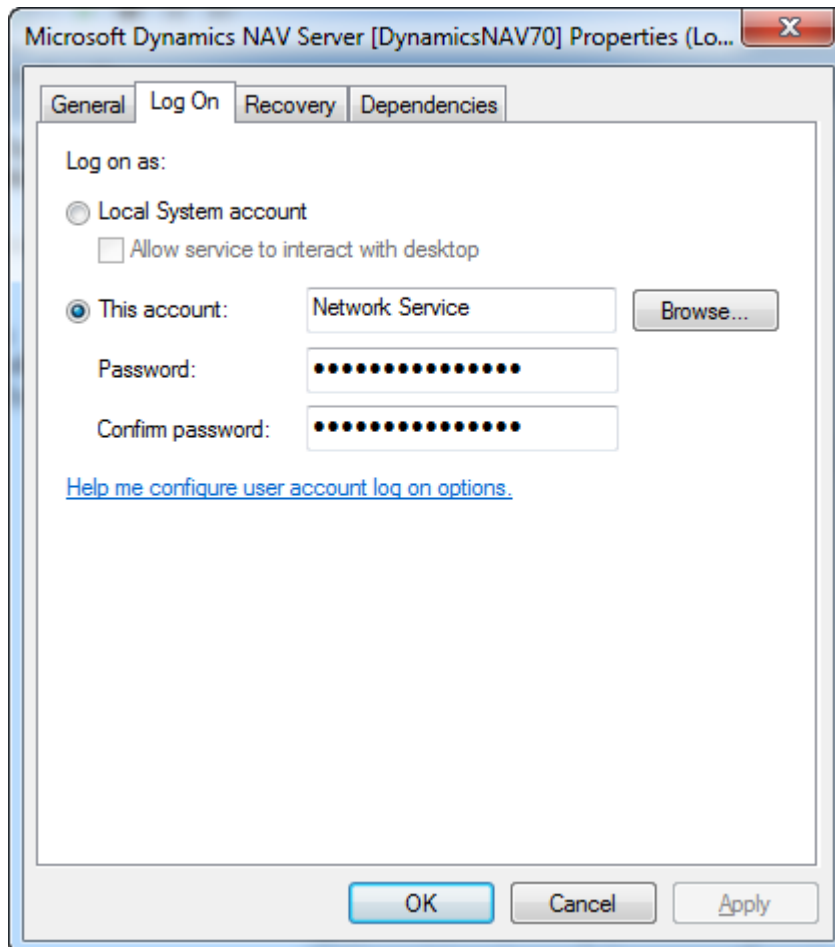
< Back Next > Cancel

6. Click Next → Finish → OK

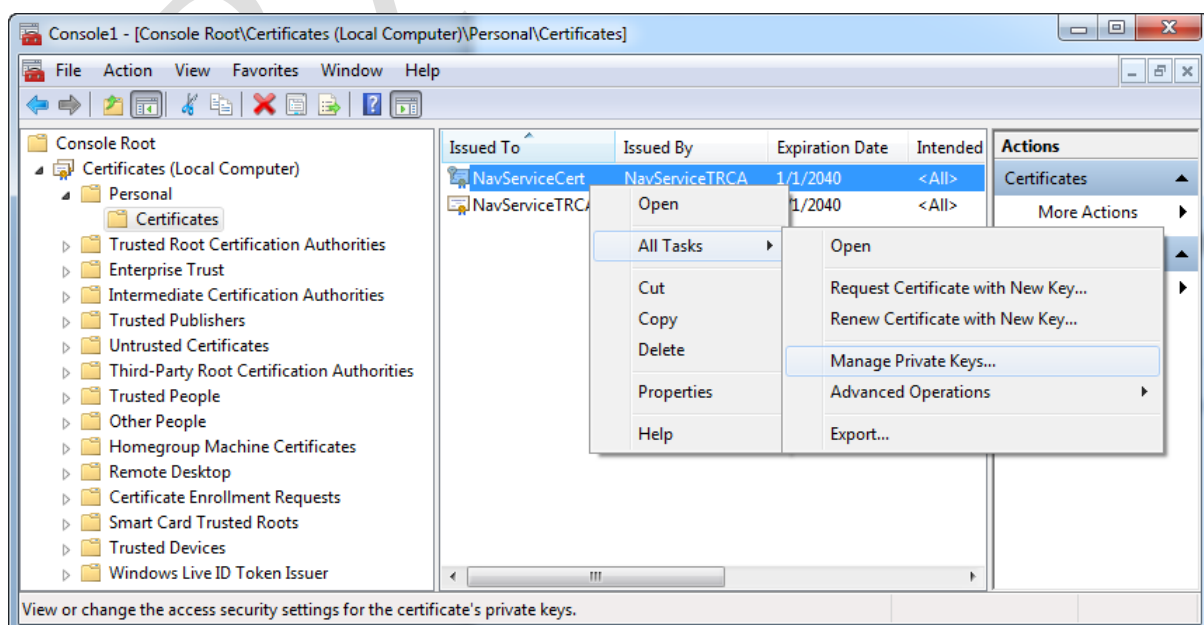


4.5 Grant access “NavServiceCert” certificate to service account

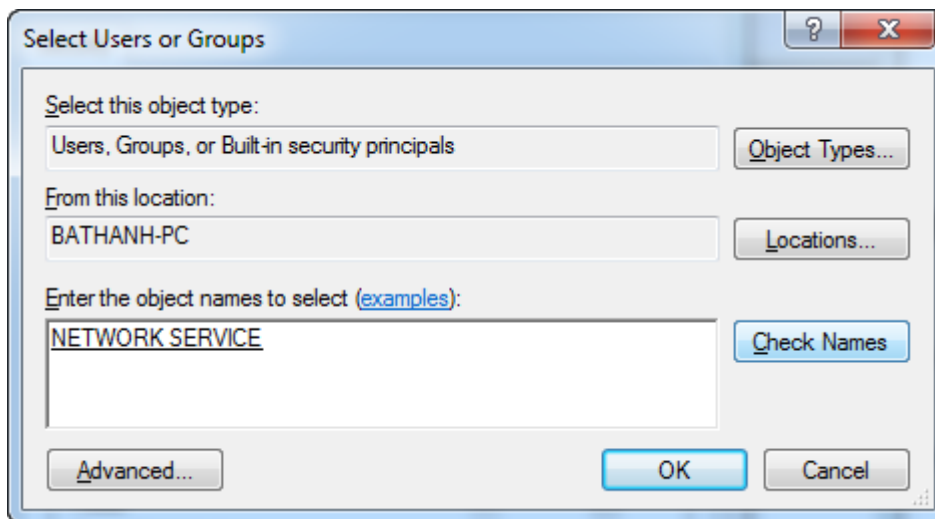
1. Check the service account that starts NAV Server service



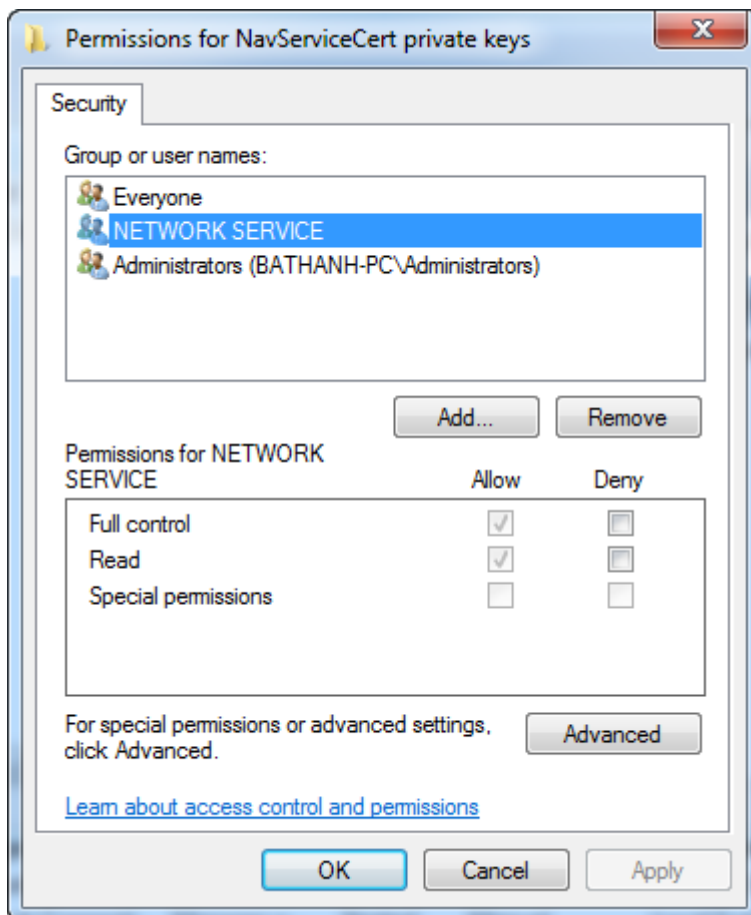
2. Right-click NavServiceCert → All Tasks → Manage Private Keys...



3. Click Add → type service account in step 1, i.e. Network Service → click Check Names → OK

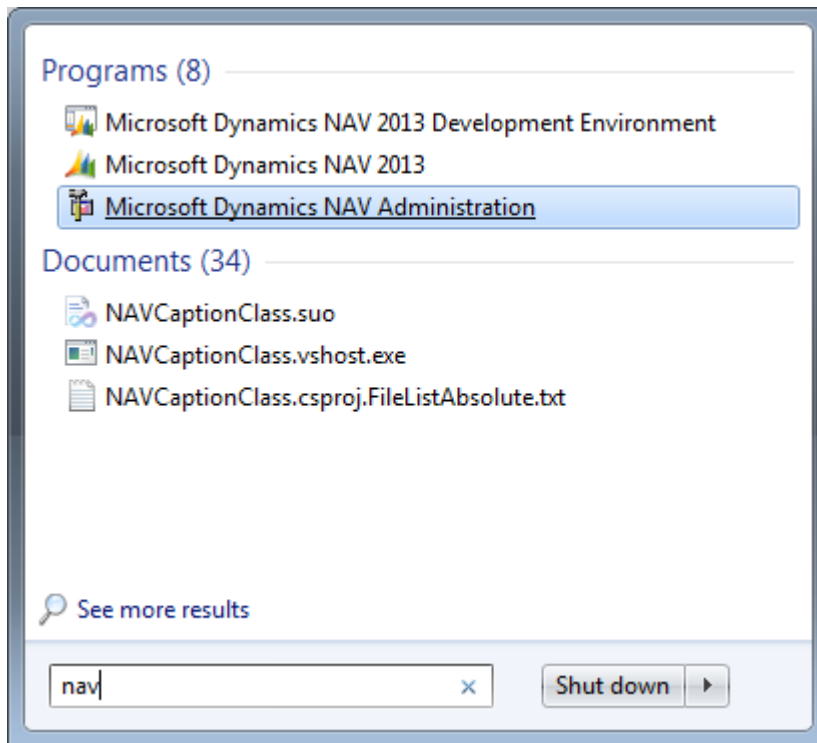


4. Grant Full control permission for the service account → click OK

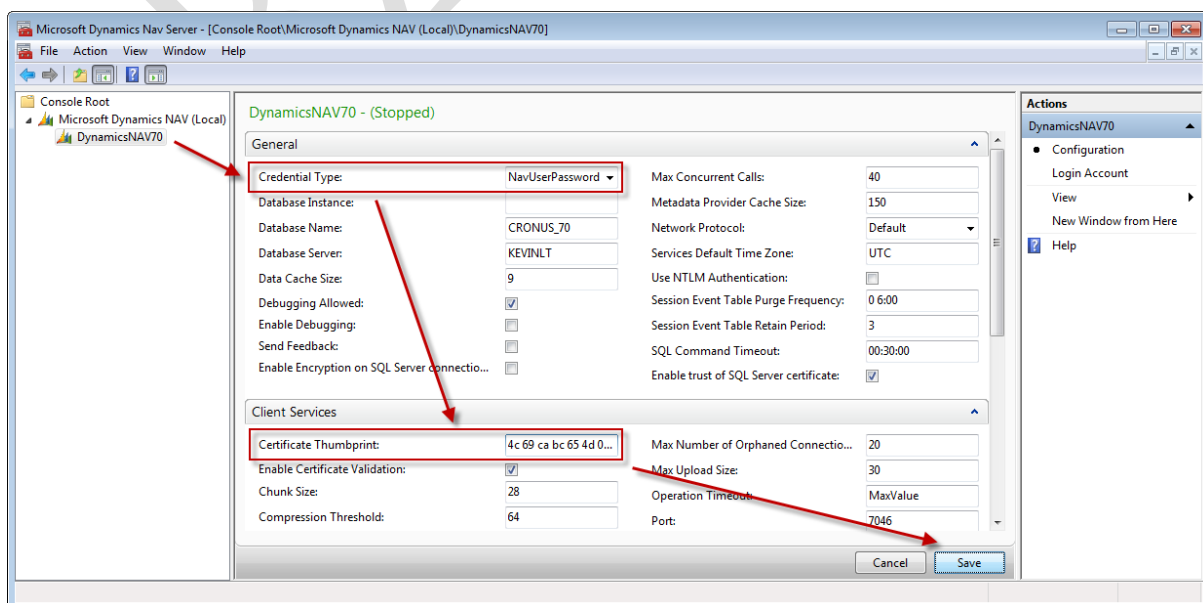


4.6 Configure NAV Server Service by NAV Administration Tool

1. Open Microsoft Dynamics NAV Administration Tool, you can use Windows search

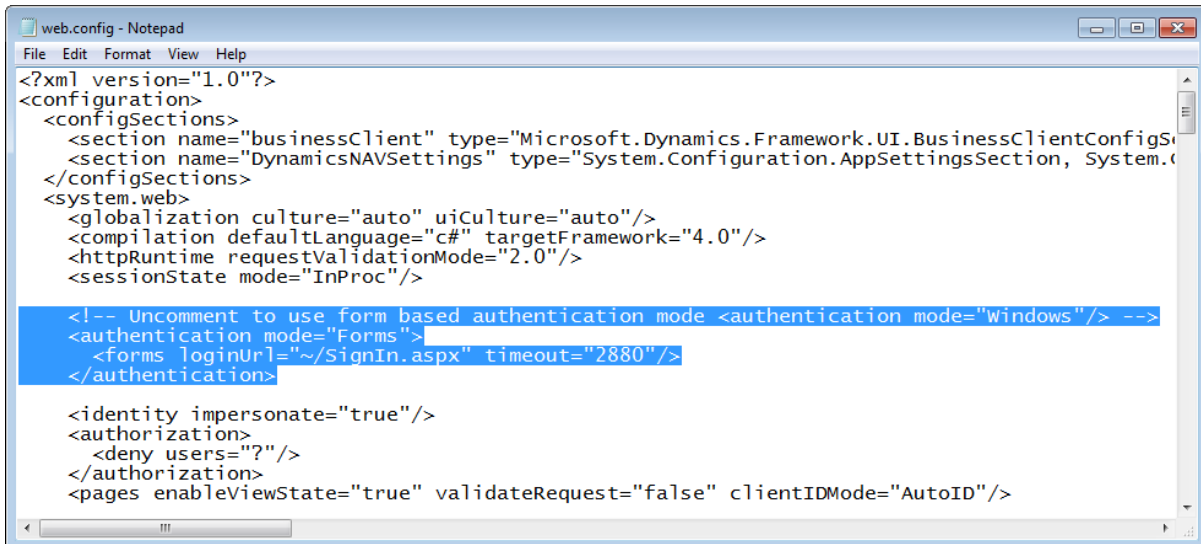


2. Edit desired instance, i.e. DynamicsNAV70
3. Change ClientServicesCredentialType (General tab) to UserName or NavUserPassword
4. Add thumbprint to CertificateThumbprint (Client Services tab)
(Thumbprint is "4c 69 ca bc 65 4d 07 d5 61 f1 43 61 21 55 44 00 bf 30 79 f5")
5. Click Save and restart the Microsoft Dynamics NAV Server instance



4.7 Configure NAV Web Server - "web.config" file

1. Edit "C:\Program Files\Microsoft Dynamics NAV\70\Web Client\web.config" file
2. Switch <authentication mode="Windows" /> to <authentication mode="Forms"> as below
(Apply for RTM version only)

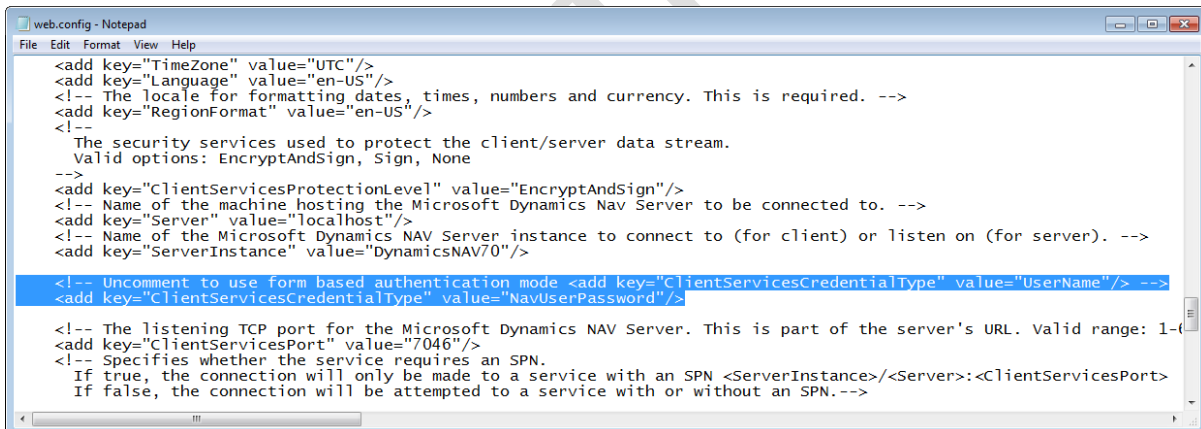


```

web.config - Notepad
File Edit Format View Help
<?xml version="1.0"?>
<configuration>
  <configSections>
    <section name="businessClient" type="Microsoft.Dynamics.Framework.UI.BusinessClientConfigS
    <section name="DynamicsNAVSettings" type="System.Configuration.AppSettingsSection, System.C
  </configSections>
  <system.web>
    <globalization culture="auto" uiCulture="auto"/>
    <compilation defaultLanguage="c#" targetFramework="4.0"/>
    <httpRuntime requestValidationMode="2.0"/>
    <sessionState mode="InProc"/>
    <!-- Uncomment to use form based authentication mode <authentication mode="Windows"/> -->
    <authentication mode="Forms">
      <forms loginUrl="~/SignIn.aspx" timeout="2880"/>
    </authentication>
    <identity impersonate="true"/>
    <authorization>
      <deny users="?" />
    </authorization>
    <pages enableViewState="true" validateRequest="false" clientIDMode="AutoID"/>
  </system.web>
</configuration>

```

3. Uncomment ClientServicesCredentialType key with UserName or NavUserPassword value

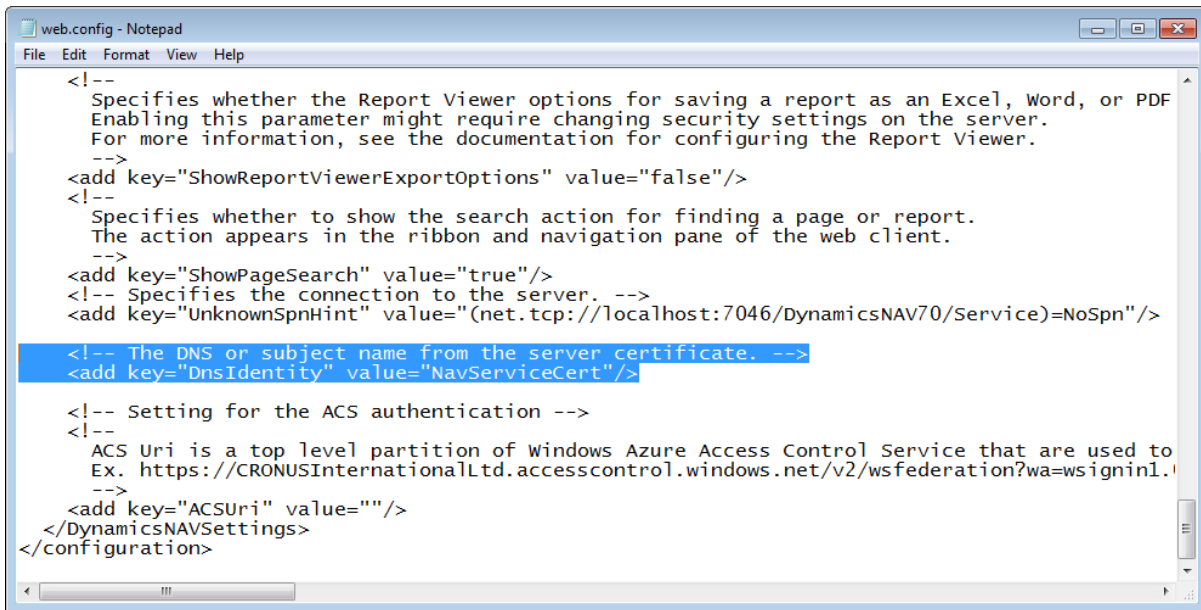


```

web.config - Notepad
File Edit Format View Help
<add key="TimeZone" value="UTC"/>
<add key="Language" value="en-US"/>
<!-- The locale for formatting dates, times, numbers and currency. This is required. -->
<add key="RegionFormat" value="en-US"/>
<!--
  The security services used to protect the client/server data stream.
  Valid options: EncryptAndSign, Sign, None
-->
<add key="ClientServicesProtectionLevel" value="EncryptAndSign"/>
<!-- Name of the machine hosting the Microsoft Dynamics Nav Server to be connected to. -->
<add key="Server" value="localhost"/>
<!-- Name of the Microsoft Dynamics NAV Server instance to connect to (for client) or listen on (for server). -->
<add key="ServerInstance" value="DynamicsNAV70"/>
<!-- Uncomment to use form based authentication mode <add key="ClientServicesCredentialType" value="UserName"/> -->
<add key="ClientServicesCredentialType" value="NavUserPassword"/>
<!-- The listening TCP port for the Microsoft Dynamics NAV Server. This is part of the server's URL. Valid range: 1-
<add key="ClientServicesPort" value="7046"/>
<!-- Specifies whether the service requires an SPN.
  If true, the connection will only be made to a service with an SPN <ServerInstance>/<Server>:<ClientServicesPort>
  If false, the connection will be attempted to a service with or without an SPN.-->

```

4. Add "NavServiceCert" value to DnsIdentity key



```
<!--
  Specifies whether the Report Viewer options for saving a report as an Excel, Word, or PDF
  Enabling this parameter might require changing security settings on the server.
  For more information, see the documentation for configuring the Report Viewer.
-->
<add key="ShowReportViewerExportOptions" value="false"/>
<!--
  Specifies whether to show the search action for finding a page or report.
  The action appears in the ribbon and navigation pane of the web client.
-->
<add key="ShowPageSearch" value="true"/>
<!-- Specifies the connection to the server. -->
<add key="UnknownSpnHint" value="(net.tcp://localhost:7046/DynamicsNAV70/Service)=NoSpn"/>

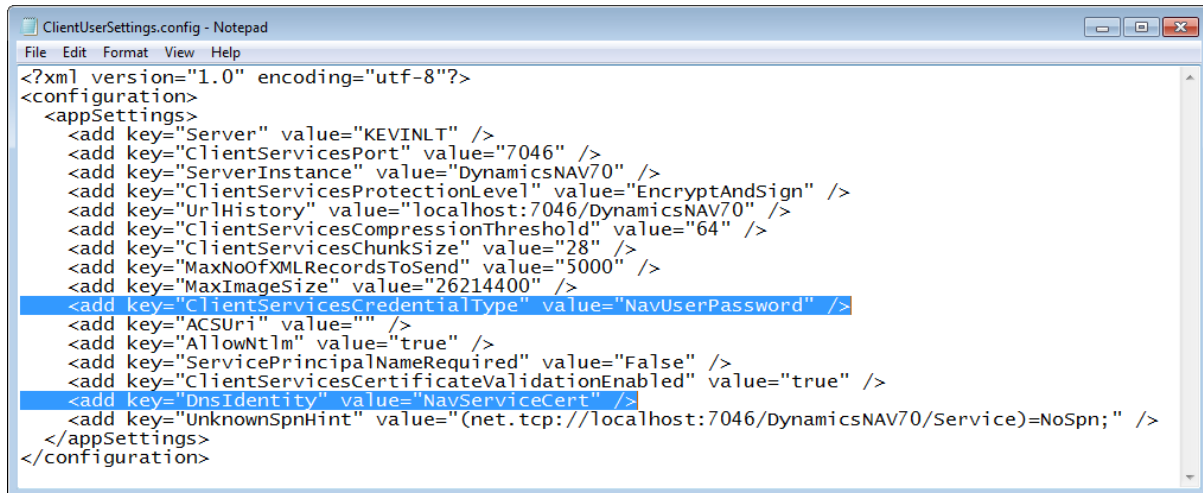
<!-- The DNS or subject name from the server certificate. -->
<add key="DnsIdentity" value="NavServiceCert"/>

<!-- Setting for the ACS authentication -->
<!--
  ACS Uri is a top level partition of Windows Azure Access Control Service that are used to
  Ex. https://CRONUSInternationalLtd.accesscontrol.windows.net/v2/ws federation?wa=wsignin1.
-->
<add key="ACSUri" value=""/>
</DynamicsNAVSettings>
</configuration>
```

5. Save "C:\Program Files\Microsoft Dynamics NAV\70\Web Client\web.config" file

4.8 Configure NAV Client - "ClientUserSettings.config" file

1. Edit "%AppData%\Microsoft\Microsoft Dynamics NAV\70\ClientUserSettings.config" file
2. Change value of ClientServicesCredentialType key to UserName or NavUserPassword
3. Add "NavServiceCert" value to DnsIdentity key



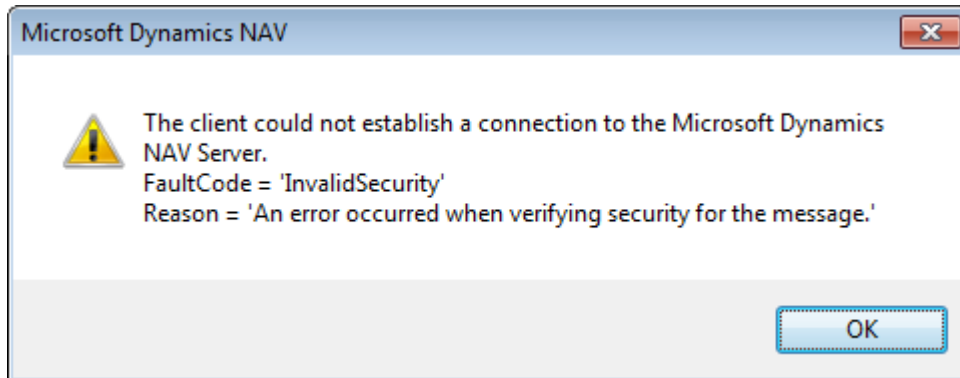
4. Save "%AppData%\Microsoft\Microsoft Dynamics NAV\70\ClientUserSettings.config" file

5. Troubleshoot

5.1 The client could not establish a connection to the Microsoft Dynamics NAV Server. FaultCode = 'InvalidSecurity' Reason = 'An error occurred when verifying security for the message.'

Symptom:

Client could not establish a connection to NAV Server, users receive below message:

**Reason:**

It is due to different time or time zone between client and server.

Solution:

Check client and server time.

5.2 The service MicrosoftDynamicsNavServer\$DynamicsNAV70 failed to start... It is likely that certificate 'CN=NavServiceCert' may not have a private key that is capable of key exchange or the process may not have access rights for the private key

Symptom:

Cannot start Microsoft Dynamics NAV Server Service, Windows Event Viewer shows:

Server instance: DynamicsNAV70

Session type: UnknownClient

Session ID: 0

The service MicrosoftDynamicsNavServer\$DynamicsNAV70 failed to start. This could be caused by a configuration error. Detailed error information: System.ArgumentException: It is likely that certificate 'CN=NavServiceCert' may not have a private key that is capable of key exchange or the process may not have access rights for the private key. Please see inner exception for detail.

```
at System.ServiceModel.Security.SecurityUtils.EnsureCertificateCanDoKeyExchange(X509Certificate2 certificate)
at System.ServiceModel.Security.ServiceCredentialsSecurityTokenManager.CreateLocalSecurityTokenProvider(RecipientServiceModelSecurityTokenRequirement
recipientRequirement)
at System.ServiceModel.Security.ServiceCredentialsSecurityTokenManager.CreateSecurityTokenProvider(SecurityTokenRequirement requirement)
at System.ServiceModel.Channels.SslStreamSecurityUpgradeProvider.CreateServerProvider(SslStreamSecurityBindingElement bindingElement, BindingContext context)
at System.ServiceModel.Channels.SslStreamSecurityBindingElement.BuildServerStreamUpgradeProvider(BindingContext context)
at System.ServiceModel.Channels.ConnectionOrientedTransportChannelListener..ctor(ConnectionOrientedTransportBindingElement bindingElement, BindingContext
context)
at System.ServiceModel.Channels.TcpChannelListener..ctor(TcpTransportBindingElement bindingElement, BindingContext context)
at System.ServiceModel.Channels.TcpTransportBindingElement.BuildChannelListener[TChannel](BindingContext context)
at System.ServiceModel.Channels.SessionChannelDemuxer`2..ctor(BindingContext context, TimeSpan peekTimeout, Int32 maxPendingSessions)
at System.ServiceModel.Channels.ChannelDemuxer.CreateTypedDemuxer(Type channelType, BindingContext context)
at System.ServiceModel.Channels.ChannelDemuxer.GetTypedDemuxer(Type channelType, BindingContext context)
at System.ServiceModel.Channels.ChannelDemuxer.BuildChannelListener[TChannel](BindingContext context, ChannelDemuxerFilter filter)
at System.ServiceModel.Channels.ChannelBuilder.BuildChannelListener[TChannel]()
at System.ServiceModel.Channels.ChannelBuilder.BuildChannelListener[TChannel](MessageFilter filter, Int32 priority)
at System.ServiceModel.Security.SecuritySessionServerSettings.CreateInnerChannelListener()
at System.ServiceModel.Channels.SecurityChannelListener`1.InitializeListener(ChannelBuilder channelBuilder)
at System.ServiceModel.Channels.TransportSecurityBindingElement.BuildChannelListenerCore[TChannel](BindingContext context)
at System.ServiceModel.Channels.SecurityBindingElement.BuildChannelListener[TChannel](BindingContext context)
at System.ServiceModel.Channels.ReliableChannelListener`3..ctor(ReliableSessionBindingElement binding, BindingContext context)
at System.ServiceModel.Channels.ReliableListenerOverDuplexSession`2..ctor(ReliableSessionBindingElement binding, BindingContext context)
at System.ServiceModel.Channels.ReliableSessionBindingElement.BuildChannelListener[TChannel](BindingContext context)
at Microsoft.Dynamics.Nav.Types.Channels.ChunkingBindingElement.BuildChannelListener[TChannel](BindingContext context)
at System.ServiceModel.Channels.Binding.BuildChannelListener[TChannel](Uri listenUriBaseAddress, String listenUriRelativeAddress, ListenUriMode listenUriMode,
BindingParameterCollection parameters)
at System.ServiceModel.Description.DispatcherBuilder.MaybeCreateListener(Boolean actuallyCreate, Type[] supportedChannels, Binding binding,
BindingParameterCollection parameters, Uri listenUriBaseAddress, String listenUriRelativeAddress, ListenUriMode listenUriMode, ServiceThrottle throttle,
IChannelListener& result, Boolean supportContextSession)
at System.ServiceModel.Description.DispatcherBuilder.BuildChannelListener(StuffPerListenUriInfo stuff, ServiceHostBase serviceHost, Uri listenUri, ListenUriMode
listenUriMode, Boolean supportContextSession, IChannelListener& result)
at System.ServiceModel.Description.DispatcherBuilder.InitializeServiceHost(ServiceDescription description, ServiceHostBase serviceHost)
at System.ServiceModel.ServiceHostBase.InitializeRuntime()
at System.ServiceModel.ServiceHostBase.OnOpen(TimeSpan timeout)
at System.ServiceModel.Channels.CommunicationObject.Open(TimeSpan timeout)
at Microsoft.Dynamics.Nav.WindowsServices.NavServerWindowsService.StartWcfServices()
at Microsoft.Dynamics.Nav.WindowsServices.NavServerWindowsService.OnStart(String[] args).
```

Reason:

It is due to configuration error (such as missing certificates, access rights for the private key) or certificates cache error.

Solution:

For configuration error, check and reconfigure NAV Server as section 3.1.

For certificates cache error, open command prompt (C:\Windows\System32\cmd.exe) and type "certutil -urlcache * delete" to clear cache and load new certificates.

6. Version Control

Version (YYMMDD)	Description
130601	Released.
131101	Review with Navision 2013 R2.

4BZSoftware

This is last page.

Thank you!