



BackBox[©] E4.13 SSL Setup

Abstract

This SSL Setup document is for E4.13

Published: May 2024



Legal Notice

© Copyright 2013, 2024 ETI-NET Inc. All rights reserved.

Confidential computer software. Valid license from ETI-NET Inc. required for possession, use or copying.

The information contained herein is subject to change without notice. The only warranties for ETI-NET-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. ETI-NET shall not be liable for technical or editorial errors or omissions contained herein.

BackBox is registered trademark of ETI-NET Inc.

StoreOnce is a registered trademark of Hewlett Packard Development, L.P.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation. Tivoli Storage Manager (TSM) is a registered trademark of IBM Corporation.

QTOS is a registered trademark of Quality Software Associates Inc.

All other brand or product names, trademarks or registered trademarks are acknowledged as the property of their respective owners.

This document, as well as the software described in it, is furnished under a License Agreement or Non-Disclosure Agreement. The software may be used or copied only in accordance with the terms of said Agreement. Use of this manual constitutes acceptance of the terms of the Agreement. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, and translation to another programming language, for any purpose without the written permission of ETI-NET Inc.

Copyright © 2013, 2024 ETI-NET Inc. All rights reserved.

Table of contents

INTRODUCTION	4
Related Documentation	4
Enabling SSL	4
SSL Configuration	4
Enable/Disable SSL	5
SSL IN THE UI	6
SSL IN THE NONSTOP	7
Stop all BackBox Programs	7
Enabling /Disabling SSL	7
Restarting the EMS Extractor BBEXT	8
Troubleshooting	8
SSL IN THE VTC	9
Enabling /Disabling SSL	9
Troubleshooting	10
APPENDIX A - TRUST ROOT CERTIFICATION	12
Adding Certificates into Trust Root Certification Authorities	12
Certificates Configuration	12
APPENDIX B - CERTIFICATE STORE	16
APPENDIX C - CERTIFICATES UPGRADE ON NONSTOP	25

INTRODUCTION

This manual describes the SSL enabling procedure on the BackBox control path, i.e. on the TCP/IP connections between the BackBox components.

Depending on the BackBox component, the provider of the SSL library is different.

Platform	BackBox component	SSL product
NonStop	Domain manager, EMS Extractor, BBCMD & BB053 utilities	OpenSSL
MS-Windows	UI, High-level services	Schannel
MS-Windows	VTC low-level services such as the tape emulator	Schannel



Schannel Security Service Provider (SSP) is a part of Windows Server components that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Internet standard authentication protocols.

Related Documentation

This manual is part of the BackBox documentation package and it is recommended to be consulted in addition to the following manuals: [BackBox User Manual](#) and [BackBox Messages Manual and Troubleshooting](#).

Although the SSL configuration to each BackBox component is done in part through the BackBox interface, each SSL provider supplies its own documentation and configuration tools.

https://learn.microsoft.com/en-us/windows/win32/com/schannel_Managing_Microsoft_Certificate_Services_and_SSL

Enabling SSL

BackBox can run with or without SSL.

The default configuration is no SSL. SSL must be either enabled in all components, or disabled in all components:

- of a BackBox domain
- of a VTC (that can be shared by several domains)

SSL is best enabled as the final step of establishing the BackBox management layer:

1. After all components have been successfully installed and made sure that they communicate through TCP/IP, i.e. when the BackBox UI is able to report the internal configuration of all VTCs (UI tab Configuration > VT Controller).
2. Before or after the tape emulation has been configured. It is recommended to first configure the BackBox tape emulation.

SSL Configuration

Any SSL configuration in BackBox depends on the Certificate Authority, on how the servers and client certificates are produced and transferred, on the chosen encryption algorithms, and on other security options.



The certificates provided with BackBox initial installation should be replaced with the customer's own certificates, based on the security guidelines and policies in place. For more details, see [Appendix B - Certificate Store](#) and [Appendix C - Certificates Upgrade on Nonstop](#).

This manual includes a section that document how SSL can be enabled for each BackBox component. It also identifies the tools to configure the local SSL library.

There are two complementary tools to configure SSL:

- The local BackBox component, which accepts the essential parameters.
- The local SSL library, which provides its own specific configuration tool.

Enable/Disable SSL

All permanent processes on all BackBox domain components must be stopped to allow this change to take effect. There must be no tape activity.

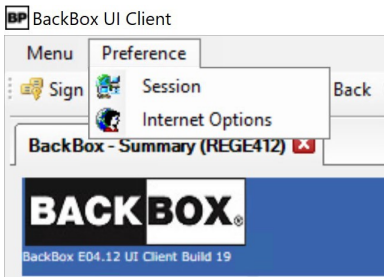
To stop the permanent BackBox processes perform the following actions in order:

1. Stop the BackBox activity.
2. Stop the virtual tapes in SCF.
3. Stop the Windows services in VTCs.
4. Stop the NonStop BackBox processes.

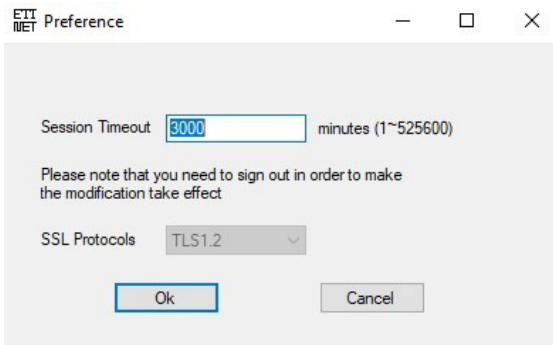
SSL IN THE UI



SSL must be enabled in all installations of the BackBox UI. To enable the SSL:

1. Go to Preference > Session.



2. Modify the session timeout value (in minutes, the maximum value is 525600) or use the default value.



	If the UI and the VTC are installed on the same server enable the SSL through the VTC Management Console. For more info see the section SSL in the VTC .
	If the UI is separately installed on another instance than the VTC MC, go to UI > Preferences and set up the SSL protocol manually to match the VTC MC settings.

If users have their own certificates (not the default ones in BackBox installation packages), they need to add their CA certificate in Trust Root Certificates Authorities store. To do so go to Preference > Internet Options > Content > Certificates > Trust Root Certificates Authorities or using MMC (See [Adding Certificates into Trust Root Certification Authorities](#) in the [Appendix A](#)).


3. Click OK.

SSL IN THE NONSTOP

To install SSL, the user should:

1. Generate and transfer certificates to the NonStop, if you don't want to use the ones included in the installation package.
2. Stop all BackBox programs.


Stop all BackBox Programs

 If you are running the EMS Extractor program BBEXT as a permanent process, you need to stop it first in SCF.
Example: `TACL> SCF ABORT PROCESS $ZZKRN.#BBOXEXT`

Use the macro `BB054_SHUTDOWN` to stop all BackBox programs of a given domain before enabling SSL:

```
VOLUME <BackBox-domain-installation-sub-volume> LOAD /KEEP 1/ MACROS BBSETUP  
BB054_SHUTDOWN
```

`BB054_SHUTDOWN` is preferably used over `TACL STOP`, as it stops the programs by sending an IPC message to the processes, rather than by executing `TACL STOP`.

 It will also stop the EMS Extractor program BBEXT, if EMS Extractor program BBEXT is not a permanent process.

Alternatively, when `BB054_SHUTDOWN` does not work:

```
VOLUME <BackBox-domain-installation-sub-volume> STATUS *, PROG  
*
```

And after verification:

```
STATUS *, PROG *, STOP
```

Enabling /Disabling SSL

Enabled SSL in `SSLCFG` - file content (TLSv1.2 enabled):

```
servkeypass test  
servkey <backBox-domain-installation-sub-volume>.NSKDER servcert <backBox-domain-installation-  
sub-volume>.NSKCRT cacerts <backBox-domain-installation-sub-volume>.VTCCRT RANDOMDELAY 1  
MINVERSION TLSv1.2  
USESSL 1  
TRACELEVEL 0
```

Disabled SSL in `SSLCFG` - file content:

```
servkeypass test  
servkey <backBox-domain-installation-sub-volume>.NSKDER servcert <backBox-domain-installation-  
sub-volume>.NSKCRT cacerts <backBox-domain-installation-sub-volume>.VTCCRT RANDOMDELAY 1  
MINVERSION TLSv1.2  
USESSL 0  
TRACELEVEL 0
```

For `<BackBox-domain-installation-sub-volume>` use your own installation file location. There is no need to configure SSL in the peripheral nodes; just enable the SSL.

To encrypt the `SERVKEYPASS` run the program `BBpscode` to make sure that the keypass is not displayed and visible.

TACL command to run for the keypass encryption:

```
run BBpsCode <ServKeyPass to be encrypted for the NonStop SSL certificate>
```

Once the program has been run and the keypass successfully encrypted, you will be prompted with the message:

```
Successfully updated the Encrypted ServerkeyPass
```

Restarting the EMS Extractor BBEXT

Use the startup OBEY file OEXT in the BackBox- domain- installation- sub- volume or the SCF START PROCESS command.

Example: TACL> SCF START PROCESS \$ZZKRN.#BBOXEXT

Troubleshooting

If the domain manager is set for SSL, but received a non-SSL connection, the following sample message will be displayed in EMS:

Error 0x1408F10B in EMS

```
2022- 07- 22 15:17:07 \ETINIUM.$XODN ETINET.100.100 3479 GCE401EA- E3479 SSL library error
336130315 (= 0x1408F10B) on socket 7 with Server role -.
```



If the above message and tape mount need to be manually executed, it means that an old non-SSL process of the EMS Extractor BBEXT might be still running.

Restart the EMS Extractor BBEXT using the OBEY file or via SCF ABORT/START PROCESS command.

SSL IN THE VTC

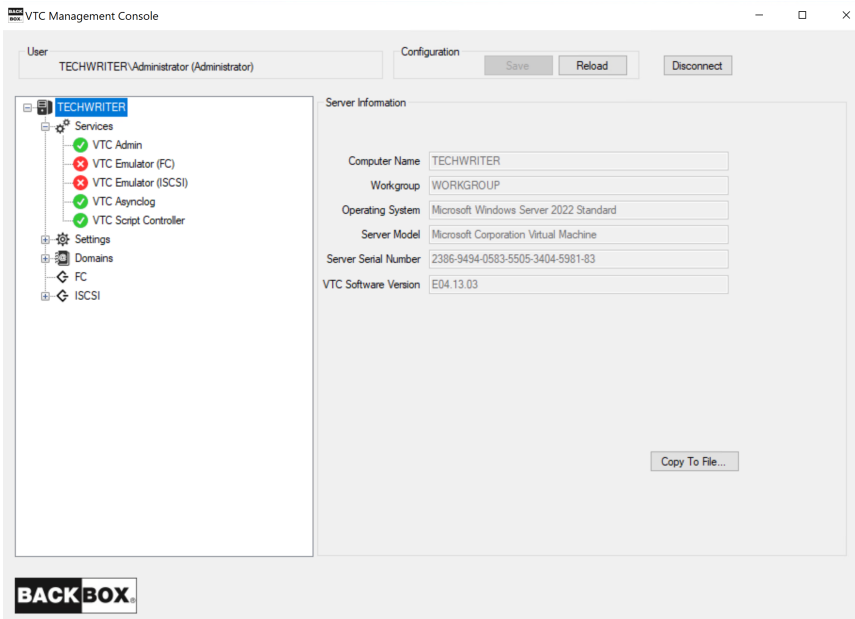
SSL must be enabled or disabled in all installations of the VTC Server.

SSL server mode for VTC Server components is implemented using Windows Schannel (Microsoft Secure Channel)..

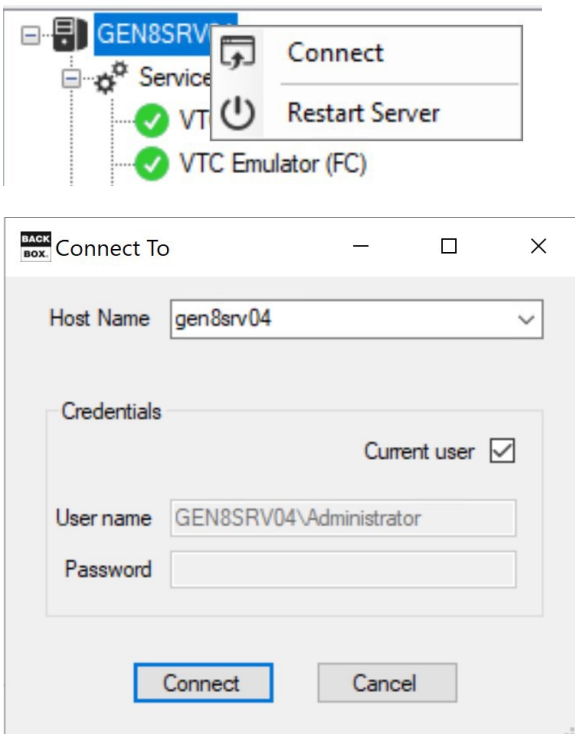
Enabling /Disabling SSL

To enable or disable SSL, start an instance of VTCManagement Console and access each VTC Server locally or remotely.

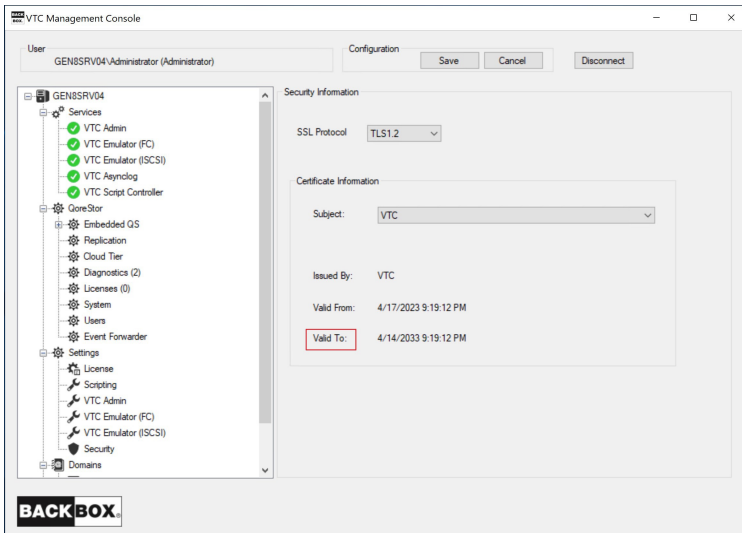
On the system where the VTC Management Console interface is installed, open the Search dialog and type VTC Management Console.




Connect to the target VTC Server if not currently the server requiring management and provide appropriate credentials. To connect to a new VTC Server, you need to right-click on the server node and select the Connect action.



Expand the Settings node and select the Security one. A Security Information panel will allow you to enter appropriate TLS/SSL information. When finish, click on the Save button.




SSL Protocols: To indicate to VTC Server components what kind of TLS/SSL channel communication should be used. The available protocols are shown in the drop-down list: NONE, TLS1.0, TLS1.1, TLS1.2.

 Go to the NonStop to set up the SSL parameters in such a way that the SSL settings are accordingly applied to correctly communicate with the VTC MC. Moreover, if you need to encrypt the server key pass code, you have to run an encryption program: BBpsCode. For more details, see section Sign In/Out in the User Guide for more information on enabling /disabling SSL.

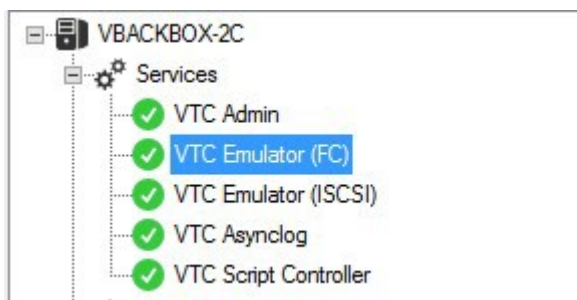
Certificate Information panel displays details about the installed certificate:

- Subject: Name of the certificate
- Issued By: Certificate issuer
- Valid From: Beginning date of the supported certificate
- Valid To: Certificate expiry date

In case of self-signed certificate, add server certificate into the Trust Root Certification Authorities Store. See [Add Certificates into Trust Root Certification Authorities](#) in the [Appendix A](#).

 Self-signed certificates distributed with the BackBox application are for test purposes only. ETI-NET is not responsible for the certificate generation and maintenance in BackBox operational environments.

After enabling or disabling SSL protocols in the VTC Server configuration, all VTC services need to be restarted for the changes to take effect. You can restart all service by right-clicking on the Services node and selecting the Restart action. The action will be applied to all services at once.



Troubleshooting

Errors are reported in the VTC Server Virtual Tape Controller Event Viewer log and connections activities are logged into xxTCP/IPSession_n files in the VTC Log Files folder.

Browsing the SSL log files

These files are C text files that can be browsed in TAFL by the BackBox macros:

```
LISTT <file-name-pattern>
```

VIEWT <file-name>

APPENDIX A - TRUST ROOT CERTIFICATION

Adding Certificates into Trust Root Certification Authorities

The way to add certificates into the Trust Root Certification Authorities Store is as follow:

1. Run MMC in command line.
2. On the menu, click file Add/Remove snap-in > select "certificates" in "Available snap-in" list > Add > choose "Computer Account" > Next and finish. You will then see certificates console.
3. In certificates console, click Trust Root Certification Authorities and add CA certificates (or the server certificate if self-signed)

Note that CA and Certificate file must be PEM format.

For more details on how to add CA or Certificate File to the Trust Root Certification Authorities Store refer to documentation of the OS you are using.

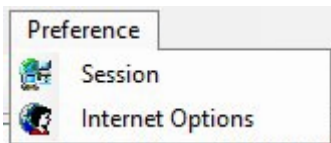
Certificates Configuration



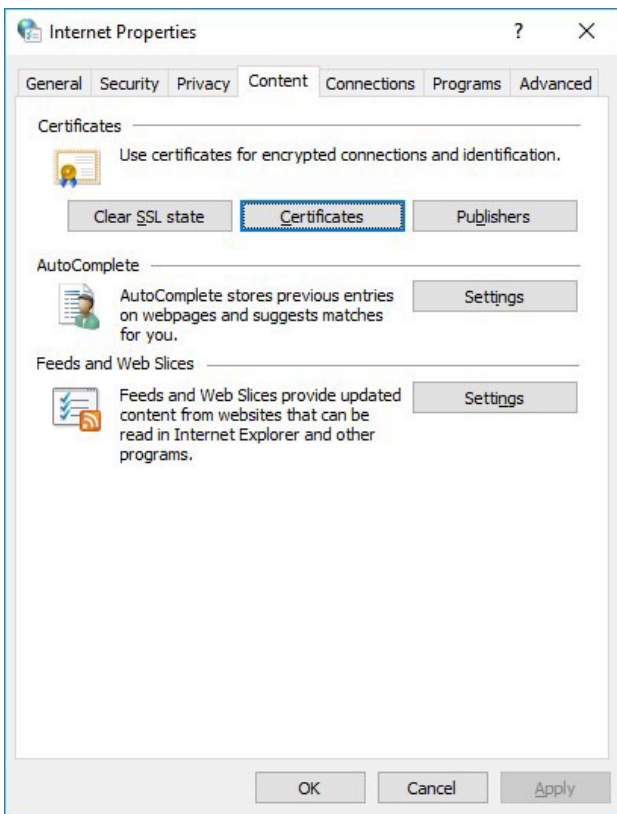
Perform the following steps only if the User Interface is installed on a workstation.

To install the CA Certificate in the operating system, follow the steps described below:

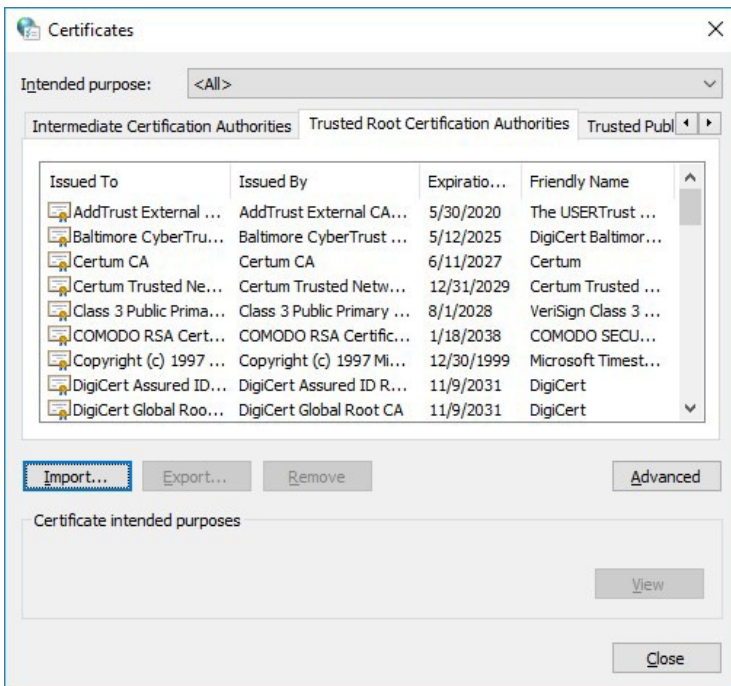
1. On the BackBox UI menu > Preference > Internet Options.

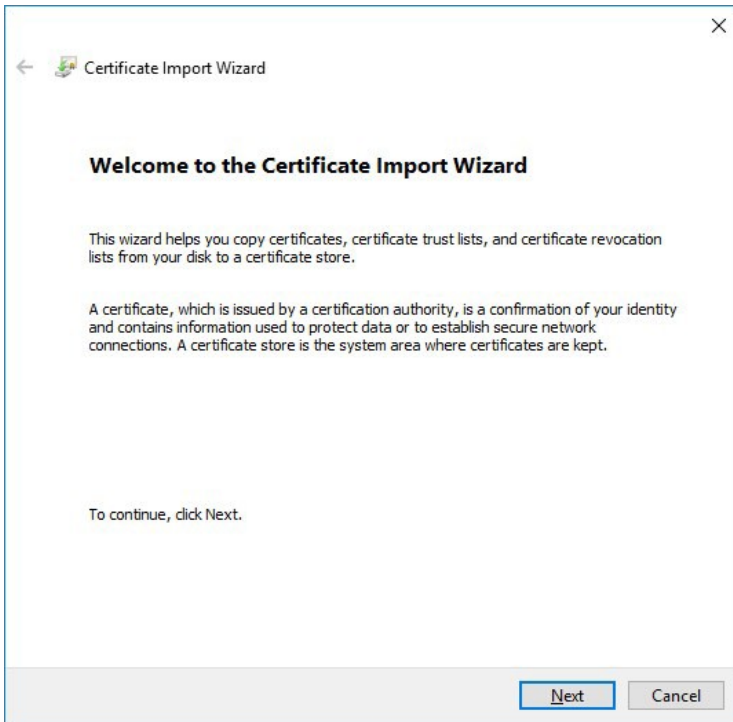


2. In the pop-up window click on the Content tab and then choose Certificates in the appropriate section.

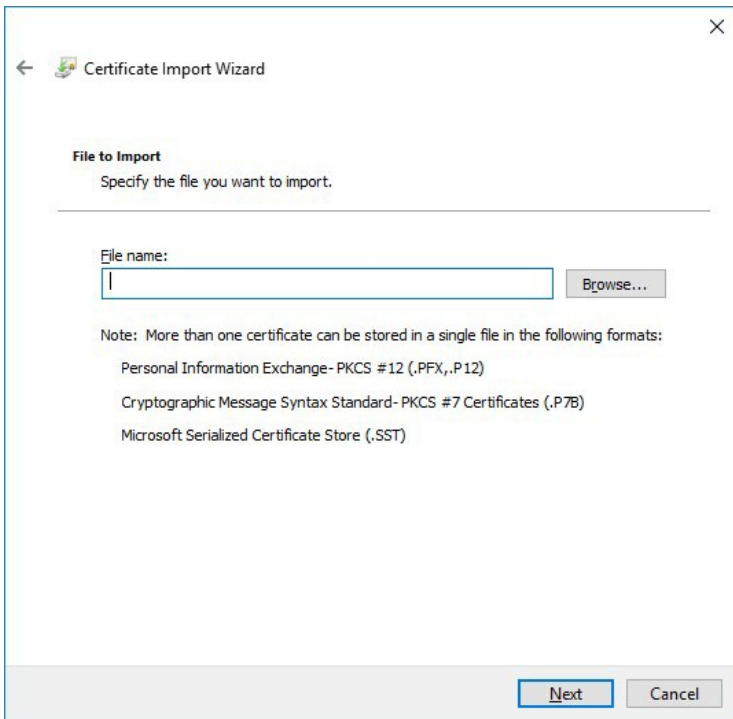



3. In the Certificates window select Trusted Root Certification Authority and Import.



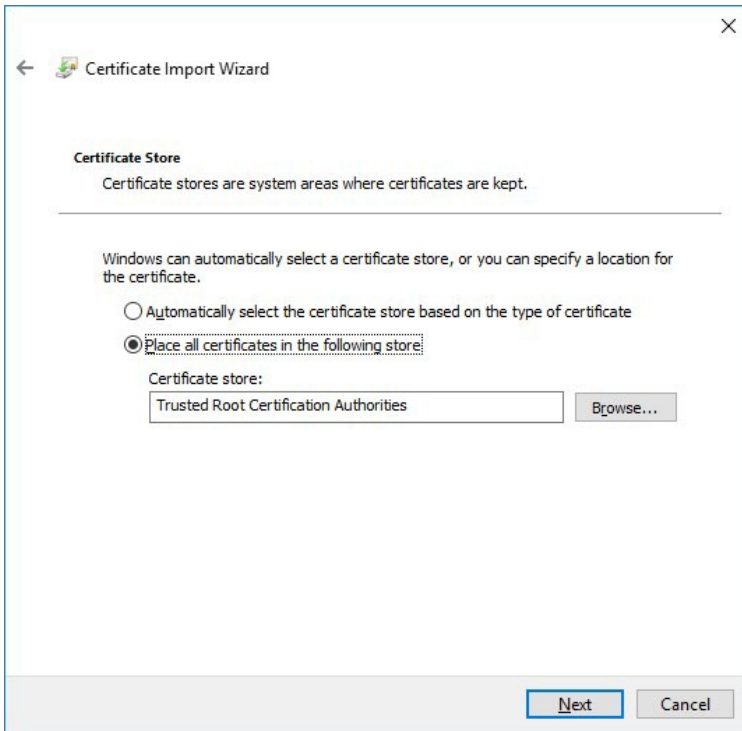


4. Specify the file to be imported. Browse it or simply pasted in the File name field. Click Next.

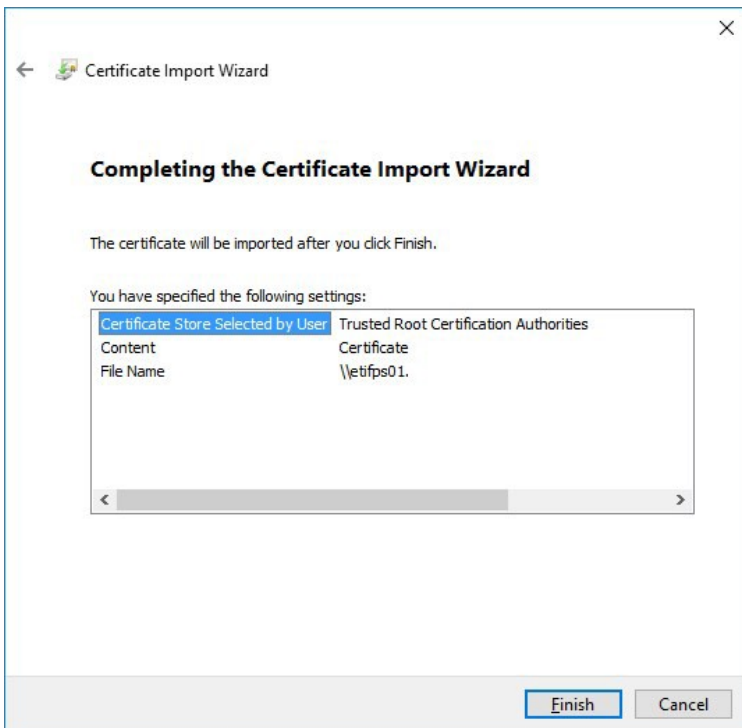


 The certificates and the key files provided by ETI- NET can be found in C:\Pro-gramData\ETINET\VTC\Cert.

5. Select a certificate store. Keep the default settings. Click Next.



6. To complete the importing process, click Finish. Verify if you selected the right path, certificate type, and content before exiting the Wizard.

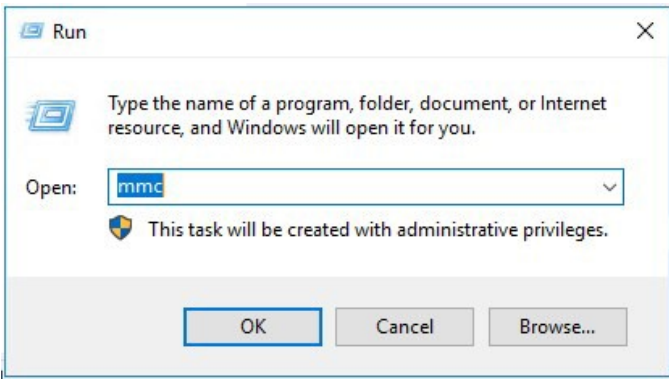


APPENDIX B - CERTIFICATE STORE

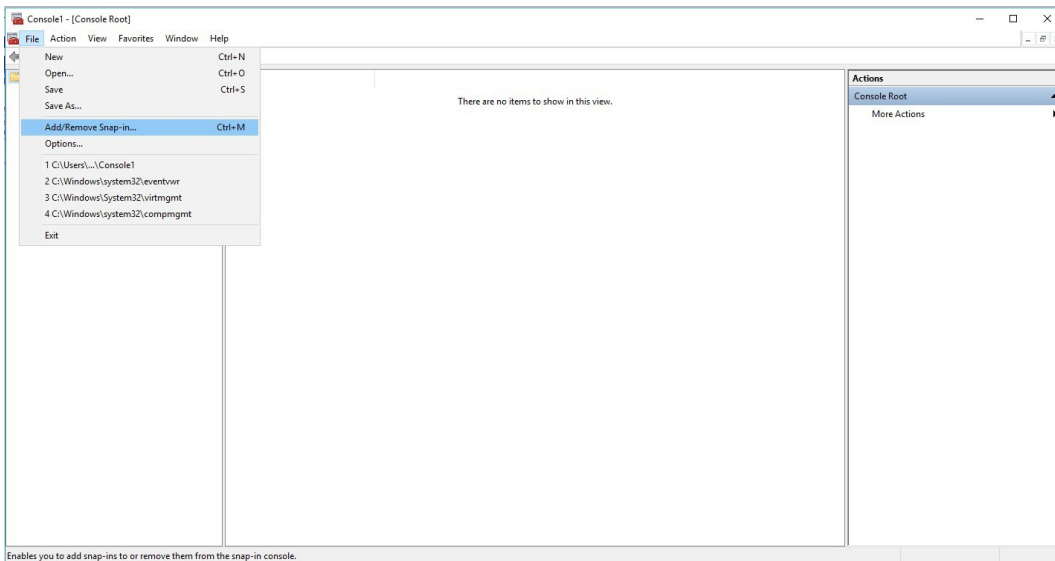
Customers using their own security certificates have to store these certificates in a special local folder after they have been issued by a certification authority. In order to copy certificate trust lists and certificate revocation lists they need to be saved in a certificate store, along with identity confirmation used to protect data and establish secure network connections.

To import your own certificates use the Microsoft Management Console (mmc)

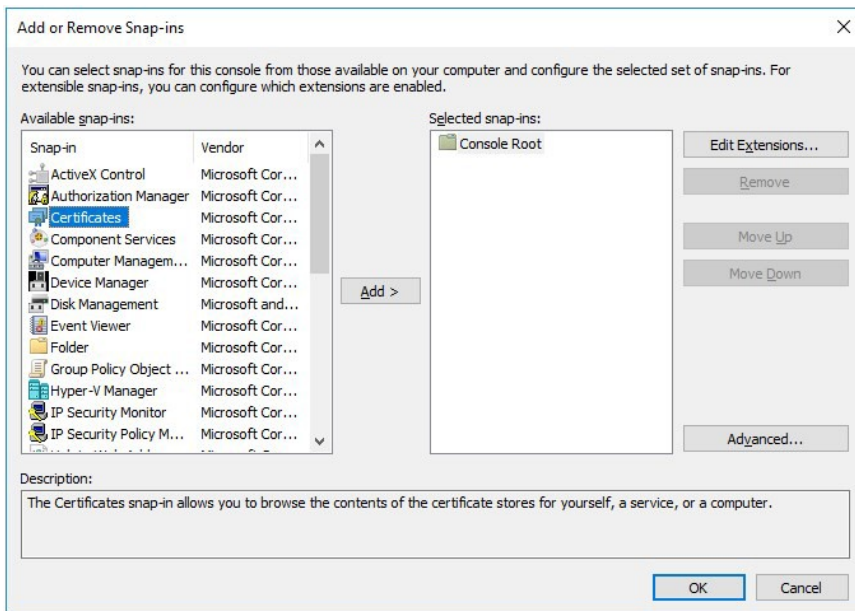
1. Right click on Windows icon, click on Run item, input mmc in the Open field and click OK.



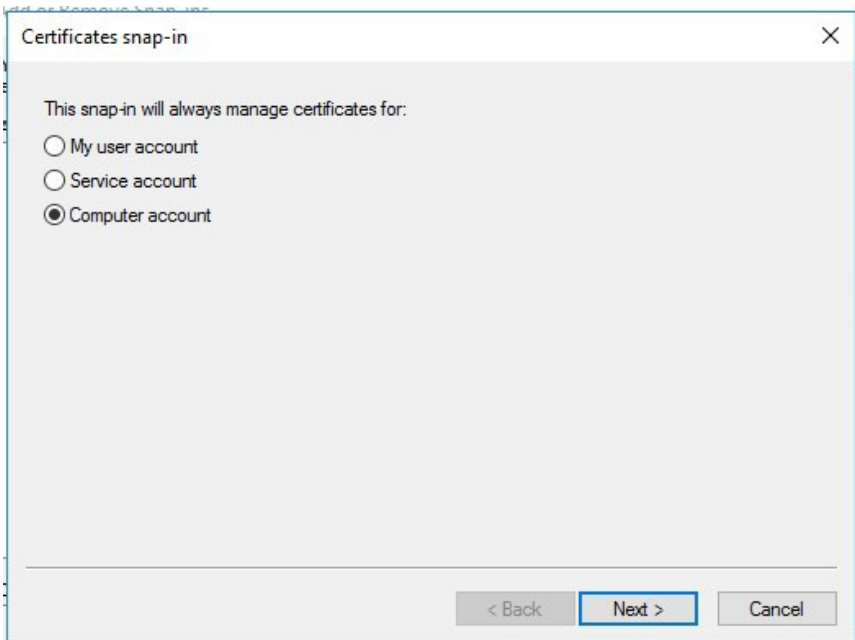
2. After the new Management Console pops up, click on File menu and click Add/Remove Snap-in item.



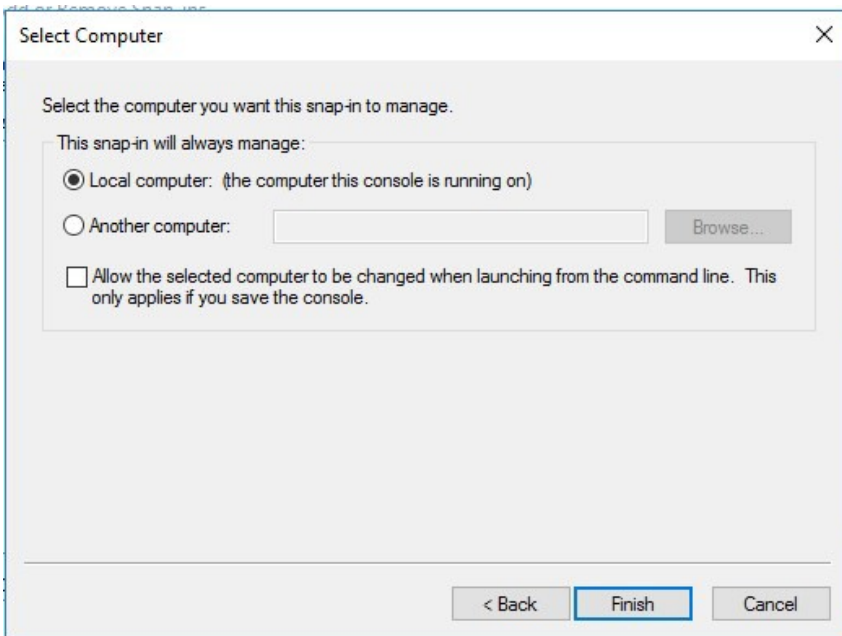
3. Choose Certificates item and click the Add button.



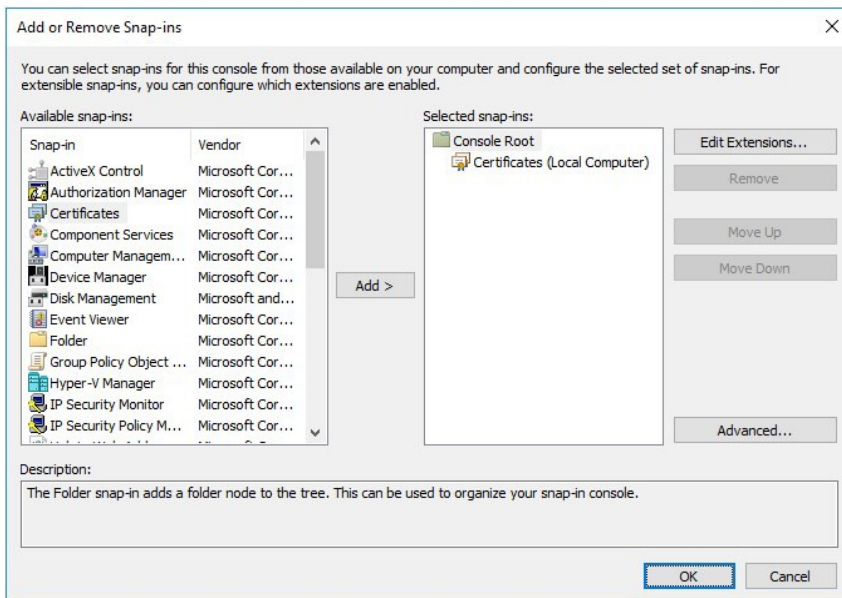
4. Choose Computer account and click Next.



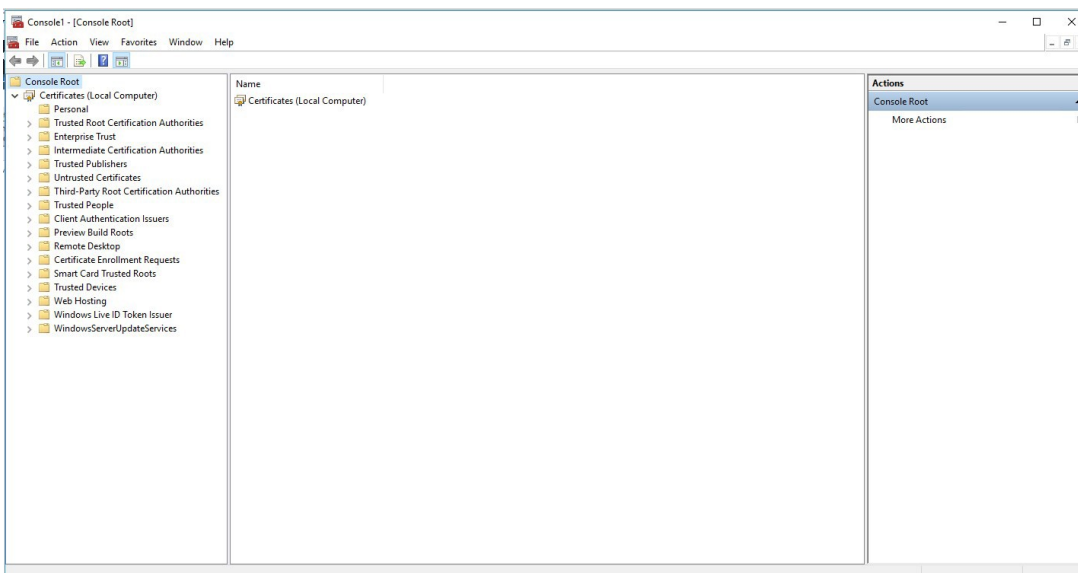
5. Keep Local computer radio box selected and click the Finish button.



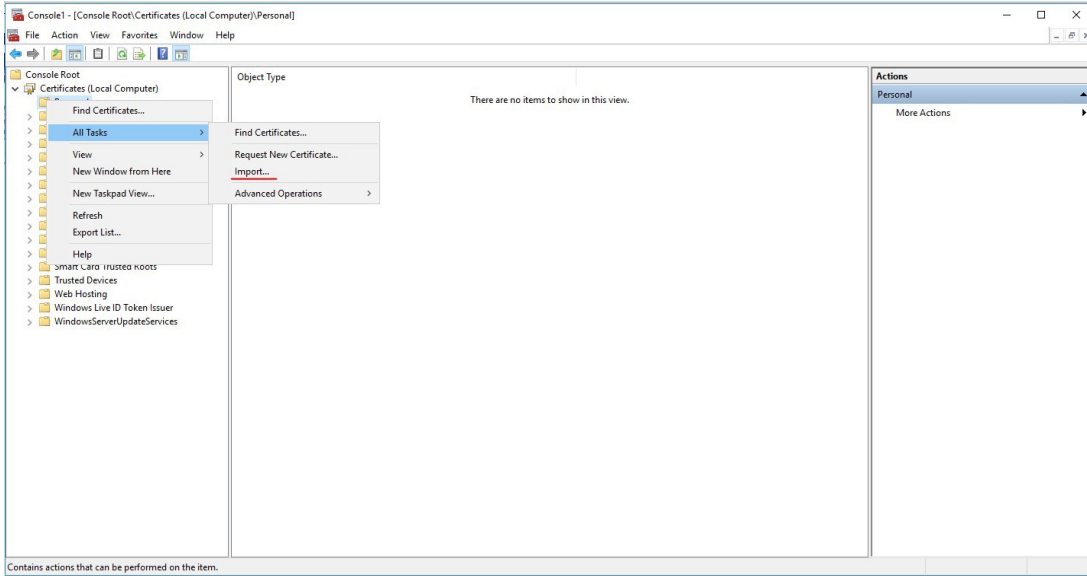
6. Click OK in the Add or Remove Snap-ins dialog.



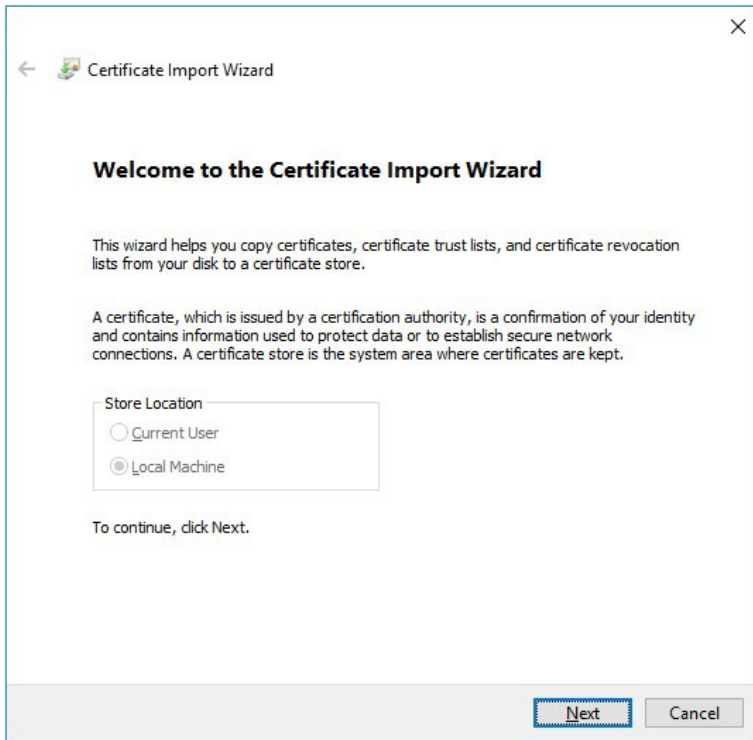
7. Expand Certificates (Local Computer) tree node.



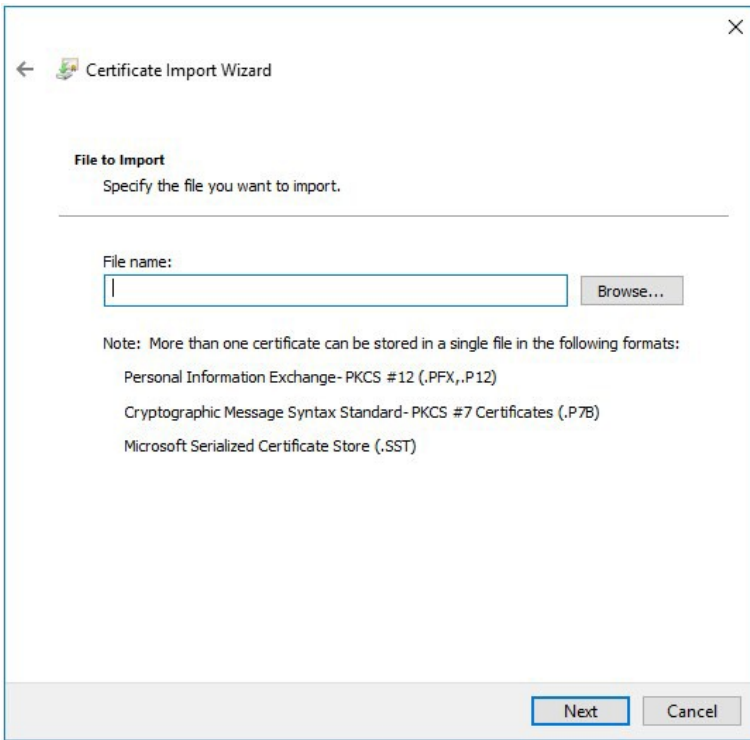
8. Right click on Personal item, chose All tasks and click Import item.



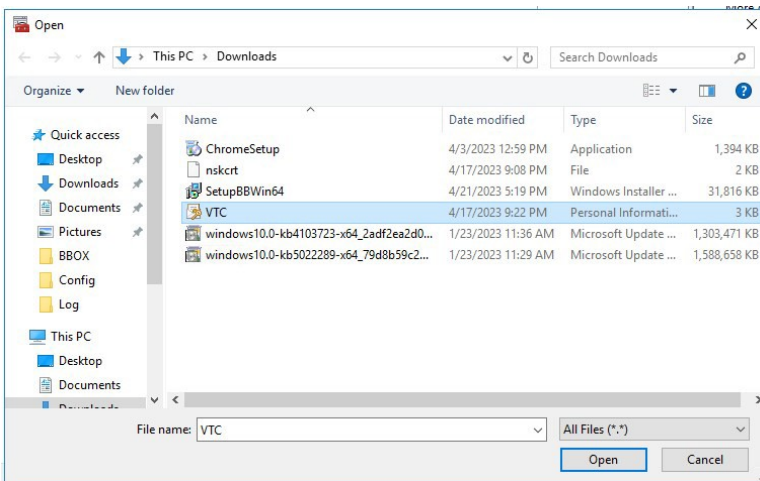
9. Click Next to start the import.



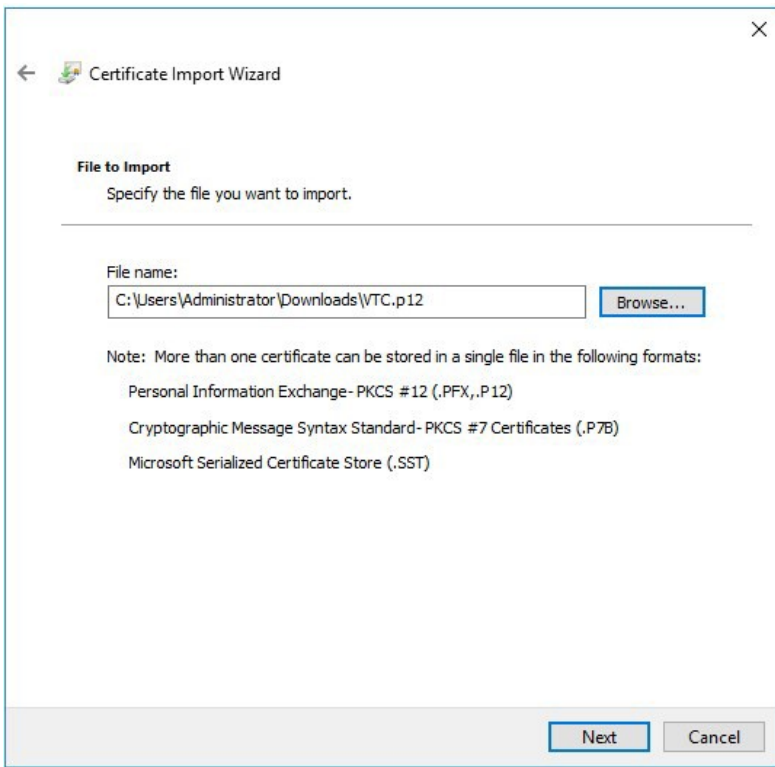
10. Click Browse to look for the file to import.



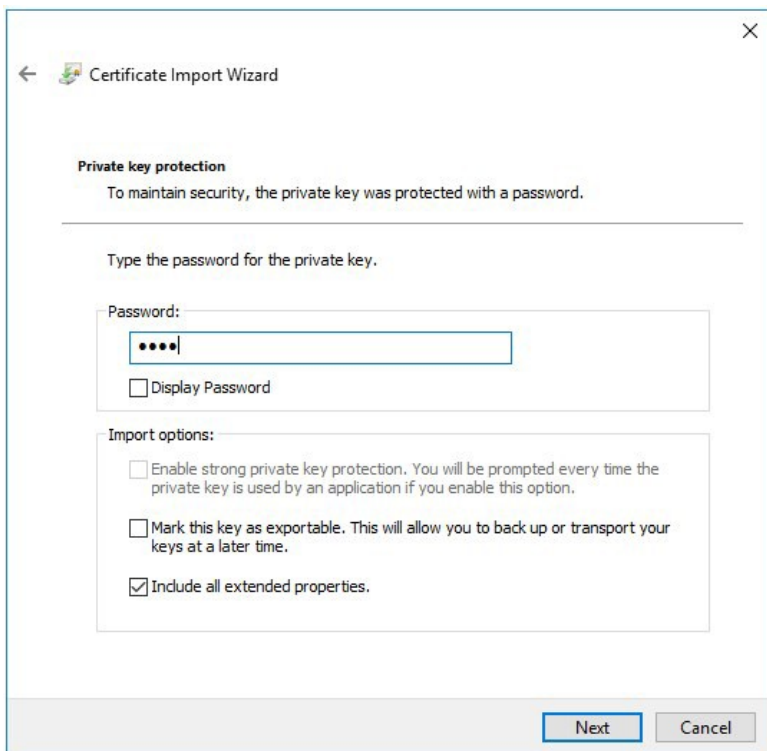
11. Select All Files (*.*) in file type drop down list, then select VTC.



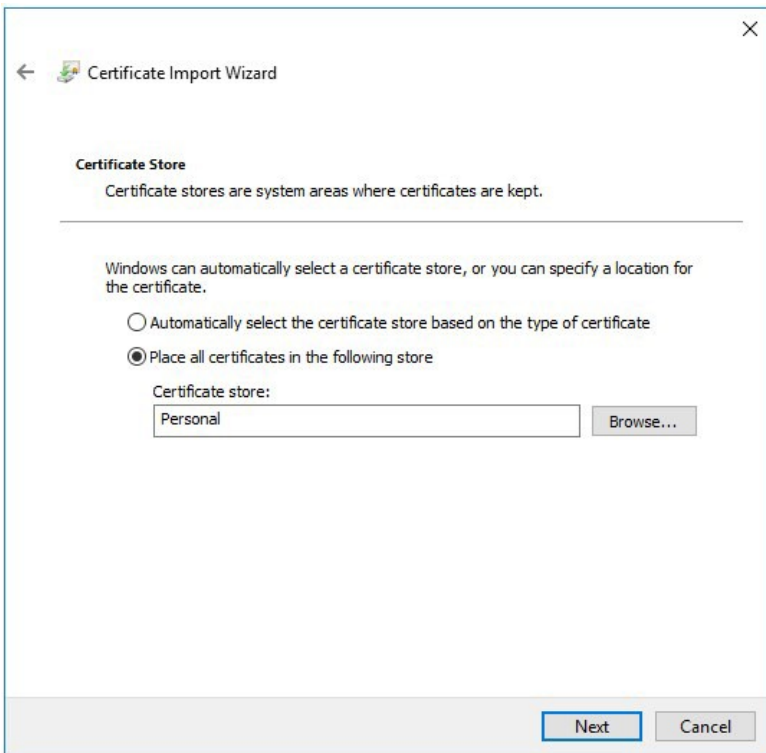
12. Click Next.



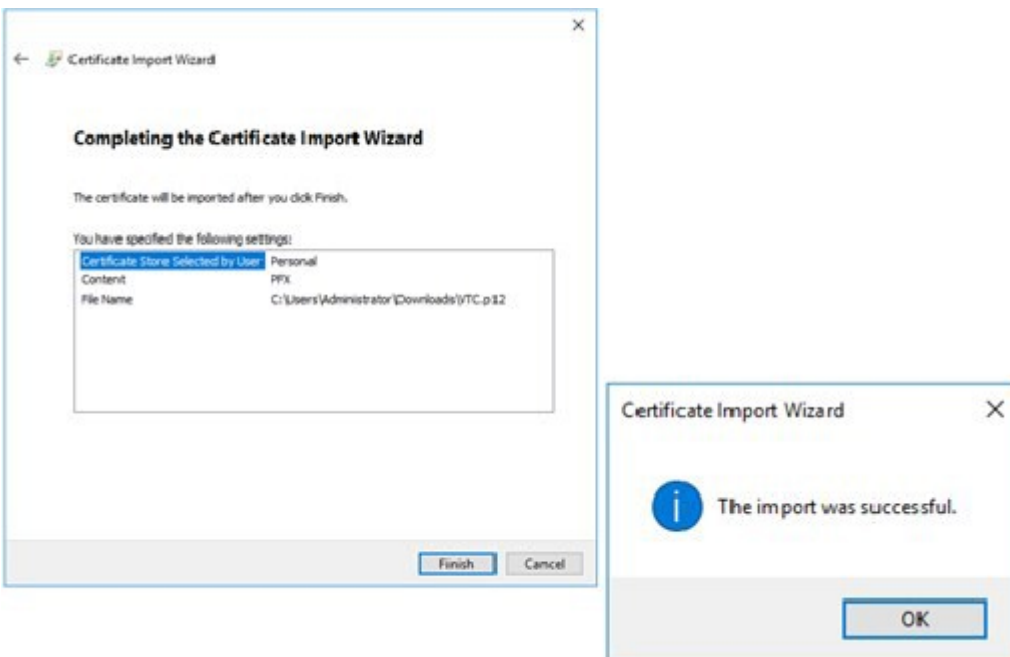
13. Input the password of private key and click Next.



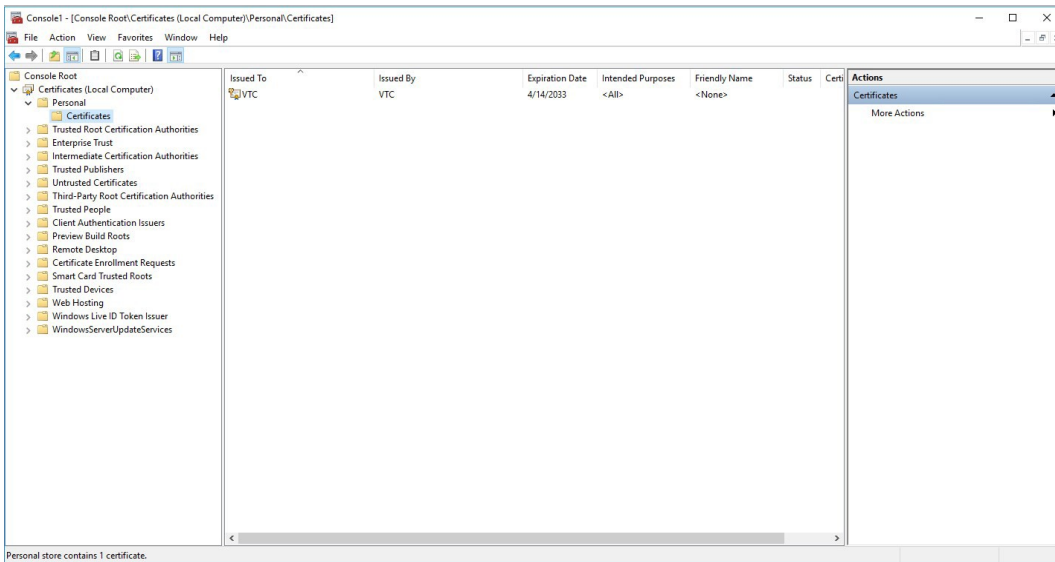
14. Choose Place all certificates in the following store and click Next.



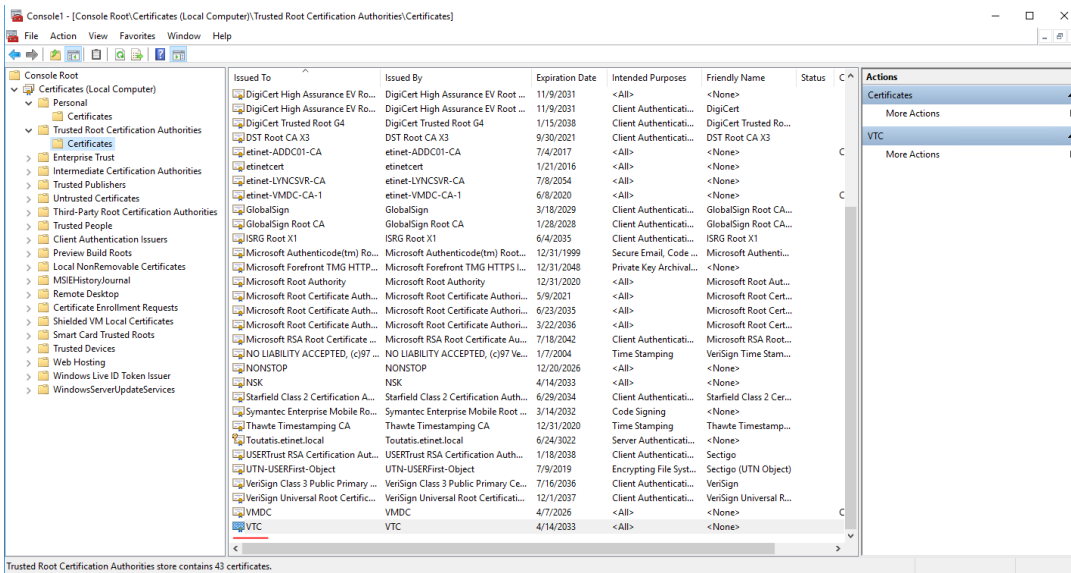
15. Once you complete the import, the Import wizard will prompt the The import was successful message.



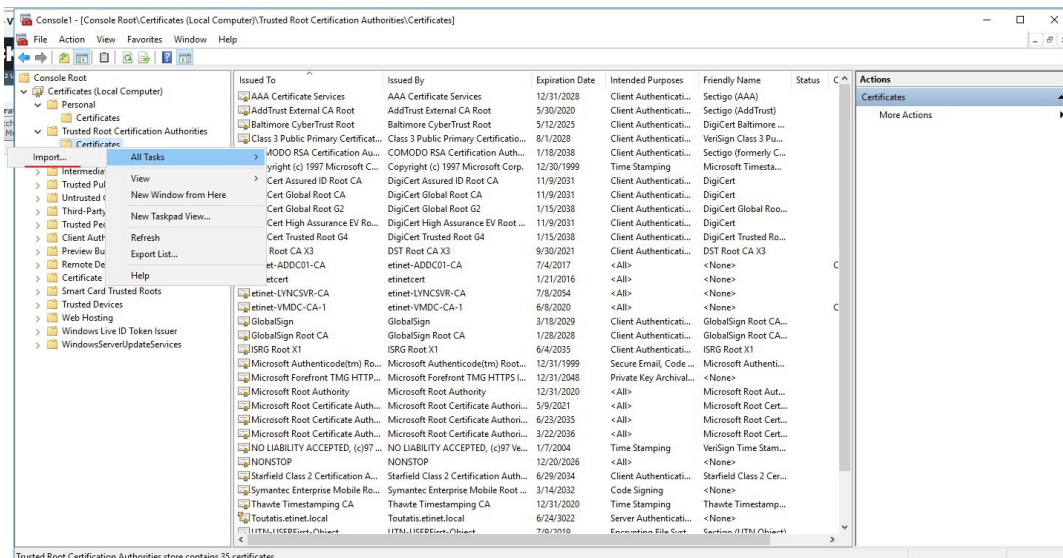
16. The VTC certificate can be located under Certificates (Local Computer) > Personal > Certificates folder.

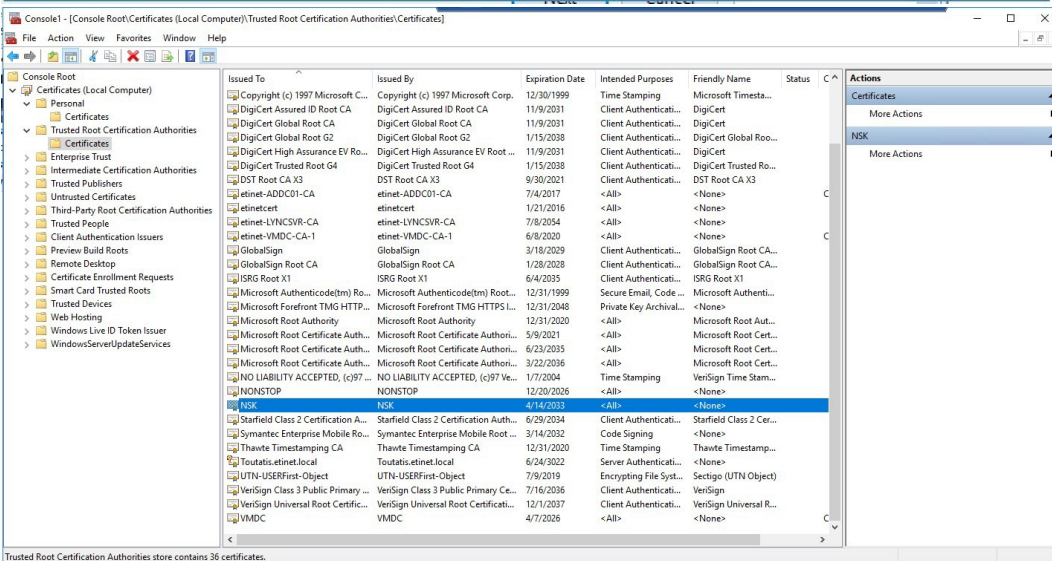
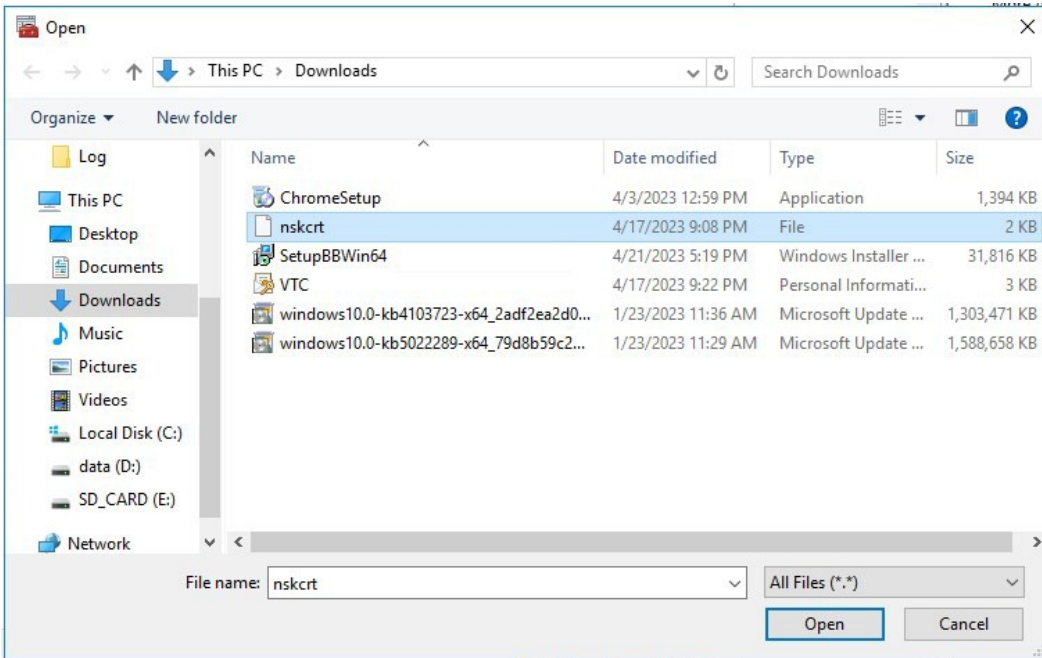


17. Repeat steps 8 to 16 to import VTC certificate to Trusted Root Certification Authorities > Certificates folder. Make sure Stand Alone Load works properly. Skip this step if the certificate is not self-signed.

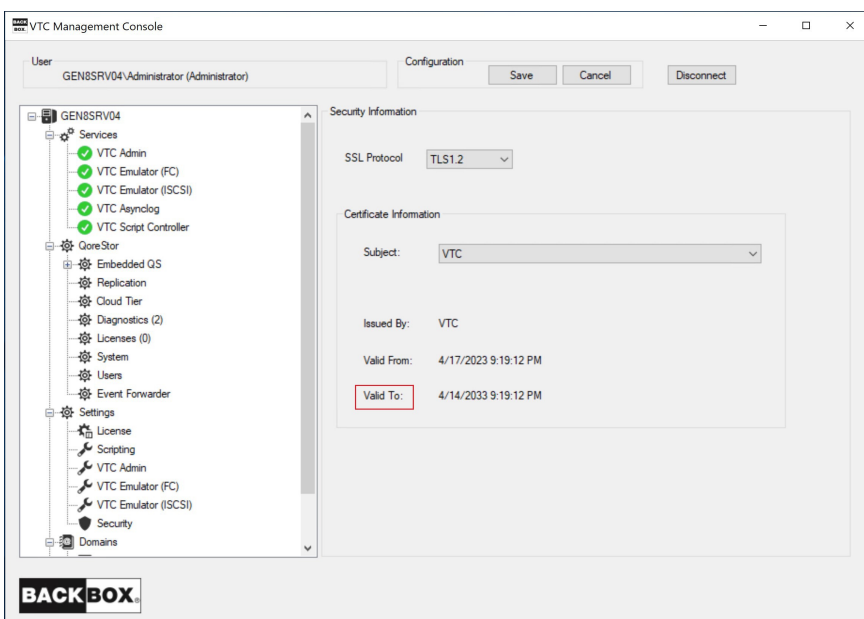


18. Repeat steps 8 to 16 to import NSK certificate to Trusted Root Certification Authorities > Certificates folder. Select nskcert in step 11. The NSK certificate can be found under Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates folder.





19. Certificate Information has been correctly added to the VTC MC and selected accordingly under Settings > Security.



APPENDIX C - CERTIFICATES UPGRADE ON NONSTOP

Certificates are part of the upgrade procedure, therefore they need to be up to date.



When upgrading to version 4.12 with SSL enabled, the default certificates provided by ETI-NET with previous version(s) need to be upgraded, as well.

In order to have the certificates updated to be at the latest version, retrieve the new certificates from the BBE412 package using the following TACL command:

```
UNPAK BBE413 E413
```