BackBox® E4.07 SSL Setup

Published: February 2019

Edition: H06.06, J06.06 or L06.06 RVUs, or subsequent H-series, J-series or L-series RVUs

Legal Notice

Table of Contents

Introduction **4**

Related Documentation 4

Enabling SSL 4

SSL configuration 5

Procedure to enable or disable SSL 5

SSL in the UI **6**

SSL in the NonStop **7**

Stop all BackPak programs 7

Enabling /disabling SSL 7

Enabling SSL Trace 8

BB053_SSL macro 8

Troubleshooting 8

SSL in the VTC **9**

Enabling /disabling SSL 9

Ciphers list configurations 11

Troubleshooting 13

Appendix **14**

Adding Certificates into Trust Root Certification Authorities 14

Certificates Configuration when using UI in workstation 14

INTRODUCTION

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

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

Platform	BackPak component	SSL product
NonStop	Domain manager, EMS Extractor, BBCMD & BB053 utilities	SecurLib/SSL is imbedded.
MS-Windows	UI, High-level services	SSL is embedded in MS .NET framework
MS-Windows	VTC low-level services such as the tape emulator	OpenSSL is included in the BackPak distribution set

Related Documentation

This manual is part of the BackPak documentation package and it is recommended to be consulted in addition to the following manuals: *BackBox User Manual* and *BackPack Messages Manual and Troubleshooting*.

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

https://www.comforte.com/products/protect/securlib-ssl/

http://www.openssl.org/docs/

http://technet.microsoft.com/en-us/library/bb727098.aspx

Enabling SSL

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

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

1. After all components have been succesfully installed and made sure that they communicate through TCP/IP, i.e. when the BackPak 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 BackPak 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 intial installation should be replaced with the customer's own cerificates, based on the security guidelines and polices in place.

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

There are two complementary tools to configure SSL:

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

Procedure to enable or disable SSL

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

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

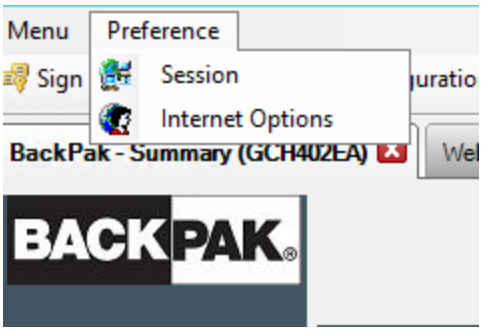
1. Stop the Backpak activity.
2. Stop the virtual tapes in SCF.
3. Stop the Windows services in VTCs.
4. Stop the NonStop BackPak processes.

SSL IN THE UI

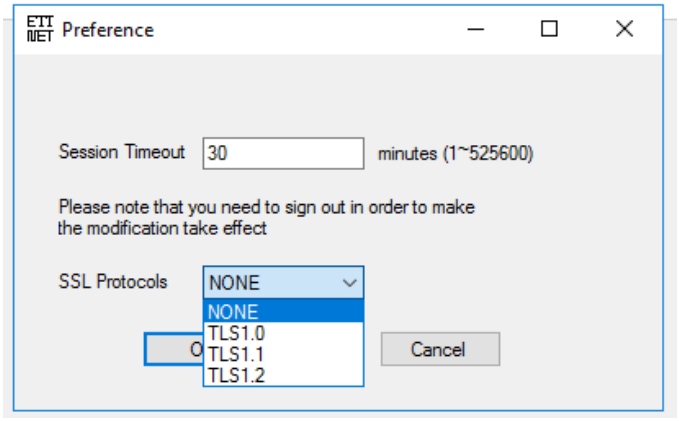
SSL must be enabled in all installations of the BackPak UI.

To enable the SSL:

1. Go to **Preference**> **Session**.



2. In the pop-up window choose from the drop-down list one of the SSL Protocols (NONE, TLS1.0, TLS 1.1, TLS 1.2), modify the session timeout value (in minutes, the maximum value is 525600) or use the default value.



The SSL Protocols selection field is disabled if the UI and the VTC are installed on the same server. In this case, SSL should be enabled through the VTC management console. For more info see the section SSL in the VTC.

If users have their own certificates (not the default ones in BackPak 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).

3. Click **OK**.

SSL IN THE NONSTOP

On the NonStop, the SSL library is provided by ComForte. The SecurLib/SSL product includes the SSL library, the OPENSSL utility and test certificates.

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 BackPak programs.

Stop all BackPak programs

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

```
VOLUME <BackPak-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.

Alternatively, when BB054_SHUTDOWN does not work:

```
VOLUME <BackPak-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 <BackPak-domain-installation-sub-volume>.NSKDER
SERVCERT <BackPak-domain-installation-sub-volume>.NSKCRT
CACERTS <BackPak-domain-installation-sub-volume>.VTCCRT
RANDOMDELAY 1
MINVERSION TLSv1.2
USESSL 1
```

Disabled SSL in SSLCFG - file content:

```
SERVKEYPASS TEST
SERVKEY <BackPak-domain-installation-sub-volume>.NSKDER
SERVCERT <BackPak-domain-installation-sub-volume>.NSKCRT
CACERTS <BackPak-domain-installation-sub-volume>.VTCCRT
RANDOMDELAY 1
MINVERSION TLSv1.2
USESSL 0
```

For *<BackPak-domain-installation-sub-volume>* use your own installation file location.

There is no need to configure SSL in the peripheral nodes, just to enable the SSL.

Enabling SSL Trace

Enabling the SSL trace is not mandatory. It can be enabled by request.

LOGLEVELFILE must be set only through the BB053_SSL macro.

LOGFILE must not be set anywhere; it is always generated internally by BackPak as a file name located in the BackPak trace sub-volume. The log file name is built with the prefix “SS” and the BackPak process name.

LOGLEVELFILE greater than 0 enables the SSL logging. Be sure the BackPak trace sub-volume is set in the BackPak configuration on the domain page.

BB053_SSL macro

```
VOLUME <BackPak-domain-installation-sub-volume>
LOAD /KEEP 1/ MACROS BBSETUP
BB053_SSL [ LOGLEVELFILE <nnn> ]
            [ CLIENTKEYPASS {yes | no} ]
            [ SERVKEYPASS {yes | no} ]
            [ CLIENTKEY {<file-name> | no}]
            [ SERVKEY {<file-name> | no}]
            [ CHECK {LIST | NOLIST}]
```

The macro stores the value specified for parameters LOGLEVELFILE, CLIENKEYPASS, CLIENTKEY, SERVKEYPASS and SERVKEY in the BackPak configuration.

Do not change any value for the following parameters: CLIENKEYPASS, CLIENTKEY, SERVKEYPASS and SERVKEY.

Troubleshooting

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

Error 0x1408F10B in EMS

2014-07-22 15:17:07 \ETINIUM.$X0DN ETINET.100.100 3479 GCE401EA-E3479 SSL library error 336130315 (= 0x1408F10B) on socket 7 with Server role –.

SSL IN THE VTC

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

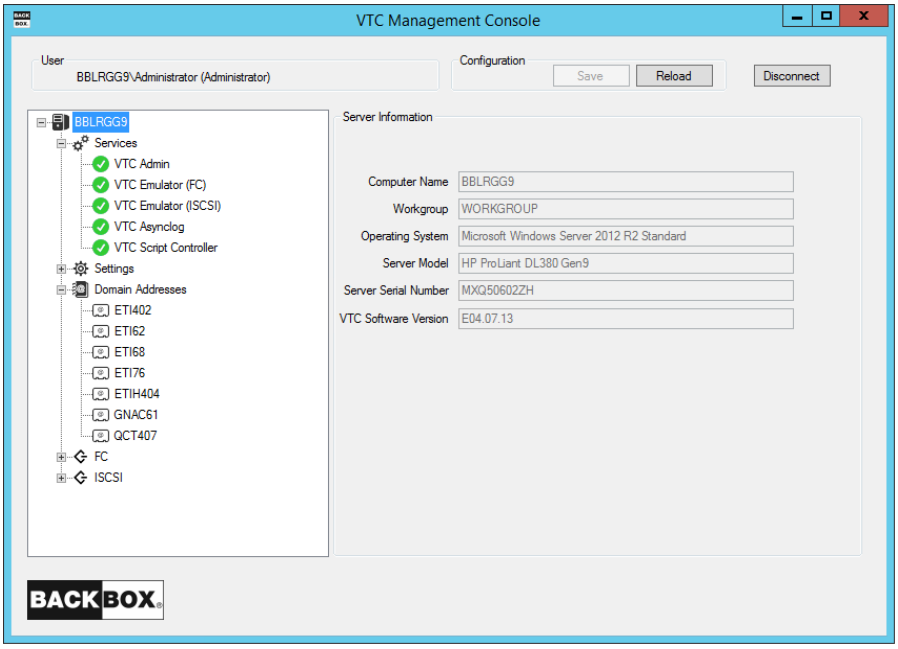
SSL server mode for VTC Server components is implemented using OpenSSL library version 1.1.0h.

SSL client mode for VTC Server components is implemented either using OpenSSL Library or Microsoft Secure Channel.

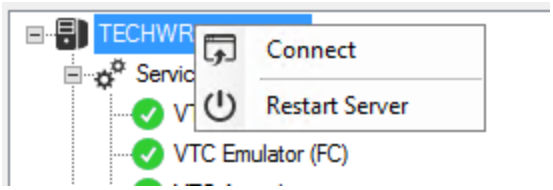
Enabling /disabling SSL

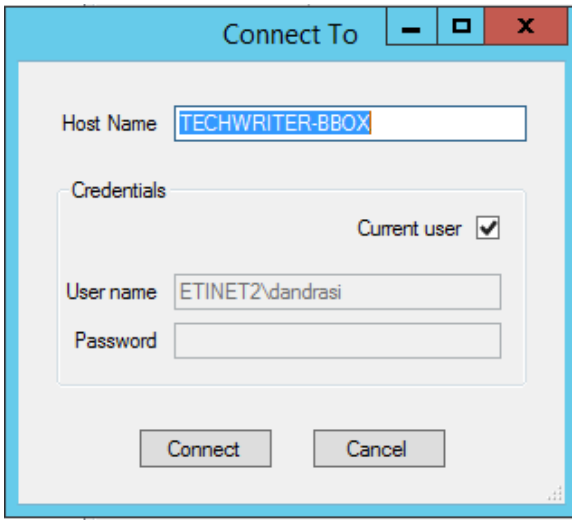
To enable or disable SSL, start an instance of VTC Management Console and access each VTC Server locally or remotely.

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

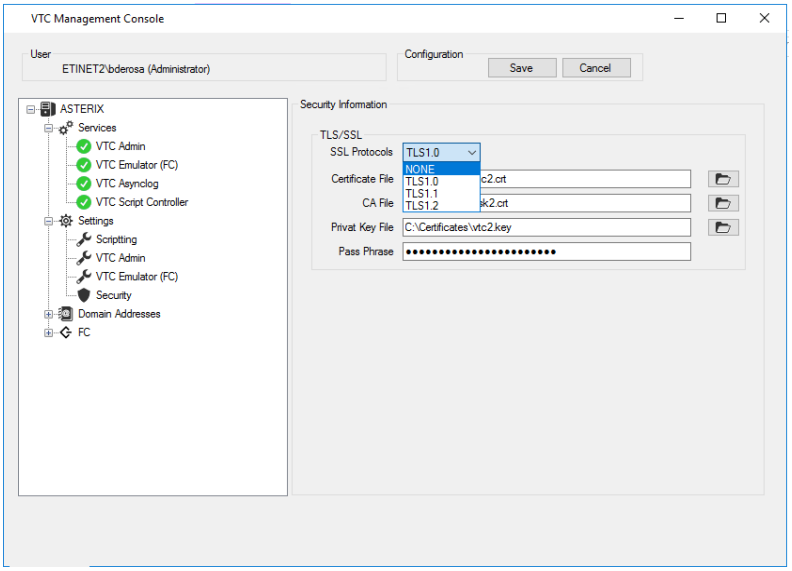


Connect to the target VTC Server if not currently the server requiring management and provide appropriate credential. To connect to a new VTC Server, you need to right-click on the server node and select the **Connect** action.





Expand the **Settings** node and select the **Security** one. A **Security Information** pannel 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.

Certificate File: Point to a mandatory PEM format certificate file used to identify the VTC Server in TLS/SSL channel communication. Only PEM format is supported. The cerificate file provided by ETI NET is the file located in **C:\ProgramData\ETINET\VTC\Cert\vtc.crt**.

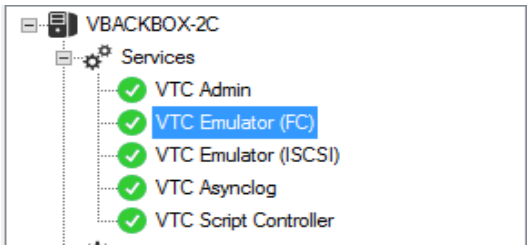
In case of self-signed certificate, add server certificate into the Trust Root Certification Authorities Store. See Add Certificates into Trust Root Certification Authorities in the *Appendix*.

CA File: Point to an optionally PEM format certificate file that identify the Certificate Authority use in TLS/SSL channel communication. Only PEM format is support. CA certificate must also be added into the Trust Root Certification Authorities Store. The CA file provided by ETI NET is the file located in **C:\ProgramData\ETINET\VTC\Cert\nsk.crt**.

Private Key File: Point to a mandatory PEM format file that contain the private key use in TLS/SSL channel communication. Only PEM format is support. The private key file should be protected using a password. The private key file provided by ETI NET is the file located in **C:\ProgramData\ETINET\VTC\Cert\vtc.key**.

Pass Phrase: Password used to protect the private key. If you use ETI NET cerificate, the pass phrase is: test

After enabling or disabling TLS/SSL 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.



Ciphers list configurations

By default, the server and client ciphers list is initialized with:

ALL:!aNULL:!eNULL:@STRENGTH

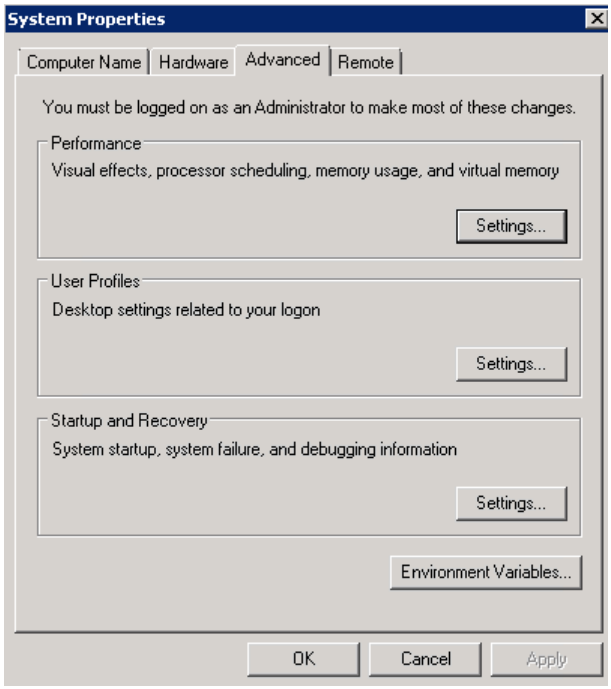
The list can be customized by providing the following system environmental variables.

VTCOPENSSL_SRV_CIPHER_LIST to customize server mode ciphers list.

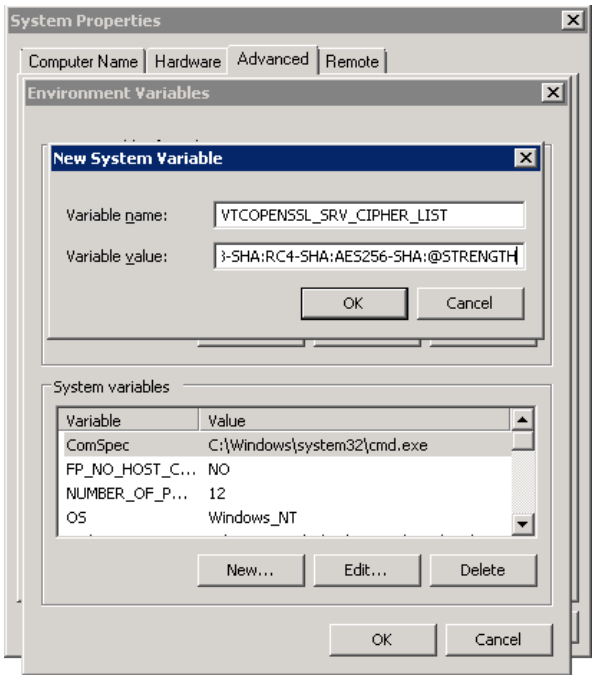
VTCOPENSSL_CLI_CIPHER_LIST to customize client mode ciphers list.

For the variable input value, refer to the OpenSSL syntax described at https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.

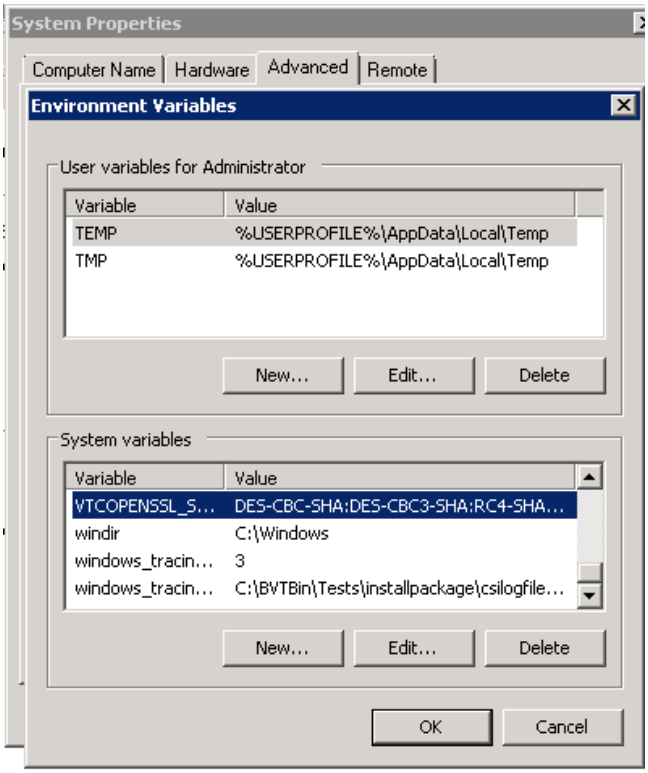
To change cipher list, open the server system **Advanced system settings** and click on **Environment Variables...**.



Add the variable(s) into **system variables**.



Acknowledge the change and verify that the variable was added correctly.



To enforce the change, all VTC services will need to be restarted on the server.

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 TACL by the BackPak macros:

LISTT <file-name-pattern>

VIEWT <file-name>

APPENDIX

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)

Please not that CA and Certificate file must be PEM format.

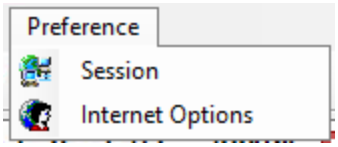
For more details on how to add CA or Certificate File to the Trust Root Certification Authorities Store please refer to according documentation for the OS you are using.

Certificates Configuration when using UI in workstation

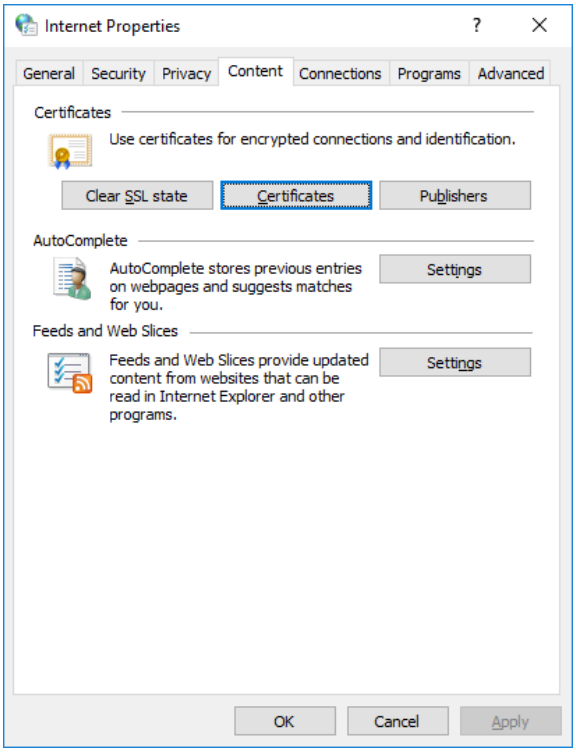
⚠ Perform the following steps only if the User Interface is installed on a workstation.

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

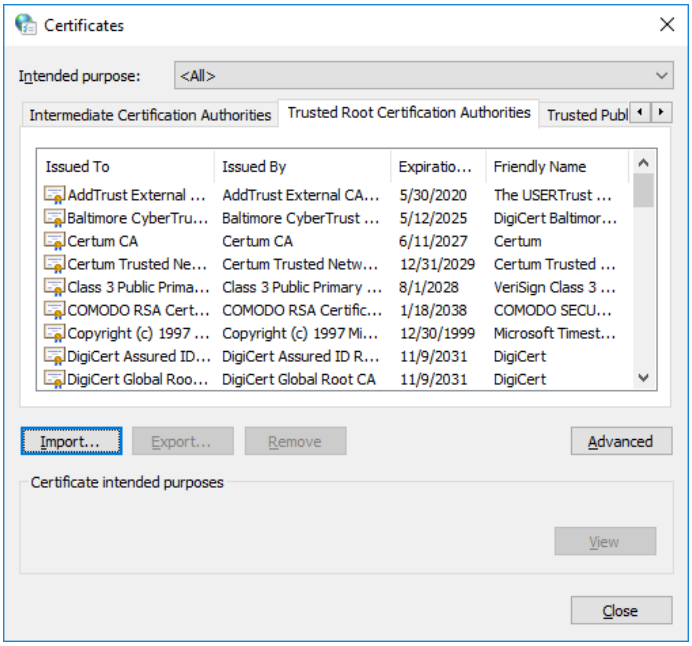
1. On the BackBox UI menu > **Preference** > **Internet Options**.

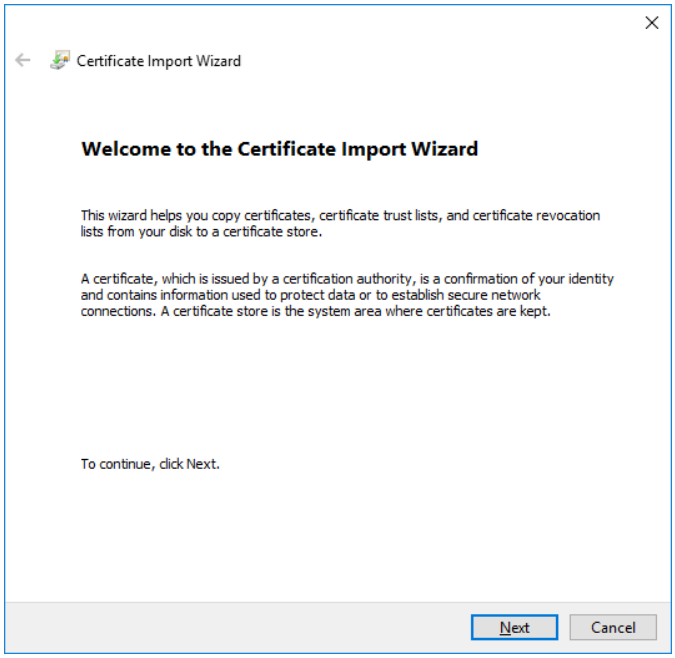


2. In the pop-up window click on the **Content** tab and then choose **Certificates** in the appropriate section.

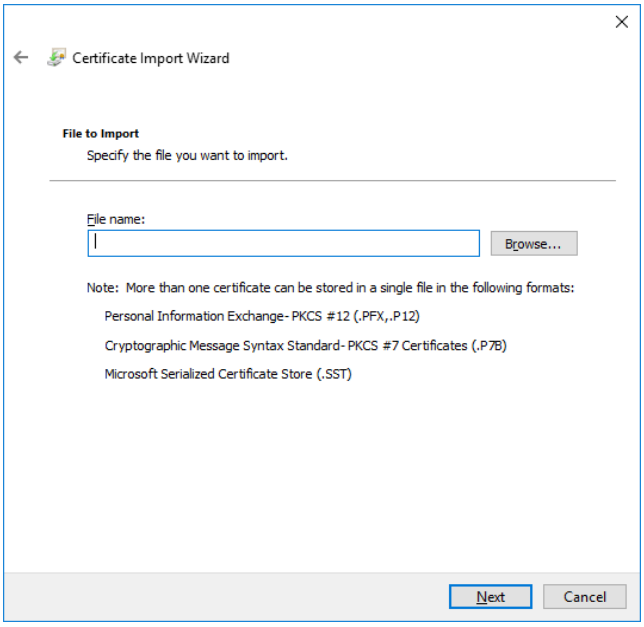


3. In the Certificates window select **Trusted Root Certification Authority** and **Import**.



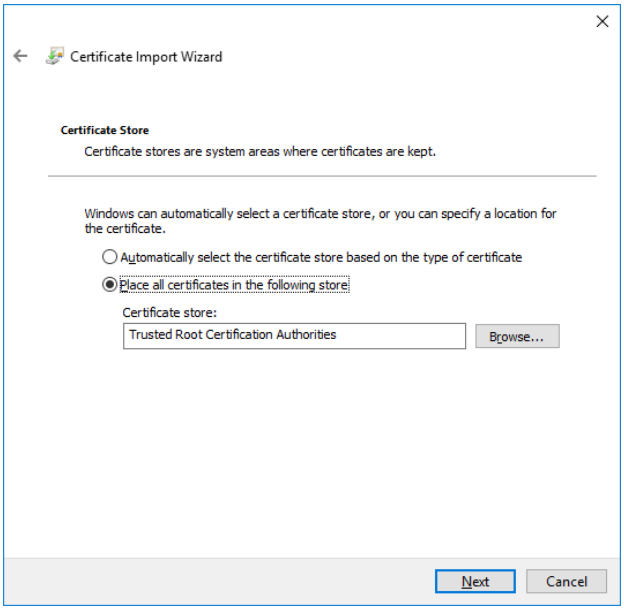


4. Specify the file to be imported. Browse it or simply pasted in the File name field. Click **Next**.



The certificates and the key files provided by ETI-NET can be found in **C:\ProgramData\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.