

# BackBox<sup>©</sup> E4.13 SSL Setup

Abstract

This SSL Setup document is for E4.13

Published: May 2024



© Copyright 2013, 2024 ETI-NET Inc. All rightsreserved.

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-NETproducts 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 rightsreserved.

## 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 1	12
Adding Certificates into Trust Root Certification Authorities	12
Certificates Configuration	12
APPENDIX B - CERTIFICATE STORE 1	16
APPENDIX C - CERTIFICATES UPGRADE ON NONSTOP 2	25

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 polices in place. For more details, see <u>Appendix B - Certificate Store</u> and <u>Appendix C - Certificates Upgrade on Nonstop</u>.

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

1. Go to Preference > Session.

Menu	Preference	
💐 Sign	🚰 Session	Back
	Internet Options	
BackBo	Internet Options	Т
BackBo	Internet Options     Summary (REGE412)	
BackBo	CKBOX	

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

ETT Preference			-		×
Session Timeout	3000	minu	tes (1~5256(	00)	
the modification t	ake effect	out in order	to make		
SSL Protocols	TLS1.2	$\sim$			
	Ok		Cancel		

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 <u>SSL in the VTC</u> .
If the UI is separately installed on another instance than the VTCMC, 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 <u>Adding Certificates into Trust Root Certification Authorities</u> in the <u>Appendix A</u>).

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.



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.\$X0DN 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.

GEN8SRV	Connect
🗸 🔨 лл	Restart Server
	lator (FC)
Box Connect To	- 🗆 X
Host Name gen8srv04	~
Credentials	Current user 🔽
User name GEN8SRV	04\Administrator
Password	
Connect	Cancel

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.

lser	Configuration		
GEN8SRV04\Administrator (Administrator)	Save Cancel Disconnect		
GEN8SRV04	Security Information		
Services			
	SSI Protocol TI S1 2		
VTC Emulator (FC)	1231.2 0		
VTC Emulator (ISCSI)			
VTC Asynclog	Cotificate Information		
VTC Script Controller	Cetulcate molination		
Gore Stor	C-block umm		
Embedded QS	Subject: VIC	1	
Replication			
Cloud Tier			
Diagnostics (2)	leaved By: VTC		
Licenses (0)	10000 DJ. 110		
System	Valid From: 4/17/2023 9-19-12 PM		
Event Forwarder	Valid To: 4/14/2033 9:19:12 PM		
Scripting			
VTC Admin			
VTC Emulator (FC)			
VTC Emulator (ISCSI)			
Security			
Domains			
I T _			

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 servery 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 <u>Add Certificates into Trust Root</u> <u>Certification Authorities</u> in the <u>Appendix A</u>.



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 TACL by the BackBox macros:

LISTT <file-name-pattern>

VIEWT <file-name>

### 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.

ntermediate Certific	cation Au	thorities	Trusted Root	Certification Aut	horities	Trusted Pub	
Issued To		Issued B	y	Expiratio	Friend	y Name	^
AddTrust Exte	rnal	AddTrust	External CA	5/30/2020	The US	ERTrust	
Baltimore Cybe	erTru	Baltimore	CyberTrust	5/12/2025	DigiCer	rt Baltimor	T
Certum CA		Certum C	A	6/11/2027	Certum	1	
Certum Truste	d Ne	Certum T	rusted Netw	12/31/2029	Certur	n Trusted	
Class 3 Public F	Prima	Class 3 P	ublic Primary	8/1/2028	VeriSig	n Class 3	
COMODO RSA	Cert	COMODO	RSA Certific	1/18/2038	COMO	DO SECU	
Copyright (c)	1997	Copyrigh	t (c) 1997 Mi	12/30/1999	Microso	oft Timest	
DigiCert Assure	ed ID	DigiCert	Assured ID R	11/9/2031	DigiCer	t	
						-	
Import	xport	R	emove			Advan	ice
ertificate intended	purpose	s					
						Mining	

← 🛃	Certificate Import Wizard
	Welcome to the Certificate Import Wizard
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
	To continue, click Next.
	<u>N</u> ext Cancel

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

×

Caraifi	the file way want to impact		
Specify	the file you want to import.		
File nam	e:		
-			Browse
Micro	soft Serialized Certificate Stor	e (.SST)	

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.

Certificate Store	
Certificate stores are system areas where certificat	tes are kept.
Windows can automatically select a certificate store the certificate.	e, or you can specify a location for
○ Automatically select the certificate store base	ed on the type of certificate
Place all certificates in the following store	
Certificate store:	
Trusted Root Cerunication Authonities	Browse

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

← 4	Certificate Import Wizard		×
	Completing the C	Certificate Import Wizard	
	The certificate will be impor	ted after you dick Finish.	
	Certificate Store Selected Content File Name	i by User Trusted Root Certification Authorities Certificate \\etifps01.	
	<		>
		<u>F</u> inish Ca	ancel

## **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.

🖻 Run	
Ø	Type the name of a program, folder, document, or Internor resource, and Windows will open it for you.
Open:	mmc
	This task will be created with administrative privilege

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

File Action view Favorites Window	v Help		- 8 >
New	Ctrl+N		
Open	Ctrl+O		Actions
Save	Ctrl+S	-	Console Root
Save As		There are no items to show in this view.	More Actions
Add/Remove Snap-in	Ctrl+M		
Options			
1 C:\Users\\Console1			
2 C:\Windows\system32\eventvwr			
3 C:\Windows\System32\virtmgmt			
4 C:\Windows\system32\compmgmt			
Exit			

3. Choose Certificates item and click the Add button.

-	Contractor and			Canada Dant	
ap-in	Vendor				Edit Extensions
ActiveX Control	Microsoft Cor				Remove
Authorization Manager	Microsoft Cor				
Certificates	Microsoft Cor				
Component Services	Microsoft Cor				Move Up
Computer Managem	Microsoft Cor				Move Down
Device Manager	Microsoft Cor		Add >		MOVE DOWN
Disk Management	Microsoft and				
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
Hyper-V Manager	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor	V			Advanced
ription:					

4. Choose Computer account and click Next.

Certificates snap-in			×
This snap-in will always manage certificates for: My user account Service account Computer account			
	< Back	Next >	Cancel

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

elect Computer		
Select the computer you want this snap-in	to manage.	
This snap-in will always manage:		
Local computer: (the computer this	console is running on)	
O Another computer:		Browse
Allow the selected computer to be only applies if you save the console	changed when launching from the co	ommand line. This

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

				beleeted andp may	
iap-in v	/endor	^		Console Root	Edit Extensions.
ActiveX Control M	Aicrosoft Cor			Certificates (Local Computer)	2
Authorization Manager M	licrosoft Cor			A CONTRACTOR OF CONTRACTOR	Remove
Certificates M	licrosoft Cor				
Component Services M	Aicrosoft Cor				Move Up
Computer Managem M	Aicrosoft Cor				
Device Manager M	Aicrosoft Cor				Move Down
Disk Management M	licrosoft and		Add >		
Event Viewer M	licrosoft Cor				
Folder M	licrosoft Cor				
Group Policy Object M	licrosoft Cor				
Hyper-V Manager M	licrosoft Cor				
IP Security Monitor M	licrosoft Cor				
IP Security Policy M M	Aicrosoft Cor	~			Advanced
<u></u>		1000			

7. Expand Certificates (Local Computer) tree node.

	zıh	- 6 7
Console Root	Name	Actions
	Cettificates (Local Computer)	Console Root

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

🗢 🔿 📶 🖾 🕼 📷					
Console Root Grutificates (Local Computer)	Object Type			Actions	
Find Certificates		There are no items to sho	w in this view.	More Actions	
All Tasks	Find Certificates				
View     View     New Window from Here	Request New Certificate Import				
> New Taskpad View	Advanced Operations >				
Refresh     Export List     Export List     Hep     Sonart Caro Inutes Roots     Work Obting     Web Hosting     Windows Live ID Toke Insuer     Windows Server/UpdateServices					

#### 9. Click Next to start the import.

Welcome to	the Certific	ate Impor	t Wizard		
This wizard helps yo lists from your disk t	u copy certificate o a certificate sto	s, certificate tru re.	ist lists, and cer	ificate revocation	
A certificate, which and contains inform connections. A certi	is issued by a cert ation used to prot ficate store is the	ification author ect data or to e system area wi	ity, is a confirma stablish secure i here certificates	tion of your identi network are kept.	ty
Store Location					
O <u>C</u> urrent User					
<u>L</u> ocal Machine					
To continue, click Ne	ext.				

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

🛃 Certi	ficate Import \	Wizard			
File to	Import				
Sp	ecify the file yo	u want to import.			
File	e name:				3 <u></u> 3
1					Browse
No	te: More than	one certificate can	be stored in a	single file in the fo	llowing formats:
	Personal Inform	mation Exchange-1	PKCS #12 (.PFX	(,.P12)	
	Cryptographic	Message Syntax S	tandard-PKCS	#/ Certificates (.)	·/B)
	MICTOSOTE SETIA	iiizeu Cerunicate St	ore (.551)		

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

🚰 Open		<u>1</u>		X
$\leftrightarrow \rightarrow \land \uparrow \clubsuit$	This PC > Downloads	5 V	Search Downloads	Q
Organize 🔻 New fo	lder			•
Quick access Desktop  Downloads  Documents  Pictures BBOX	Name ChromeSetup nskct SetupBBWin64 VTC windows10.0-kb4103723-x64_2adf2ea2d0 windows10.0-kb5022289-x64_79d8b59c2	Date modified 4/3/2023 12:59 PM 4/17/2023 9:08 PM 4/21/2023 5:19 PM 4/17/2023 9:22 PM 1/23/2023 11:36 AM 1/23/2023 11:29 AM	Type Application File Windows Installer Personal Informati Microsoft Update Microsoft Update	Size 1,394 KB 2 KB 31,816 KB 3 KB 1,303,471 KB 1,588,658 KB
Config Log This PC Desktop	name: VTC	~	All Files (*.*)	~
			Open	Cancel

12. Click Next.

Specify the file	you want to import.	
File name:		
C:\Users\Adn	ninistrator\Downloads\VTC.p12	Browse
Microsoft S	erialized Certificate Store (.SST)	

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

Pr	ivate key protection
	To maintain security, the private key was protected with a password.
	Type the password for the private key.
	Display Password
	Import options:
	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.

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

Certificate Store				
Certificate s	tores are system areas w	here certificates a	re kept.	
Windows ca the certifica	n automatically select a ce te.	ertificate store, or	you can specif	y a location for
O Autor	natically select the certific	ate store based or	the type of c	ertificate
Place	all certificates in the follow	wing store		
Certi	ficate store:			-
Pers	sonai			Browse

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

- 🗜 Certificate Import Wiz	ard		
Completing the	e Certificate Import Wizard		
The certificate will be in	ported after you click Firish.		
You have specified the	following settings:		
Certificate Store Selec	tect by User Personal		
Content	PPX		
25		Certificate Import Wizard	×
		The import was successful.	
	Finish Cancel		1

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

🦈   Za 🖬   🖬   🖻 📑 🚺 🛅								
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status Cert	Actions	
Certificates (Local Computer)	<b><sup>®</sup></b> INTC	VTC	4/14/2033	<all></all>	<none></none>		Certificates	
Certificate     Certification Authonities     Enterprise Trust     Instremediate Certification Authonities     Trusted Publishers     Untrusted Certification Authonities     Trusted Publishers     Trusted Publishers     Trusted Publishers     Trusted Publishers     Trusted Publishers     Trusted Publishers     Certificate Certification Authonities     Sender Authonities     Trusted Publishers     Certificate Certification Authonities     Windows: Intel Toten Issuer     WindowsServerUpdateServices							More Actions	

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.

aprole Root	· · · ·				51 N. M.	<b>6</b> 1	<i>c</i> *	Antina	
Certificates (Local Computer)	Issued to	Issued By	Expiration Date	intended Purposes	Friendly Name	Status	. C	Actions	
Personal	DigiCert High Assurance EV Ko	DigiCert High Assurance EV Root	11/9/2031	SAIR A REAL FOR	<ivone></ivone>			Certificates	
Certificates	LaDigiCert High Assurance EV Ko	DigiCert High Assurance EV Root	11/9/2031	Client Authenticati	DigiCent			More Actions	
Trusted Root Certification Authorities	DigiCert Trusted Root 64	DigiCert Trusted Koot G4	1/15/2038	Client Authenticati	DigiCert Trusted Ko			VTC	
Certificates	LaDST ROOT CA X3	UST KOOT CA X3	9/30/2021	Client Authenticati	UST ROOT CA AS			vic	
Enterprise Trust	Laletinet-ADDC01-CA	etinet-ADDC01-CA	//4/2017	<all></all>	<none></none>		C	More Actions	
Intermediate Certification Authorities	ligietinetcert	etinetcert	1/21/2016	<all></all>	<none></none>				
Trusted Publishers	La etinet-LYNCSVR-CA	etinet-LYNCSVR-CA	//8/2054	<all></all>	<none></none>				
Untrusted Certificates	ligi etinet-VMDC-CA-1	etinet-VMDC-CA-1	6/8/2020	<all></all>	<none></none>		C		
Third-Party Root Certification Authorities	GlobalSign	GlobalSign	3/18/2029	Client Authenticati	GlobalSign Root CA				
Trusted People	GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticati	GlobalSign Root CA				
Client Authentication Issuers	ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticati	ISRG Root X1				
Preview Build Roots	Microsoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root	12/31/1999	Secure Email, Code	Microsoft Authenti				
Local NonRemovable Certificates	Microsoft Forefront TMG HTTP	Microsoft Forefront TMG HTTPS I	12/31/2048	Private Key Archival	<none></none>				
MSIEHistoryJournal	Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<all></all>	Microsoft Root Aut				
Remote Desktop	Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	5/9/2021	<all></all>	Microsoft Root Cert				
Certificate Enrollment Requests	Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	6/23/2035	<all></all>	Microsoft Root Cert				
Shielded Vivi Local Certificates	Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	3/22/2036	<all></all>	Microsoft Root Cert				
Trusted Davies	Microsoft RSA Root Certificate	Microsoft RSA Root Certificate Au	7/18/2042	Client Authenticati	Microsoft RSA Root				
Web Horting	NO LIABILITY ACCEPTED, (c)97	NO LIABILITY ACCEPTED, (c)97 Ve	1/7/2004	Time Stamping	VeriSign Time Stam				
Windows Live ID Token Issuer	NONSTOP	NONSTOP	12/20/2026	<all></all>	<none></none>				
Windows Servert IndateServices	🕎 NSK	NSK	4/14/2033	<all></all>	<none></none>				
	Starfield Class 2 Certification A	Starfield Class 2 Certification Auth	6/29/2034	Client Authenticati	Starfield Class 2 Cer				
	Symantec Enterprise Mobile Ro	Symantec Enterprise Mobile Root	3/14/2032	Code Signing	<none></none>				
	🔄 Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp				
	🖏 Toutatis.etinet.local	Toutatis.etinet.local	6/24/3022	Server Authenticati	<none></none>				
	🔄 USERTrust RSA Certification Aut	USERTrust RSA Certification Auth	1/18/2038	Client Authenticati	Sectigo				
	UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst	Sectigo (UTN Object)				
	🔄 VeriSign Class 3 Public Primary	VeriSign Class 3 Public Primary Ce	7/16/2036	Client Authenticati	VeriSign				
	🔄 VeriSign Universal Root Certific	VeriSign Universal Root Certificati	12/1/2037	Client Authenticati	VeriSign Universal R				
	<b>WMDC</b>	VMDC	4/7/2026	<all></all>	<none></none>		c		
	VTC	VTC	4/14/2033	<all></all>	<none></none>				

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

ar 🔁 🔂 🗎	0 🔒 🛛 📷								
Console Root		Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	c ^	Actions
Certificates (Local (	Computer)	AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati	Sectigo (AAA)			Certificates
Personal		AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Client Authenticati	Sectigo (AddTrust)			Mare Actions
<ul> <li>Certificates</li> <li>Trusted Root Certification Authorities</li> </ul>		Baltimore CyberTrust Root	Baltimore CyberTrust Root Class 3 Public Primary Certificatio	5/12/2025	12/2025 Client Authenticati 1/2028 Client Authenticati	DigiCert Baltimore			MOTE ACTIONS
		Glass 3 Public Primary Certificat		8/1/2028		VeriSign Class 3 Pu			
Certificates	All Tasks	MODO RSA Certification Au	COMODO RSA Certification Auth	1/18/2038	Client Authenticati	Sectigo (formerly C			
Internetic	All Tasks	vright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta			
Tructed Pul	View	> Cert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031 Clien 11/9/2031 Clien	Client Authenticati	DigiCert			
Intrusted (	New Window from Here	Cert Global Root CA	DigiCert Global Root CA		Client Authenticati	DigiCert			
Third-Party		Cert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati	DigiCert Global Roo			
Trusted Per	New Taskpad View	Cert High Assurance EV Ro	DigiCert High Assurance EV Root	11/9/2031	Client Authenticati	DigiCert			
Client Auth	Refresh	Cert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati	DigiCert Trusted Ro			
Preview Bu	Export List	Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati	DST Root CA X3			
> Remote De	export costin	et-ADDC01-CA	etinet-ADDC01-CA	7/4/2017	<all></all>	<none></none>		с	
> 📫 Certificate	Help	etcert	etinetcert	1/21/2016	<all></all>	<none></none>			
<ul> <li>Smart Card Trust</li> <li>Trusted Devices</li> <li>Web Hosting</li> </ul>	sted Roots	etinet-LYNCSVR-CA	etinet-LYNCSVR-CA	7/8/2054	<all></all>	<none></none>			
	5	etinet-VMDC-CA-1	etinet-VMDC-CA-1	6/8/2020	<all></all>	<none></none>	c	c	
		GlobalSign	GlobalSign	3/18/2029	Client Authenticati	GlobalSign Root CA			
> III Windows Live II	D Token Issuer	GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticati	GlobalSign Root CA			
WindowsServer	rUpdateServices	ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticati	ISRG Root X1			
		Microsoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root	12/31/1999	Secure Email. Code	Microsoft Authenti			
		Microsoft Forefront TMG HTTP	Microsoft Forefront TMG HTTPS I	12/31/2048	Private Key Archival	<none></none>			
		Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<all></all>	Microsoft Root Aut			
		Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	5/9/2021	<all></all>	Microsoft Root Cert			
		Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	6/23/2035	<all></all>	Microsoft Root Cert			
		Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	3/22/2036	<all></all>	Microsoft Root Cert			
		NO LIABILITY ACCEPTED, (c)97	NO LIABILITY ACCEPTED, (c)97 Ve	1/7/2004	Time Stamping	VeriSign Time Stam			
		NONSTOP	NONSTOP	12/20/2026	<all></all>	<none></none>			
		Starfield Class 2 Certification A	Starfield Class 2 Certification Auth	6/29/2034	Client Authenticati	Starfield Class 2 Cer			
		Symantec Enterprise Mobile Ro	Symantec Enterprise Mobile Root	3/14/2032	Code Signing	<none></none>			
		Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp			
		Toutatis.etinet.local	Toutatis.etinet.local	6/24/3022	Server Authenticati	<none></none>			
		TITM.USEPEint.Object	UTN-USERFirst-Object	7/0/2010	Encounting File Surt	Section (UTM Object)		~	



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

Jser	Con	figuration		
GEN8SRV04\Administrator (Administrator)		Save Cancel Discor	nnect	
GEN8SRV04	A Security Information			
Services				
VTC Admin	SSI Protocol	TIS12		
		reone -		
VTC Emulator (ISCSI)				
	Certificate Informa	tion		
VTC Script Controller				
GoreStor	Subject:	VTC	~	
⊞ → ∰ Embedded QS	oubject.	VIC	Ť	
Replication				
一. doud Tier				
Diagnostics (2)	Issued By:	VTC		
Licenses (0)				
	Valid From:	4/17/2023 9:19:12 PM		
Ö Users				
Event Forwarder	Valid To:	4/14/2033 9:19:12 PM		
E Settings				
Scripting				
VTC Admin				
VTC Emulator (FC)				
VTC Emulator (ISCSI)				
Security				
🖻 💯 Domains	~			

## **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