BACKBOX®

BackBox[®] E4.11 SSL Setup

Published: October 2022

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



Legal Notice

© Copyright 2022 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-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 trademarks 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.

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
Restarting the EMS Extractor BBEXT	8
Troubleshooting	8
SSL in the VTC	9
Enabling /disabling SSL	9
Ciphers list configurations	1
Troubleshooting	4
Appendix1	5
Adding Certificates into Trust Root Certification Authorities	5
Certificates Configuration when using UI in workstation1	5

INTRODUCTION

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

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

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

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:

- After all components have been successfully 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 initial installation should be replaced with the customer's own certificates, 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:

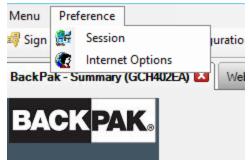
- 1. Stop the Backpak activity.
- 2. Stop the virtual tapes in SCF.
- 3. Stop the Windows services in VTCs.
- 4. Stop the NonStop BackPak processes.

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.

ETT NET Preference		-		×
Session Timeout 30	minute	es (1~52560)0)	
Please note that you need to sig the modification take effect	in out in order to	make		
SSL Protocols NONE	\sim			
NONE				
TLS1.0		ancel		
UTLS1.1	u	ancei		
TLS1.2				

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 <u>Adding Certificates into Trust Root Certification Authorities</u> 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



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 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.



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

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 enable the SSL.

Restarting the EMS Extractor BBEXT

Use the startup OBEY file OEXT in the BackPak-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 OpenSSL library version 1.1.1q.

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**.

GEN8SRV04\Administrator (Administrator)	Contra	guration Save Ca	Disconnec	t	
GENUSRV04 • ^Q Services • ^Q Services • VTC Emulator (FC) • VTC Emulator (FC) • VTC Emulator (FC) • VTC Emulator (FC) • VTC Script Controller • VTC Script Controller • VTC Script Controller • Other Embedded QS •	Workgroup Operating System		andard Copy To File.		

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.



Connect To 📒 🗖 🗙
Host Name TECHWRITER-BBOX
Credentials Current user 🗹
User name ETINET2\dandrasi
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.

VTC Management Console User ETINET2'bderosa (Administrator)		Configuration Save Cancel		×
ASTERIX Of Services Of Cadmin VTC Admitor (FC) Of Cadminator (FC) Of Cadminator (FC) VTC Asynclog VTC Soriet Controller Of Settings VTC Admin VTC Adminator (FC) Settings County Domain Addresses Of C	Privat Key File			

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 certificate 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:\Pro-gramData\ETINET\VTC\Cert\vtc.key**.

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

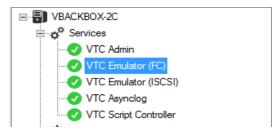


The Pass Phrase - if generated along with the certificate - will be validated by VTC MC.

Certificate, **CA** and **Private Key** files need to be granted for the SYSTEM local user with full access. See the screenshot below:

	Security	Details	Previous V	ersions	
Object	name: C	:\WIN-S	TORAGE\LB	COPYF1.INI	D
Group	or user nam	ies:			
SR S	YSTEM				
SE A	dministrator	s (GEN8	SRV04\Admir	nistrators)	
🥵 U	sers (GEN8	SRV04	Users)		
lo cha	nge permis	sions, clie	ck Edit.		Edit
emis	sions for SY	'STEM		Allow	Deny
Full	control			~	
Mod	fy			\checkmark	
Rea	d & execute			\checkmark	
Rea	d			\checkmark	
Write	e			\checkmark	
Spe	cial permiss	ions			
	cial permis	sions or a	idvanced set	tinas	Advanced
or spe					Advanced
	dvanced.				

All VTC services need to be restarted for the changes to take effect. You can restart all services 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 <u>https://www.openssl.or</u>-g/docs/man1.0.2/apps/ciphers.html.

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

System Properties
Computer Name Hardware Advanced Remote
You must be logged on as an Administrator to make most of these changes.
Performance Visual effects, processor scheduling, memory usage, and virtual memory
Settings
User Profiles
Desktop settings related to your logon
Settings
Startup and Recovery
System startup, system failure, and debugging information
Settings
Environment Variables
OK Cancel Apply

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

em Properties				L
omputer Name Hardv	vare Advanced	Remote		
vironment ¥ariable	es		1	×
New System Varia	ble		×	1
Variable <u>n</u> ame: Variable <u>v</u> alue:		_SRV_CIPHER_L	@STRENGTH	
	L		Cancel	
-System variables		<u></u>]
		OK		
Variable ComSpec FP_NO_HOST_C	C:\Windows\sy NO]
Variable ComSpec FP_NO_HOST_C NUMBER_OF_P	C:\Windows\sy NO 12			
Variable ComSpec FP_NO_HOST_C	C:\Windows\sy NO			
Variable ComSpec FP_NO_HOST_C NUMBER_OF_P	C:\Windows\sy NO 12			

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

System Properties	
Computer Name Hardw	vare Advanced Remote
Environment Variable	25
User variables for Ac	ministrator
Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp
	New Edit Delete
System variables	
Variable	Value
VTCOPENSSL_S	
windir	C:\Windows
windows tracin	3
windows_tracin	C:\BVTBin\Tests\installpackage\csilogfile 🧲
	New Edit Delete
_	OK Cancel

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.
- 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)



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.

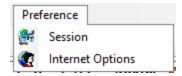
Certificates Configuration when using UI in workstation



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.

🍖 Internet Properties		?	×
General Security Privacy Content Connections	Programs	Adva	nced
Certificates	ns and identif	ication	.
Clear <u>S</u> L state <u>C</u> ertificates	Pu <u>b</u> lish	ers	
AutoComplete			- 1
AutoComplete stores previous entries on webpages and suggests matches for you.	Settin	gs	
Feeds and Web Slices			_
Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.	Settin	gs	
ОК	Cancel	App	bly

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

ntermediate Certification Au	thorities Trusted Root C	eruncadon Aut	nondes	Trusted Pub	
Issued To	Issued By	Expiratio	Friendly	/ Name	
AddTrust External	AddTrust External CA	5/30/2020	The US	ERTrust	
Baltimore CyberTru	Baltimore CyberTrust	5/12/2025	DigiCer	t Baltimor	1
Certum CA	Certum CA	6/11/2027	Certum		
Certum Trusted Ne	Certum Trusted Netw	12/31/2029	Certum	Trusted	
Class 3 Public Prima	Class 3 Public Primary	8/1/2028	VeriSigr	n Class 3	
COMODO RSA Cert	COMODO RSA Certific	1/18/2038	COMOD	O SECU	
Copyright (c) 1997	Copyright (c) 1997 Mi	12/30/1999	Microso	ft Timest	
DigiCert Assured ID	-	11/9/2031	DigiCer	t	
DigiCert Global Roo	DigiCert Global Root CA	11/9/2031	DigiCer	t	
Import Export	<u>R</u> emove			<u>A</u> dvar	10
				View	



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

ŀ	Specify the file you want to import.	
	Ele name: Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange-PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST)	

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**.

🖉 Certificate Import Wizard	
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
 Automatically select the certificate store based on the type of certificate 	
Trusted Root Certification Authorities Browse	
	Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

← 🎍	Certificate Import Wizard		
	Completing the C	Certificate Import Wizard	
	The certificate will be impor	ted after you dick Finish.	
	You have specified the follo	owing settings:	
	Certificate Store Selected	by User Trusted Root Certification Authoritie Certificate	s
	File Name	\etifps01.	
	<		>
		Fini	sh Cancel