ELO Suite for SAP ArchiveLink® (SAP NetWeaver® & SAP S/4HANA®)

ELO Smart Link for SAP® ERP – Configuring an SSL connection

Table of contents

ELO Smart Link for SAP® ERP – Configuring an SSL connection

Introduction

This documentation describes how to configure an SSL connection between an SAP system or the associated content repository and the ELO Smart Link for SAP® ERP interface, called ELO Smart Link in the following.

Basics

Certain requirements have to be met to configure an SSL connection between these two systems. For example, the SAP system kernel should be up-to-date and the SAP system should have the current cryptography library (CommonCryptoLib). The profile parameters used should also be configured so that the ELO Application Server cipher suites can be accepted.

You will find more information on SAP configuration and the required versions on the SAP support site under the following notes:

- *510007* – Additional information about setting up SSL on the Application Server ABAP
- *2287896* – saphttp and SSL: client cipersuites configuration

> **Information**
>
> Accessing the SAP Support Launchpad requires an S-user on SAP sites.

The ELO server setup must have also been performed with the settings for configuring an SSL connection with certificate chain.

Issues

One common reason why the SAP system won't connect to ELO Smart Link for SAP® ERP via SSL even though certificates have been imported is that no common cipher suite is found during negotiation.

This is because many SAP systems are only configured for the old TLS protocol version 1.0 as standard. By updating the kernel and the cryptography library, the SAP system also supports newer protocols. However, these have to be activated in the configuration (see information in the chapter Basics).

To test this scenario, we recommend setting the cipher suite parameters to `967:PFS:HIGH:MEDIUM:+e3DES::EC\_P256:EC\_HIGH`.

As the SAP system has to be restarted every time changes are made to these profile parameters, we recommend using a very high profile parameter value right from the start.

Configuration in the SAP system

First, export the certificate from ELO and import it to the corresponding SAP system. Use an up-to-date browser. In this example, we used Firefox.

Certificate export

The certificate can be exported right within the browser using the ELO Smart Link for SAP® ERP configuration interface.

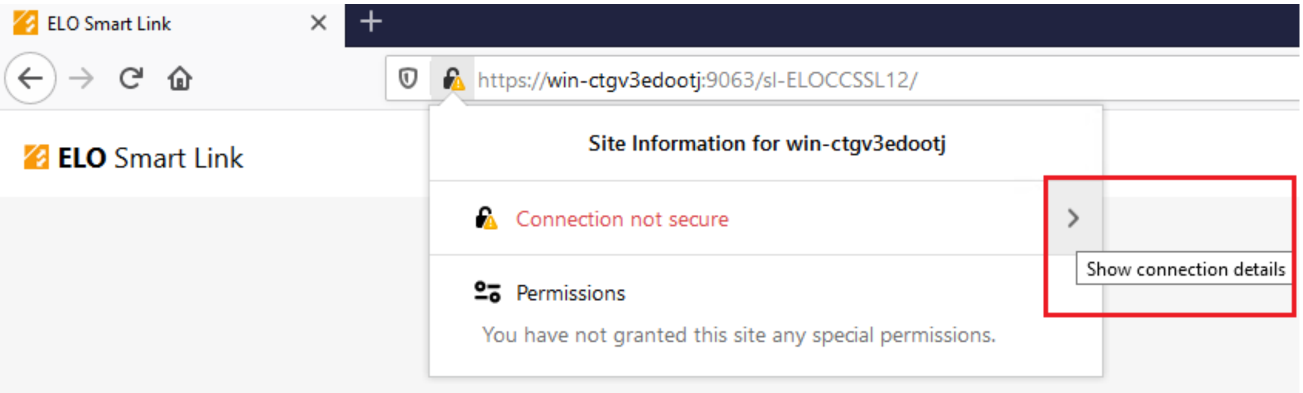

ELO Smart Link
https://win-ctgv3edootj:9063/sl-ELOCCSSL12/
ELO Smart Link
Site Information for win-ctgv3edootj
Connection not secure
Show connection details
Permissions
You have not granted this site any special permissions.

Fig.: Browser: Connection details

1. Navigate to the connection details in the browser address bar.

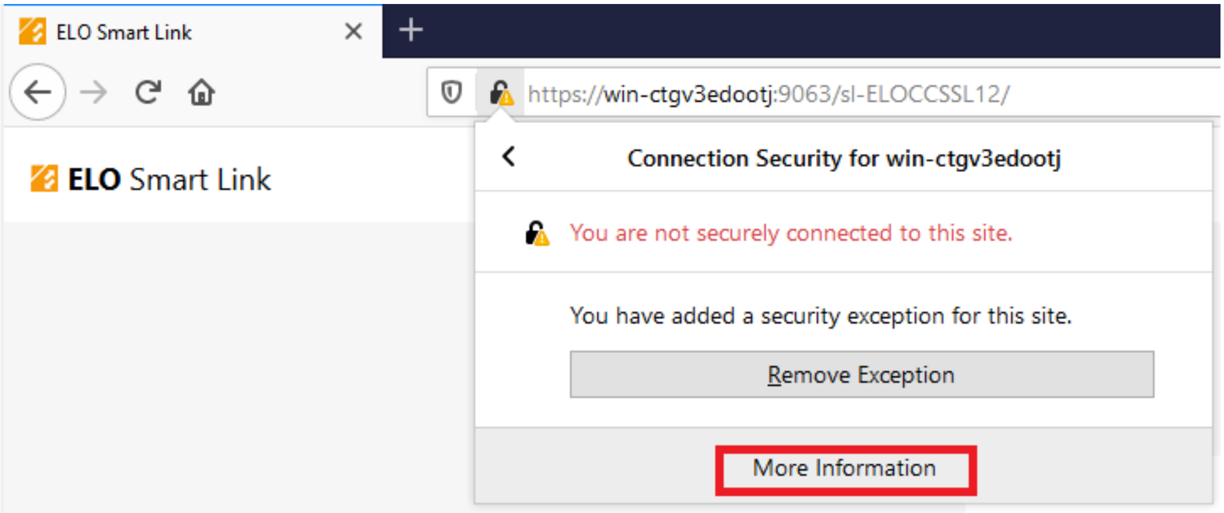
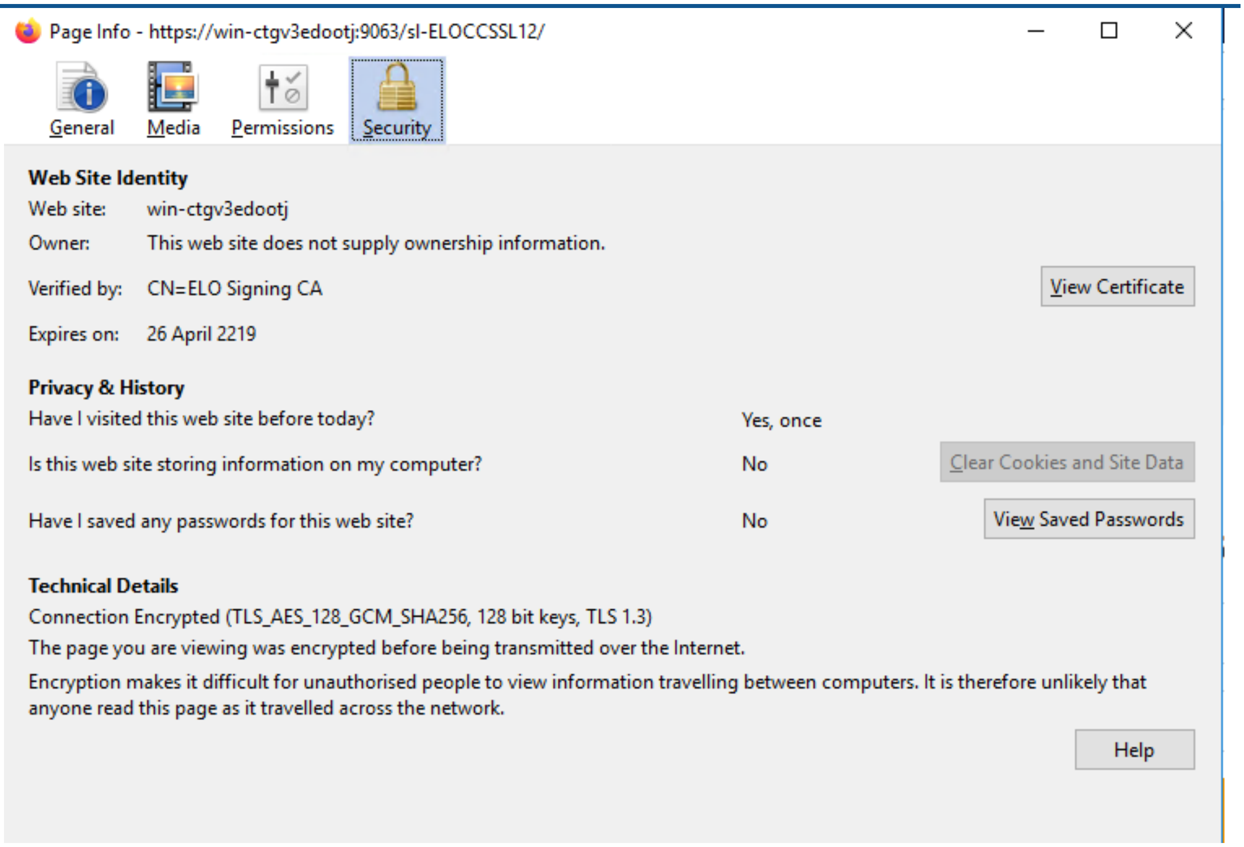

ELO Smart Link
https://win-ctgv3edootj:9063/sl-ELOCCSSL12/
ELO Smart Link
Connection Security for win-ctgv3edootj
You are not securely connected to this site.
You have added a security exception for this site.
Remove Exception
More Information

Fig.: Browser: More Information

2. In the connection details, now select *More Information*.


Page Info - https://win-ctgv3edootj:9063/sl-ELOCCSSL12/
General
Media
Permissions
Security
View Certificate
Clear Cookies and Site Data
View Saved Passwords
Help

Web Site Identity

Web site: win-ctgv3edootj

Owner: This web site does not supply ownership information.

Verified by: CN=ELO Signing CA

Expires on: 26 April 2219

Privacy & History

Have I visited this web site before today? Yes, once

Is this web site storing information on my computer? No

Have I saved any passwords for this web site? No

Technical Details

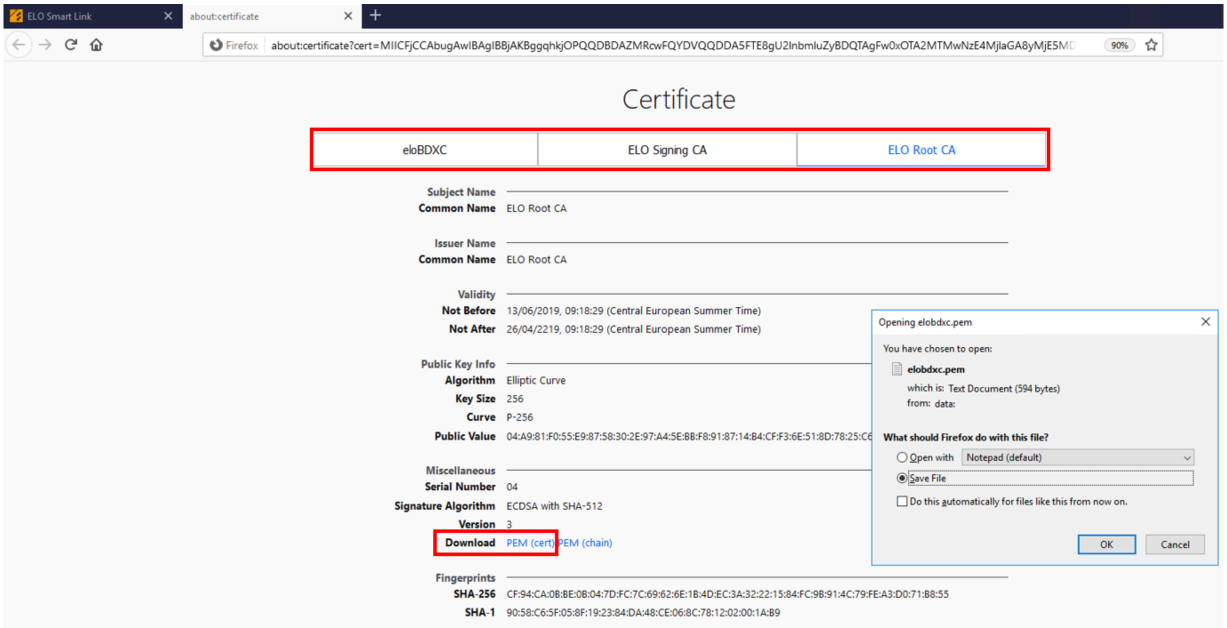
Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorised people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

Fig.: Web Site Identity

3. In the following window, select *Security* in the ribbon. Under *Web Site Identity*, click *View Certificate*.



about:certificate?cert=MIICFjCCAbugAwIBAgIBBjAKBggqhkjOPQQDBDAZMRcwFQYDVQQDDA5FTE8gU2lnbmluZyBDQTAgFw0xOTA2MTMwNzE4MjlaGA8yMjE5MD

Certificate

Subject Name
Common Name ELO Root CA

Issuer Name
Common Name ELO Root CA

Validity
Not Before 13/06/2019, 09:18:29 (Central European Summer Time)
Not After 26/04/2219, 09:18:29 (Central European Summer Time)

Public Key Info
Algorithm Elliptic Curve
Key Size 256
Curve P-256
Public Value 04:A9:81:F0:55:E9:87:58:30:2E:97:A4:5E:BB:F8:91:87:14:B4:CF:F3:6E:51:8D:78:25:C6

Miscellaneous
Serial Number 04
Signature Algorithm ECDSA with SHA-512
Version 3
Download PEM (cert) PEM (chain)

Fingerprints
SHA-256 CF:94:CA:0B:BE:0B:04:7D:FC:7C:69:62:6E:1B:4D:EC:3A:32:22:15:84:FC:9B:91:4C:79:FE:A3:D0:71:B8:55
SHA-1 90:58:C6:5F:05:8F:19:23:84:DA:48:CE:06:8C:78:12:02:00:1A:B9

Opening elobdxc.pem

You have chosen to open:
elobdxc.pem
which is: Text Document (594 bytes)
from: data:

What should Firefox do with this file?
○ Open with Notepad (default)
● Save File
□ Do this automatically for files like this from now on.

Fig.: Certificate view

4.

Export the entire certificate hierarchy. Select each of the certificates and export them separately. As the certificates have to be imported to the SAP system in the correct order, we recommend numbering the certificates when downloading them.

Certificate import

1. To import the certificates, open the transaction *STRUST* in the SAP system.

2. In the certificate store, select the *SSL Client (Standard)* folder.

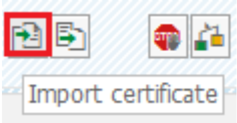
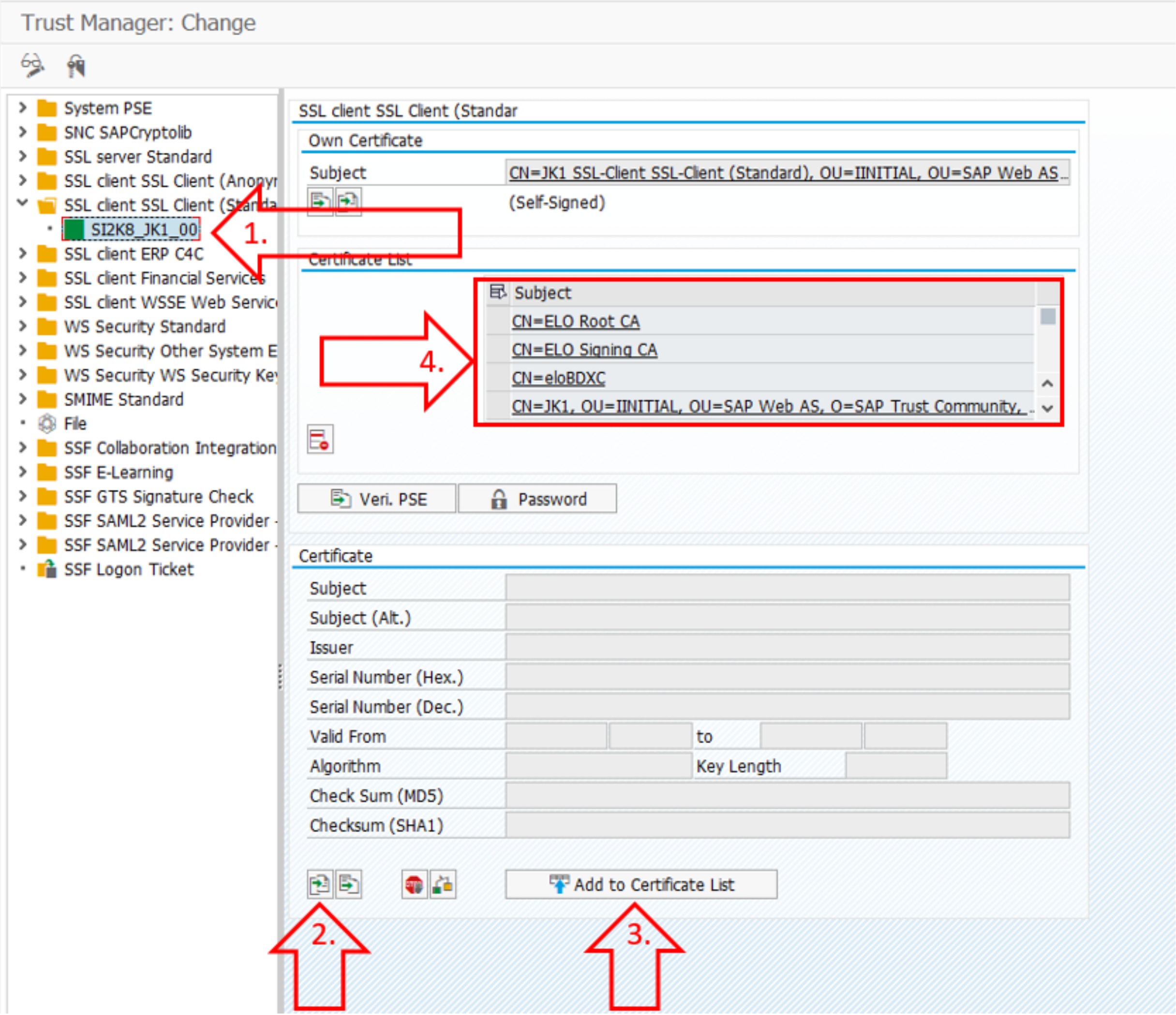


Fig.: Importing certificates


Trust Manager: Change
System PSE
SNC SAPCryptolib
SSL server Standard
SSL client SSL Client (Anonyı
SSL client SSL Client (Standa
SI2K8_JK1_00
SSL client ERP C4C
SSL client Financial Services
SSL client WSSE Web Servic
WS Security Standard
WS Security Other System E
WS Security WS Security Ke
SMIME Standard
File
SSF Collaboration Integration
SSF E-Learning
SSF GTS Signature Check
SSF SAML2 Service Provider -
SSF SAML2 Service Provider -
SSF Logon Ticket
1.
2.
3.
4.
Veri. PSE
Password
Add to Certificate List

SSL client SSL Client (Standar

Own Certificate

Subject CN=JK1 SSL-Client SSL-Client (Standard), OU=IINITIAL, OU=SAP Web AS

(Self-Signed)

Certificate List

Subject
CN=ELO Root CA
CN=ELO Signing CA
CN=eloBDXC
CN=JK1, OU=IINITIAL, OU=SAP Web AS, O=SAP Trust Community,

Certificate

Subject	
Subject (Alt.)	
Issuer	
Serial Number (Hex.)	
Serial Number (Dec.)	
Valid From	to
Algorithm	Key Length
Check Sum (MD5)	
Checksum (SHA1)	

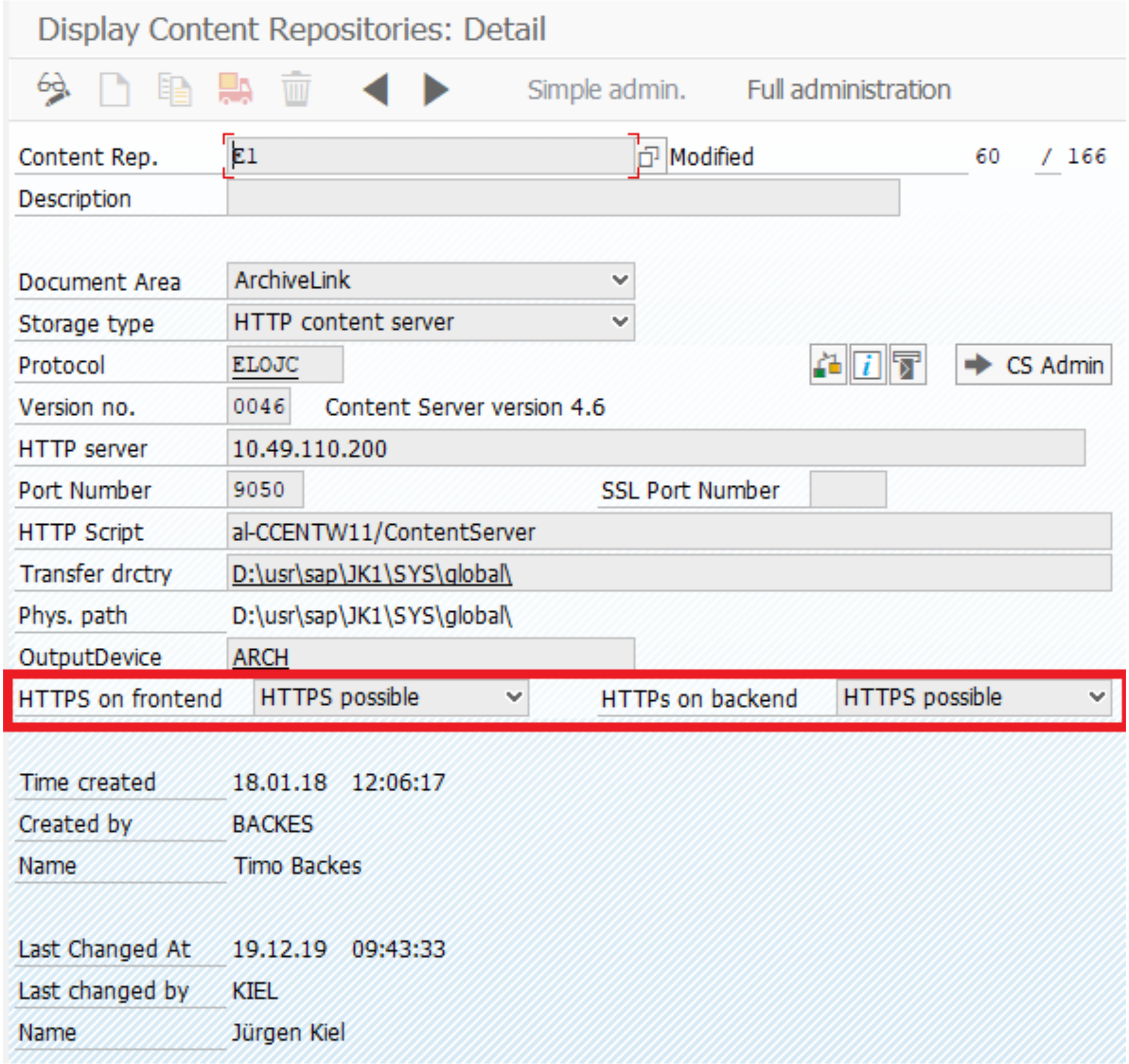
Fig.: Trust Manager in the SAP system

3. Click *Import certificate*, select the file path and exported certificates individually, then add each of these certificates to the certificate list by clicking *Add to Certificate List*.

Configuring the content repository

In the next step, the content repositories also have to be switched to HTTPS.

1. To do this, open transaction *OAC0*. This transaction contains another option for configuring an HTTPS connection.

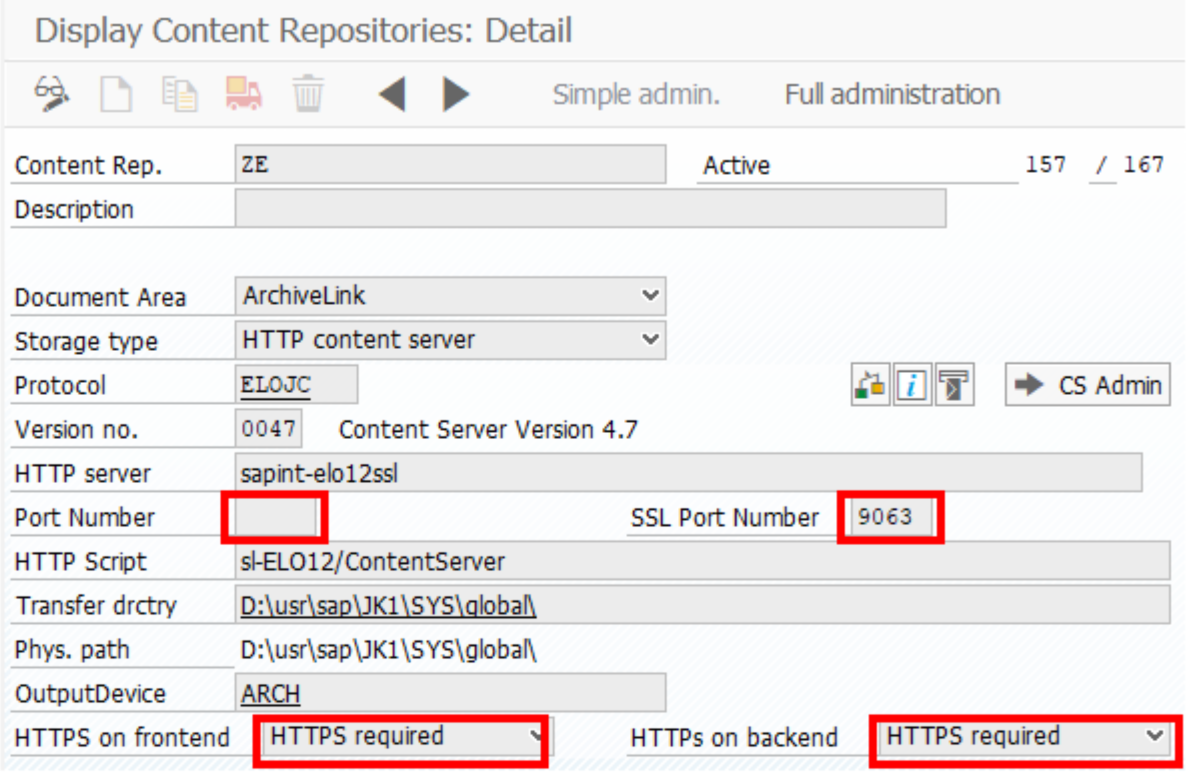


Display Content Repositories: Detail

Content Rep.	E1	Modified	60 / 166
Description			
Document Area	ArchiveLink		
Storage type	HTTP content server		
Protocol	ELOJC		
Version no.	0046	Content Server version 4.6	
HTTP server	10.49.110.200		
Port Number	9050	SSL Port Number	
HTTP Script	al-CCENTW11/ContentServer		
Transfer drctry	D:\usr\sap\JK1\SYS\global\		
Phys. path	D:\usr\sap\JK1\SYS\global\		
OutputDevice	ARCH		
HTTPS on frontend	HTTPS possible	HTTPs on backend	HTTPS possible
Time created	18.01.18 12:06:17		
Created by	BACKES		
Name	Timo Backes		
Last Changed At	19.12.19 09:43:33		
Last changed by	KIEL		
Name	Jürgen Kiel		

Fig.: Content repositories – HTTPS

2. In the command field/transaction field, enter %HTTPS and confirm with the ENTER key.



Content Rep.	ZE	Active	157 / 167
Description			
Document Area	ArchiveLink		
Storage type	HTTP content server		
Protocol	ELOJC		
Version no.	0047	Content Server Version 4.7	
HTTP server	sapint-elo12ssl		
Port Number		SSL Port Number	9063
HTTP Script	sl-ELO12/ContentServer		
Transfer drctry	D:\usr\sap\JK1\SYS\global\		
Phys. path	D:\usr\sap\JK1\SYS\global\		
OutputDevice	ARCH		
HTTPS on frontend	HTTPS required	HTTPs on backend	HTTPS required

Fig.: Connection settings

3. If you only want to communicate via HTTPS, make the following settings.

Port number	
SSL port number	9063
Frontend HTTPS	HTTPS required
Backend HTTPS	HTTPS required

The port entered here corresponds to the port selected in the ELO Smart Link for SAP® ERP installation.

> **Please note**
>
> The value entered to the *HTTP server* field must match the name in the certificate. For example, the IP address cannot be entered here if the certificate has been issued with a name.

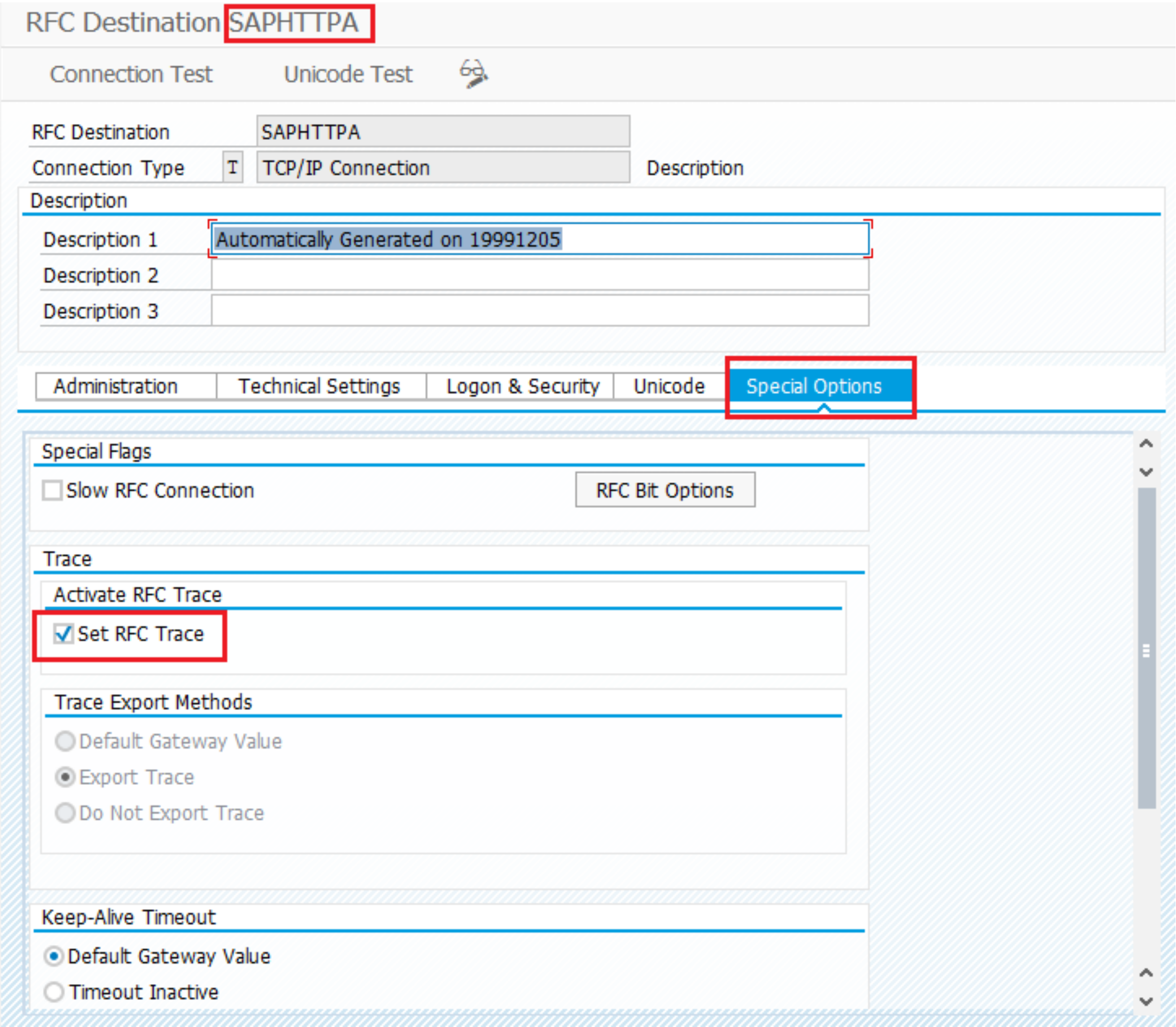
Once all settings have been applied, the SAP system and ELO now communicate exclusively via an HTTPS connection.

Troubleshooting

The HTTPS calls used by the SAP system are performed on the application server with a utility library. For this reason, you won't find any detailed log files for troubleshooting purposes. We therefore recommend configuring the following scenario to ensure logging and enable subsequent troubleshooting.

1. Call the transaction *SM59* and double-click the TCP/IP connection *SAPHTTPA* to select it.

2. The *Show/Change* button takes you to edit mode for the transaction.



RFC Destination SAPHTTPA

RFC Destination: SAPHTTPA

Connection Type: T TCP/IP Connection

Description

Description 1: Automatically Generated on 19991205

Description 2:

Description 3:

Special Flags

□ Slow RFC Connection

Trace

Activate RFC Trace

☑ Set RFC Trace

Trace Export Methods

○ Default Gateway Value

● Export Trace

○ Do Not Export Trace

Keep-Alive Timeout

● Default Gateway Value

○ Timeout Inactive

Fig.: RFC Destination SAPHTTPA

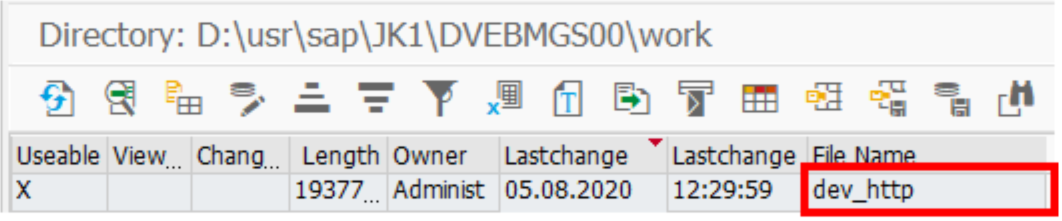
3. Switch to the *Special Options* tab and check the box next to *Set RFC Trace* in the *Trace* area.

4. Now, save the settings.

5.

Next, you want to perform a call (connection) between the SAP system and ELO. For example, you can perform a connection test with a configured content repository in transaction *OAC0*.

6. Call the transaction *AL11*.



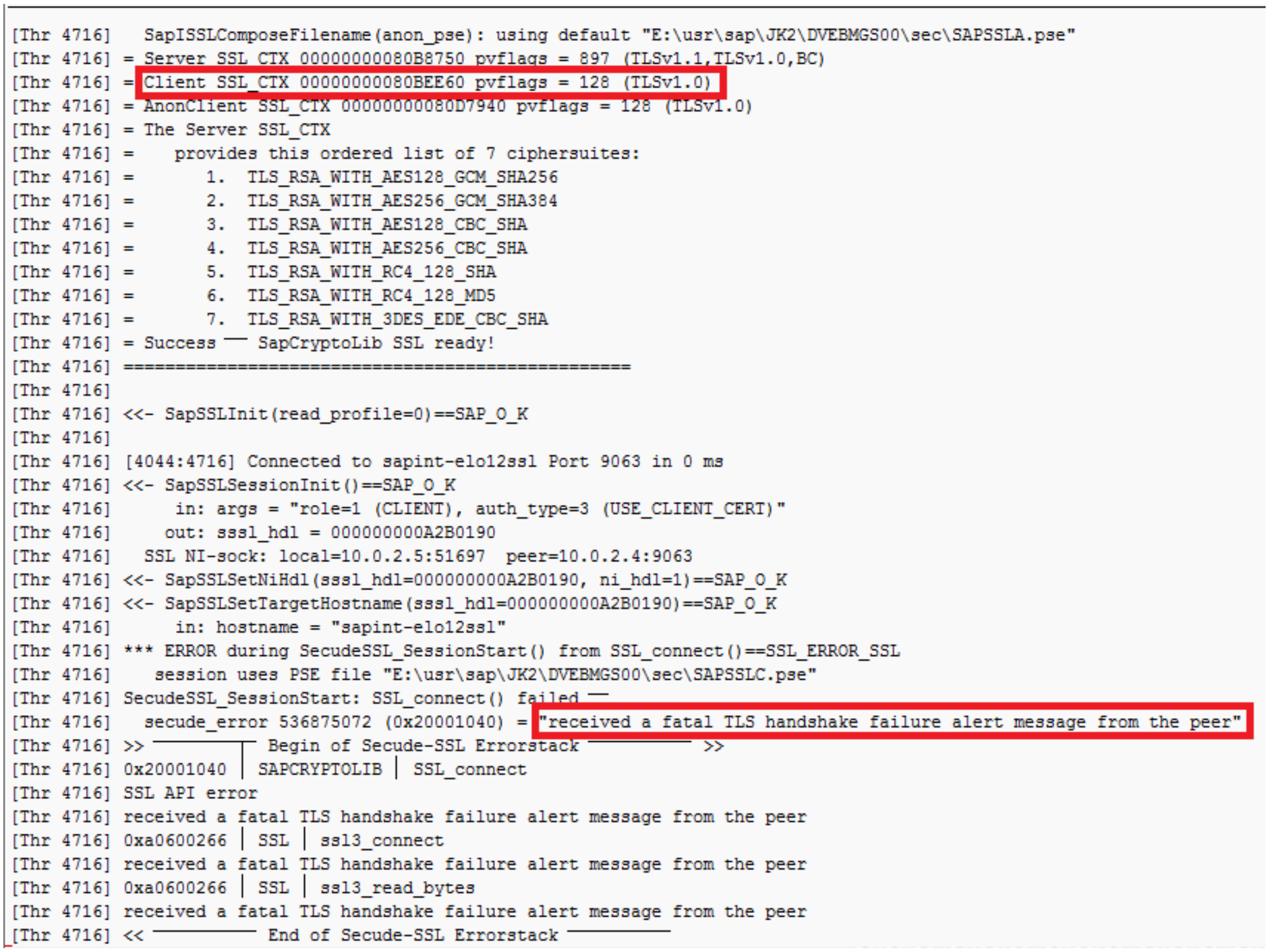
Directory: D:\usr\sap\JK1\DVEBMGS00\work

Useable	View...	Chang...	Length	Owner	Lastchange	Lastchange	File Name
X			19377...	Administ	05.08.2020	12:29:59	dev_http

Fig.: Work directory

7. Double-click the entry *DIR_HOME* in the list to select it (work directory). In this directory, you should now find a file named *dev_http*.

8. You can analyze any possible errors within this file.



```
[Thr 4716]   SapISSLComposeFilename(anon_pse): using default "E:\usr\sap\JK2\DVEBMGS00\sec\SAPSSLA.pse"
[Thr 4716] = Server SSL_CTX 0000000080B8750 pvflags = 897 (TLSv1.1,TLSv1.0,BC)
[Thr 4716] = Client SSL_CTX 0000000080BEE60 pvflags = 128 (TLSv1.0)
[Thr 4716] = AnonClient SSL_CTX 00000000080D7940 pvflags = 128 (TLSv1.0)
[Thr 4716] = The Server SSL_CTX
[Thr 4716] =    provides this ordered list of 7 ciphersuites:
[Thr 4716] =        1.  TLS_RSA_WITH_AES128_GCM_SHA256
[Thr 4716] =        2.  TLS_RSA_WITH_AES256_GCM_SHA384
[Thr 4716] =        3.  TLS_RSA_WITH_AES128_CBC_SHA
[Thr 4716] =        4.  TLS_RSA_WITH_AES256_CBC_SHA
[Thr 4716] =        5.  TLS_RSA_WITH_RC4_128_SHA
[Thr 4716] =        6.  TLS_RSA_WITH_RC4_128_MD5
[Thr 4716] =        7.  TLS_RSA_WITH_3DES_EDE_CBC_SHA
[Thr 4716] = Success —— SapCryptoLib SSL ready!
[Thr 4716] =================================================
[Thr 4716]
[Thr 4716] <<- SapSSLInit(read_profile=0)==SAP_O_K
[Thr 4716]
[Thr 4716] [4044:4716] Connected to sapint-elo12ssl Port 9063 in 0 ms
[Thr 4716] <<- SapSSLSessionInit()==SAP_O_K
[Thr 4716]      in: args = "role=1 (CLIENT), auth_type=3 (USE_CLIENT_CERT)"
[Thr 4716]     out: sssl_hdl = 000000000A2B0190
[Thr 4716]   SSL NI-sock: local=10.0.2.5:51697  peer=10.0.2.4:9063
[Thr 4716] <<- SapSSLSetNiHdl(sssl_hdl=000000000A2B0190, ni_hdl=1)==SAP_O_K
[Thr 4716] <<- SapSSLSetTargetHostname(sssl_hdl=000000000A2B0190)==SAP_O_K
[Thr 4716]      in: hostname = "sapint-elo12ssl"
[Thr 4716] *** ERROR during SecudeSSL_SessionStart() from SSL_connect()==SSL_ERROR_SSL
[Thr 4716]    session uses PSE file "E:\usr\sap\JK2\DVEBMGS00\sec\SAPSSLC.pse"
[Thr 4716] SecudeSSL_SessionStart: SSL_connect() failed ——
[Thr 4716]   secude_error 536875072 (0x20001040) = "received a fatal TLS handshake failure alert message from the peer"
[Thr 4716] >> ─────────┬ Begin of Secude-SSL Errorstack ──────────── >>
[Thr 4716] 0x20001040 │ SAPCRYPTOLIB │ SSL_connect
[Thr 4716] SSL API error
[Thr 4716] received a fatal TLS handshake failure alert message from the peer
[Thr 4716] 0xa0600266 │ SSL │ ssl3_connect
[Thr 4716] received a fatal TLS handshake failure alert message from the peer
[Thr 4716] 0xa0600266 │ SSL │ ssl3_read_bytes
[Thr 4716] received a fatal TLS handshake failure alert message from the peer
[Thr 4716] << ────────── End of Secude-SSL Errorstack ──────────
```

Fig.: Example error

As an example, we entered an incorrect configuration and performed a connection test. In this case, the client cipher suite only accepts TLS version 1.0.