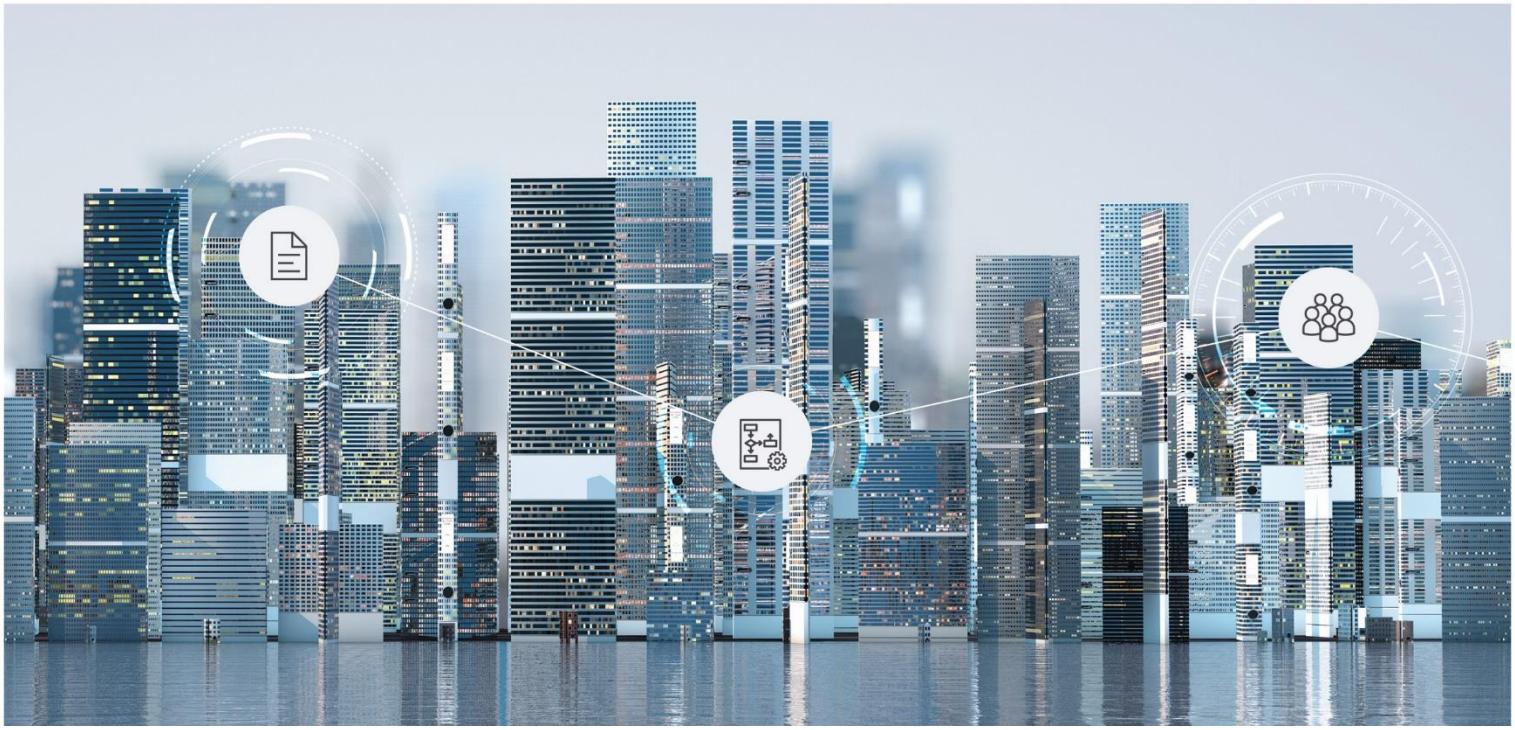
Fabasoft



White Paper

Configuration of TLS for Fabasoft Services

Fabasoft Folio 2021 Update Rollup 2

Contents

1 Introduction ____ **4**

2 Software Requirements ____ **4**

3 Configuration ____ **4**

3.1 Environment Variable “TLSDIR” 4

3.2 Configuration Files “hostkey.pem” and “hosttrusts.cfg” 6

3.3 Configuration Utility “fsckeygen” 7

3.4 Reference Configuration Using openssl 7

3.5 Using Multiple Hosts 7

1 Introduction

This white paper describes how to use and configure the secure socket layer (SSL) for Fabasoft Services.

2 Software Requirements

System environment: All information contained in this document implicitly assumes a Microsoft Windows environment or Linux environment.

Supported platforms: For detailed information on supported operating systems and software, see the software product information on the Fabasoft distribution media.

3 Configuration

Fabasoft Folio uses socket connections to connect backend services and frontend clients.

The socket communication used between frontend and backend services may be encrypted and authenticated using SSL/TLS encryption.

Clients and server processes use certificate fingerprints to identify trusted peers. The default implementation uses keys and trusts per host. Every host acting as part of a Fabasoft installation has to have a key and the correct trusts to identify services and clients.

3.1 Environment Variable "TLSDIR"

To enable encryption and authentication, the environment variable `TLSDIR` is used. This variable is configured as other environment variables used to configure the socket connection (e.g. `HOST`, `PORT`) for Fabasoft Services.

Once the variable is configured for a service or client process, the referenced directory and the required files must exist, otherwise the service or client will fail to work and report errors.

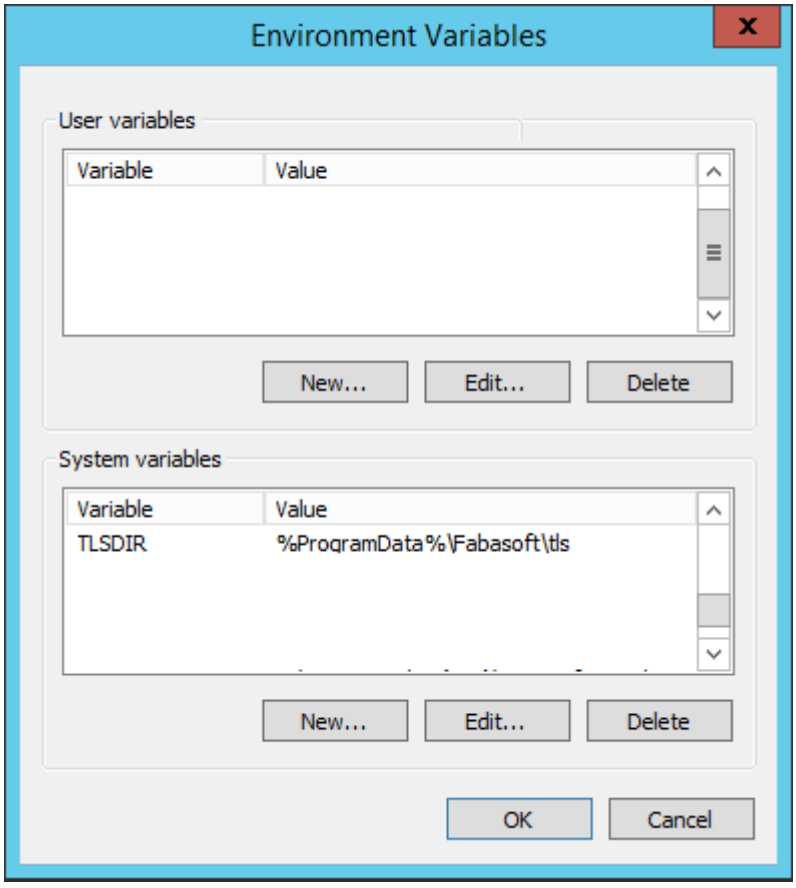
If the variable is added or changed, all services have to be restarted.

Default value of TLSDIR on Microsoft Windows

```
C:\>set TLSDIR=%ProgramData%\Fabasoft\TLS
C:\>set TLSDIR

TLSDIR=C:\ProgramData\Fabasoft\TLS
```

To set the variable for Microsoft Windows, add the environment variable in the system properties as system variable.

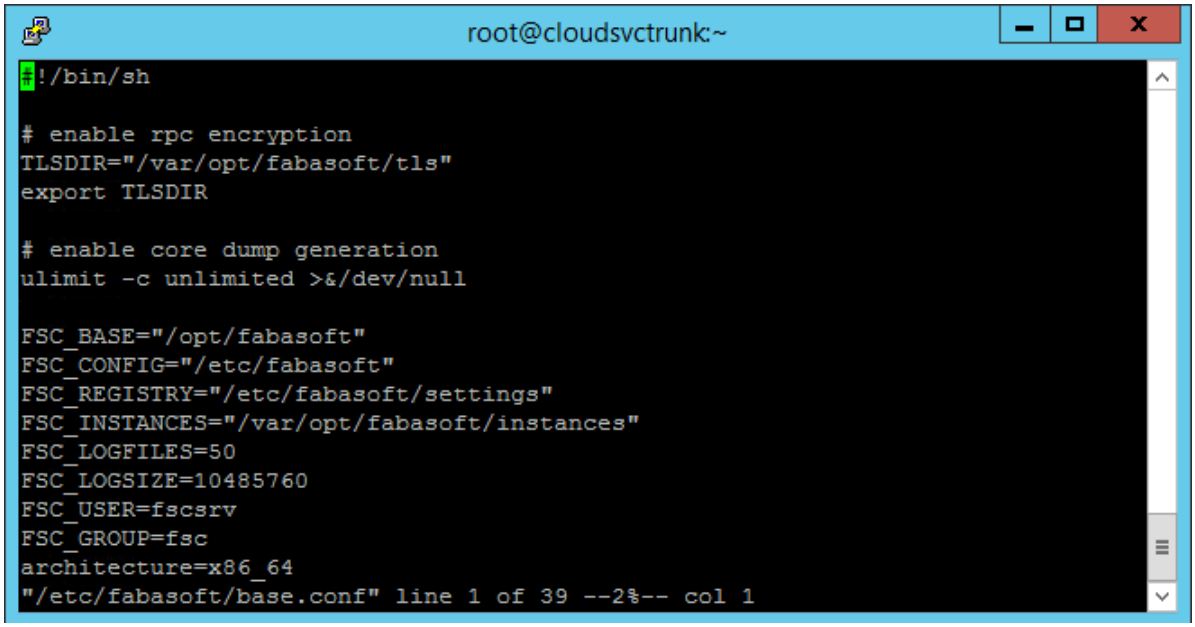


Default value of TLSDIR on Linux

```
$ export TLSDIR="/var/opt/fabasoft/tls"
$ echo $TLSDIR

/var/opt/fabasoft/tls
```

To set the variable for Linux, add the entry to the file /etc/fabasoft/base.conf.



3.2 Configuration Files “hostkey.pem” and “hosttrusts.cfg”

Once the `TLSDIR` is set it must point to a directory containing a key and a trusts file per host.

hostkey.pem

This file contains the certificate and private key and is used to authenticate the peer (client or server) of a SSL/TLS protected socket connection.

Sample file hostkey.pem

```
-----BEGIN CERTIFICATE-----
MIIEqTCCApGgAwIBAgIBATANBgkqhkiG9w0BAQsFADAYMRYwFAYDVQQDDA1FTkdC
VUlMRFZNMjI4MB4XDTE4MDgwOTE2MDA1NVoXDTQ1MTIyNDE2MDA1NVowGDEWMBQG
[…]
-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQDToM8SofUEgNyZ
EaMsLFoFD+9JO9PSgcgR984e4EMQno63Me4Zw6L42YV04nesaL4IC/KKZmVWLWSR
[…]
-----END PRIVATE KEY-----
```

hosttrusts.cfg

This file contains fingerprints (SHA-256) of accepted peer certificates.

Sample file hosttrusts.cfg

```
# Trusted host certificates (sha256 fingerprint).
c0:88:b5:5a:d0:1d:8a:46:ed:78:5b:fd:2d:d4:89:9a:75:a7:e8:37:a7:22:3a:bf:c4:4c:99:
49:24:6d:b0:67 # hostname
```

Text following a # is ignored and empty lines are ignored, too.

3.3 Configuration Utility “fsckeygen”

To create new certificates, the utility `fsckeygen` may be used. The utility will create the files `hostkey.pem` (new certificate and key) and `hosttrusts.cfg` (fingerprint of the newly created certificate).

Any existing fingerprints of trusted peer certificates must be added manually.

Sample use of fsckeygen on Microsoft Windows

```
C:\>where fsckeygen
C:\Program Files\Fabasoft\Components\Management\fsckeygen.exe

C:\>set TLSDIR
TLSDIR=C:\ProgramData\Fabasoft\TLS

C:\>fsckeygen
Fabasoft Folio fsckeygen Version 18.3.0.0
Copyright (c) Fabasoft R&D GmbH, A-4020 Linz, 1988-2018.
Files exist, use option -f to overwrite.
Usage: fsckeygen [-q] [-f] [-d tlsdir]

C:\>fsckeygen -f
Fabasoft Folio fsckeygen Version 18.3.0.0
Copyright (c) Fabasoft R&D GmbH, A-4020 Linz, 1988-2018.
File C:\ProgramData\Fabasoft\TLS\hostkey.pem written.
File C:\ProgramData\Fabasoft\TLS\hosttrusts.cfg written.
```

3.4 Reference Configuration Using openssl

As reference the corresponding `openssl` commands are listed.

Reference bash commands to generate host key and trusts

```
HOSTNAME=$(hostname -s)
NEWCERTARGS="req -newkey rsa:4096 -days 9999 -nodes -x509 -subj /CN=$HOSTNAME"
FINGERPRINTARGS="x509 -noout -fingerprint -sha256"

openssl $NEWCERTARGS -keyout key.pem -out cert.pem
openssl $FINGERPRINTARGS -in cert.pem | sed 's/.*=//' | tr A-F a-f > certfp.cfg

#
# Host Key
#
cat cert.pem key.pem > hostkey.pem

#
# Host Trusts
#
echo "# Trusted host certificates (SHA-256 fingerprint)." > hosttrusts.cfg
echo "$(cat certfp.cfg) # $HOSTNAME"                     >> hosttrusts.cfg

rm cert.pem key.pem certfp.cfg
```

3.5 Using Multiple Hosts

A typical installation of Fabasoft Services uses multiple hosts.

To enable this scenario, the host key and host trust files may be copied to all connected machines or the host trust files of all connected machines have to be edited manually to contain all fingerprints of trusted host certificates.