DOCUMENTS

LDAPS (LDAP OVER TLS)

DOCUMENTS 5.0e

Table of contents

1. Requirements

From version 5.0d HF1 (#2065) DOCUMENTS supports LDAP OVER SSL.

The first prerequisite is that LDAP OVER SLL has been activated on the AD server and that an LDAP connection can be established via TLS/SSL. This can be checked on the AD via the command line with the program "ldp":

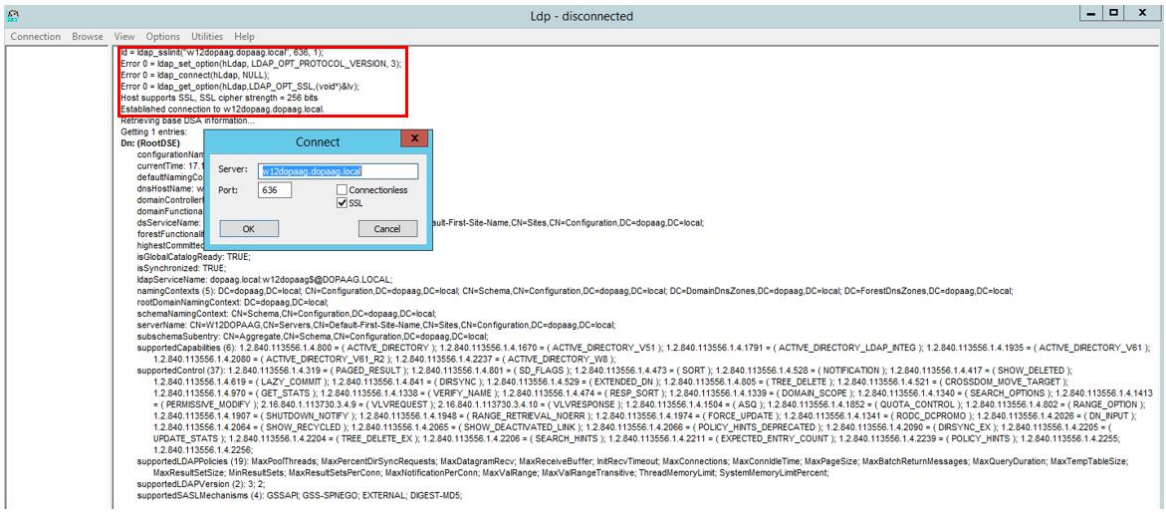

Figure 1: ldp -> connect -> SSL

A successful SSL connection setup is logged accordingly.

It is also assumed that you are familiar with setting up and configuring the LDAP job on standard port 389 (unencrypted) (e.g. using the LDAP Configuration Wizard in the DOCUMENTS Manager).

In the following, only those points are listed where there are deviations from the LDAP standard configuration:

- Generation of the necessary PEM certificate file for the TLS/SSL connection between the DOCUMENTS server and the AD (LDAPS).
- Testing the Connection Parameters and Configuring the DOCUMENTS Server to Use TLS/SSL

2. Certificate chain of the AD server

In the following, a "certificate" file in PEM format for the DOCUMENTS server is generated from the SSL certificate of the AD server.

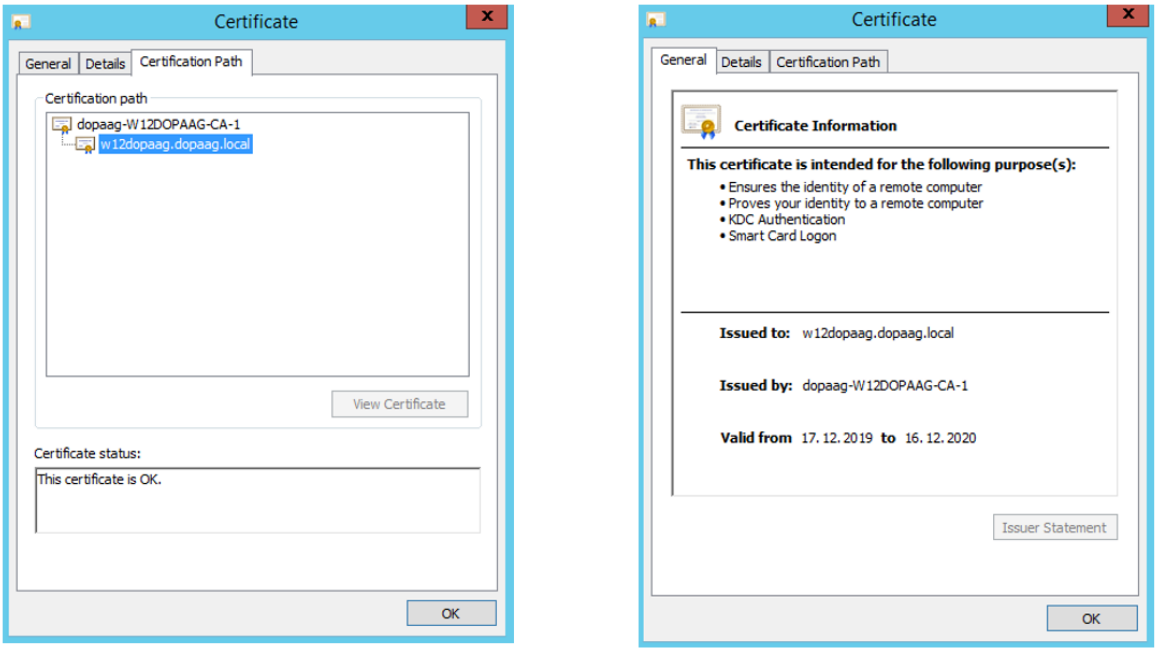

Figure 2: SSL – Certificate LDAP-Servers

The figure above shows the SSL certificate of the AD machine named "w12dopaag". The certificate was issued by the CA "CA-1". To verify the connection, the DOCUMENTS server only needs the root CA, which is exported below.

Important note
Only the top certificate (CA-1) must be exported.

Based on the certificate, a "PEM certificate" file is created in a few steps, which must then be stored on the DOCUMENTS server.

1) The certificate at the end of the certificate chain and possible intermediate certificates do not have to be considered further.

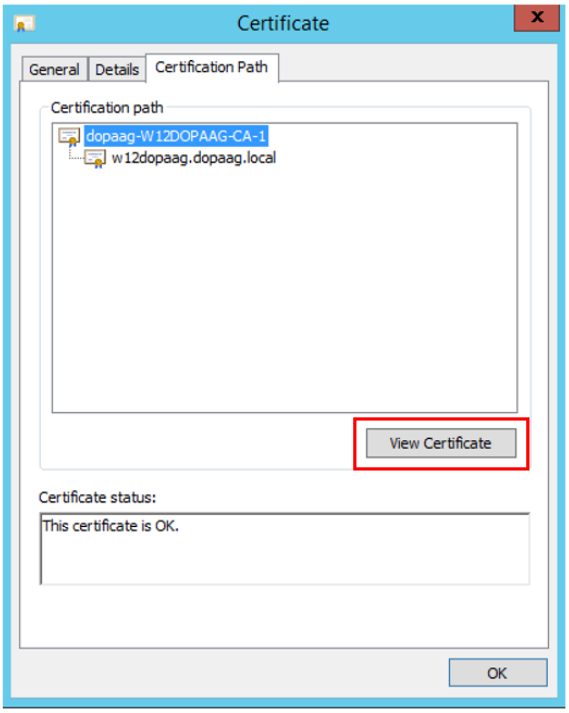

Figure 3: Select and view root certificate

2) On the detail dialog for the certificate "CA-1" a certificate export can now be initiated via the button "Copy to file".

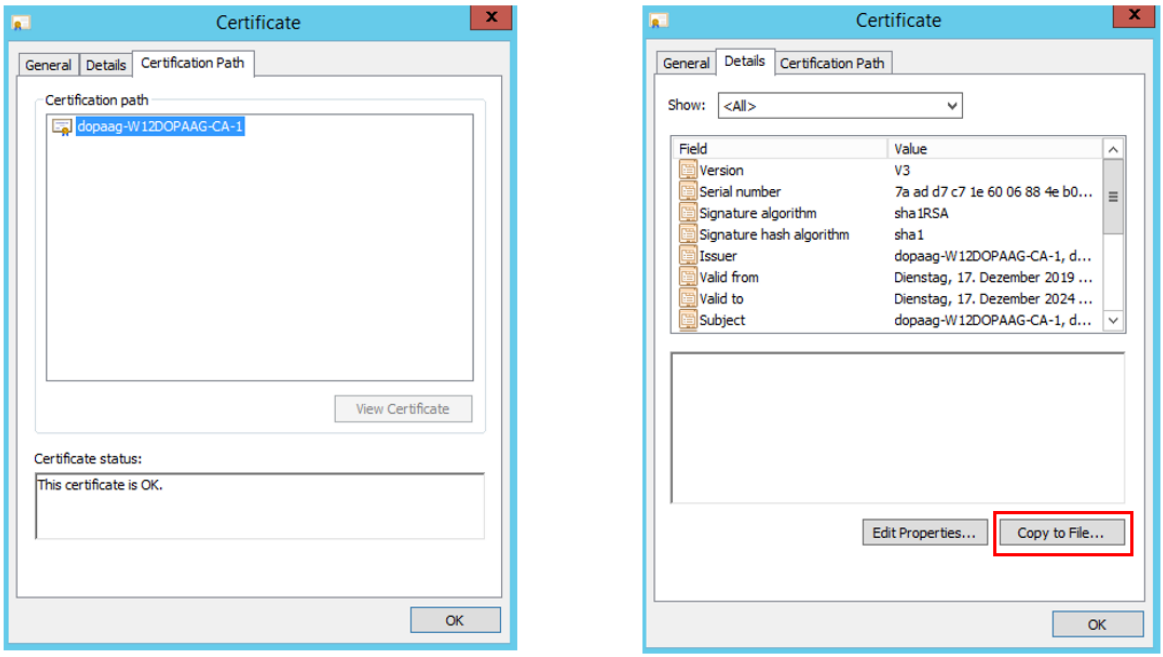

Figure 4: Start a certificate export on the opened root certificate

3) Export the certificate "Base 64 encodes X.509 (.CER)" e.g. to the file "adroot.cer".

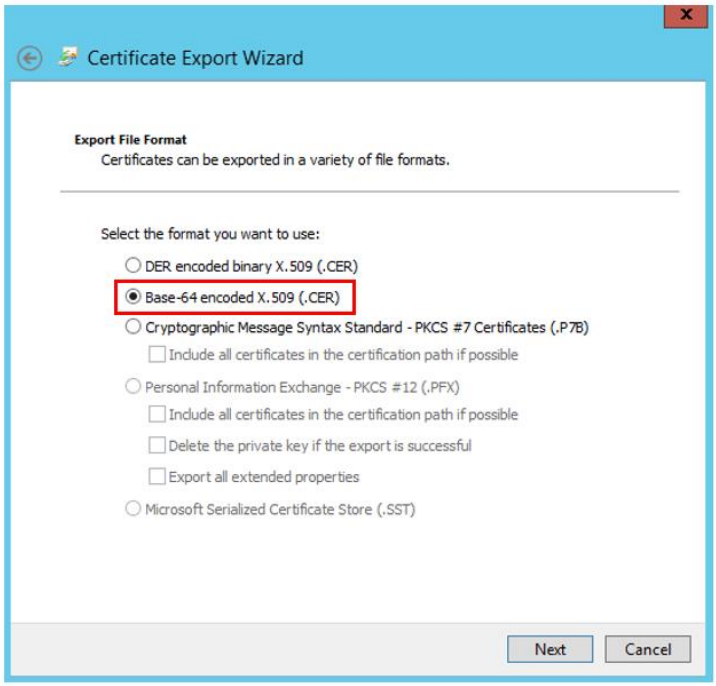

Figure 5: Initiate base-64-encoded certificate export

4) Rename the file adroot.cer to adroot.pem (the base-64 encoded X.509 (.CER) format corresponds to the PEM format).

The adroot.pem must then be made available to the DOCUMENTS server so that it can access it, for example by storing it in the server directory.

Note
A correctly configured LDAPS server implicitly delivers possible intermediate certificates during TLS/SSL handshake. If this does not happen due to incorrect configuration, additional intermediate certificates can be added to the pem file.

3. DOCUMENTS-LDAPS-configuration

First, the test script "otrTestLdapConnection.xml" must be imported. The file is delivered with the test script and is located in the directory "\server\scriptlibs\Ldap\".

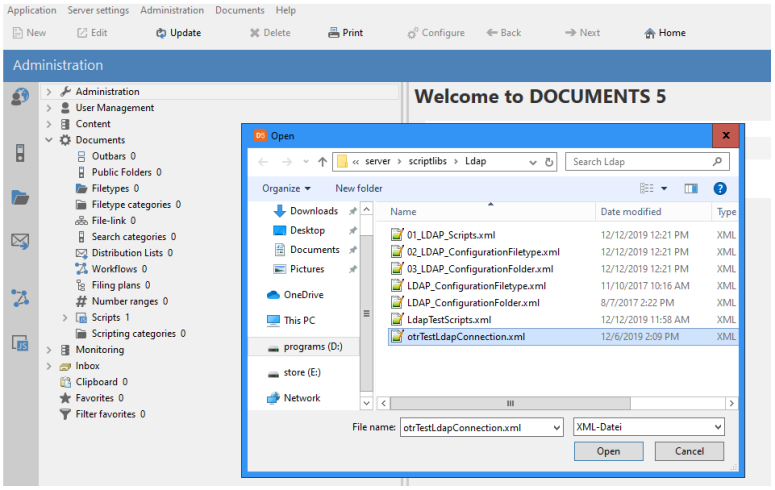

Figure 6: XML-Import openLdapSSLConnection.xml

The connection data must then be configured as script parameters and the script executed. (Please do not make any changes to the script source code, as it is signed and can therefore be executed without a scripting license).

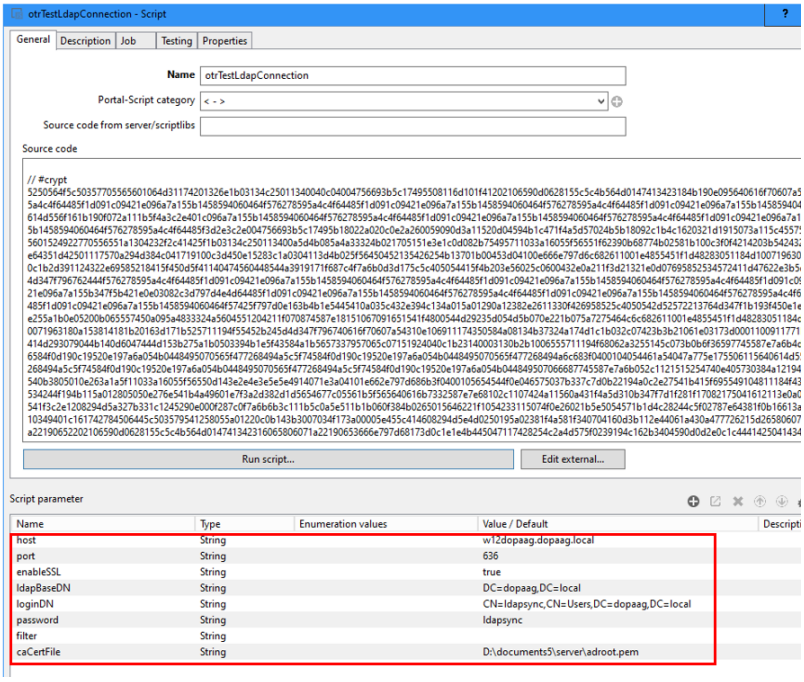

Figure 7: Connection data for SSL access

If the connection could be opened, the following message is displayed in the server window and on the client:

```
Connection established with [Domain-Name]
```

If the connection cannot be established, the error message is displayed that was passed on to the server from the openLdap interface.

Note
If changes have been made to the caCertFile, it may be necessary to restart the DOCUMENTS server because the openLdap interface caches the certificates.

If the connection test was successful, the SSL-specific parameters for the LDAP job and the LDAP logon must also be adapted as properties for the client or optionally in the script "LdapParamDomain".

If the configuration was carried out using the LDAP Wizard in the DOCUMENTS Manager, we recommend that you set the properties LdapPort, LdapEnableSSL and LdapCaCertFile for the client (in future versions of DOCUMENTS, this configuration can be carried out in the LDAP Wizard).

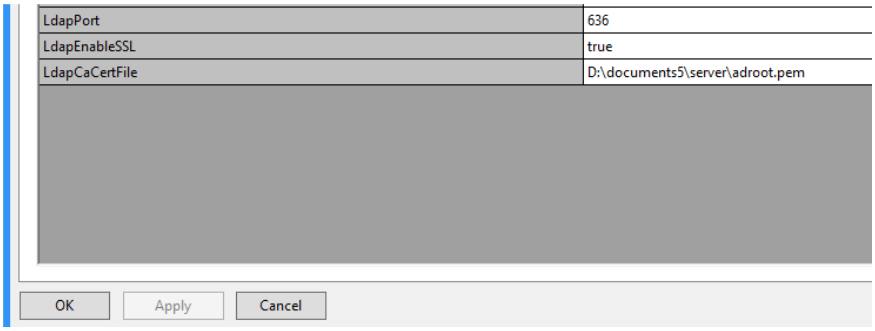

Figure 8: LDAP-SSL settings at principal

Optionally the configuration can be made in the script "server\scriptlibs\Ldap\LdapParamDomain.js" (e.g. if several LDAPS servers have to be addressed) or if the LDAP scripts were imported into the DOCUMENTS Manager (XML import: 01_LDAP_Scripts.xml), then the configuration in the DOCUMENTS Manager must be made in the PortalScript "LdapParamDomain".

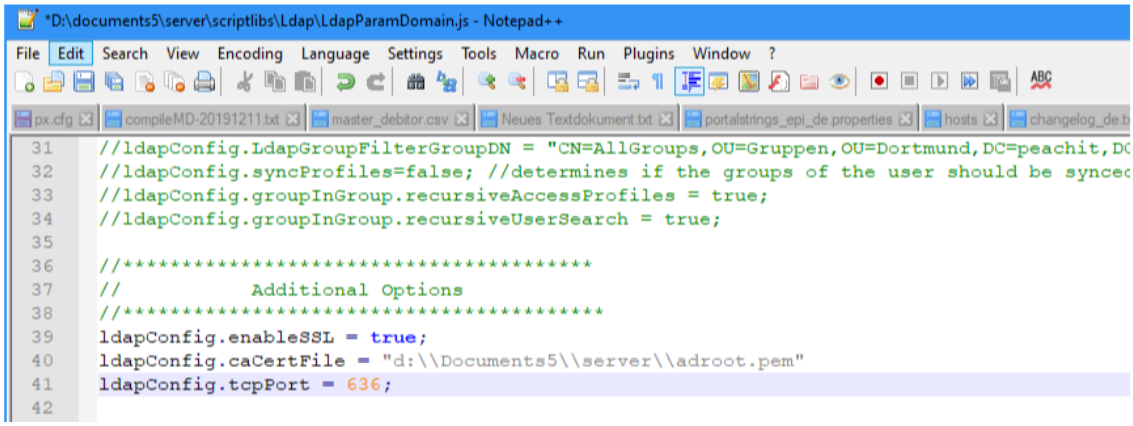

Figure 9: LdapParamDomain" script with the SSL parameters "enableSSL, tcpPort, caCertFile"

Table of figures