

### LDAPS-KOPPLUNG (LDAP OVER TLS)

DOCUMENTS 5.0e

© Copyright 2019 otris software AG. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch die otris software AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Alle in dieser Publikation aufgeführten Wort- und Bildmarken sind Eigentum der entsprechenden Hersteller.

Änderungen in der Software sind vorbehalten. Die in diesem Handbuch enthaltenen Informationen stellen keinerlei Verpflichtung seitens des Verkäufers dar.

### Inhaltsverzeichnis

1.	Voraussetzungen	.4
2.	Zertifikatskette des AD LDS	.5
3.	DOCUMENTS-LDAPS-Konfiguration	.8
Abbildung	sverzeichnis1	10

## 1. Voraussetzungen

#### DOCUMENTS unterstützt ab der Version 5.0d HF1 (#2065) LDAP OVER SSL.

Vorausgesetzt wird zunächst, dass auf dem AD LDS Server LDAP OVER SLL aktiviert wurde und dass eine LDAP-Connection über TLS/SSL hergestellt werden kann. Dies kann auf dem AD über die Kommandozeile mit dem Programm "Idp" überprüft werden:



Abb. 1: Über Idp -> Verbinden -> SSL

Ein erfolgreicher SSL-Verbindungsaufbau wird entsprechend protokolliert.

Weiter wird vorausgesetzt, dass man mit dem Einrichten und Konfigurieren des LDAP-Jobs auf dem Standardport 389 (unverschlüsselt) vertraut ist (z.B. über den LDAP Konfigurations-Wizard im DOCUMENTS Manager oder über den Konfigurationsmappentypen).

Im Folgenden werden nur die Punkte aufgeführt bei denen es zu Abweichungen zur LDAP-Standardkonfiguration kommt:

- Erzeugung der notwendigen PEM-Zertifikatsdatei für die TLS/SSL Verbindung zwischen dem DOCUMENTS Server und dem AD LDS
- Testen der Verbindungsparameter und Konfiguration des DOCUMENTS Server zur Verwendung von TLS/SSL

### 2. Zertifikatskette des AD LDS

Im Folgenden wird ausgehend vom SSL-Zertifikat des AD LDS Servers eine "Zertifikats"-Datei im PEM-Format für den DOCUMENTS-Server erzeugt.

Zertifikat	z Zertifikat 🗴
Allgemein Details Zertifizierungspfad	Allgemein Details Zertifizierungspfad
Zertifizierungspfad	Zertifikatsinformationen
국 3-AD-Server	Dieses Zertifikat ist für folgende Zwecke beabsichtigt: • Garantiert dem Remotecomputer Ihre Identität • Garantiert die Identität eines Remotecomputers
	Ausgestellt für: 3-AD-Server
Zertifikat anzeigen	Ausgestellt von: 2-Zwischen-CA
	Gültig ab 25.07.2019 bis 24.07.2020
Zertifizierungsstatus: Dieses Zertifikat ist gültig.	💡 Sie besitzen einen privaten Schlüssel für dieses Zertifikat.
<u> </u>	Ausstellererklärung
ОК	ОК

Abb. 2: SSL - Zertifikat des LDAP-Servers

In der Abbildung oben wird das SSL-Zertifikat des AD-Rechners mit dem Namen "3-AD-Server" gezeigt. Ausgestellt wurde das Zertifikat von der CA "2-Zwischen-CA", die ihrerseits durch "1-Root-CA" zertifiziert wurde. Der DOCUMENTS Server benötigt zur Verifikation der Verbindung nur das Root-CA, welches im Folgenden exportiert wird.

#### Wichtiger Hinweis

Es muss ausschließlich das oberste Zertifikat (1-Root-CA) exportiert werden.

Anhand des Zertifikates wird in wenigen Schritten eine "PEM-Zertifikats"-Datei erstellt, die dann auf dem DOCUMENTS-Server hinterlegt werden muss.

1) Das Zertifikat "3–AD-Server" am Ende der Zertifikatskette und mögliche Zwischenzertifikate (hier "2-Zwischen-CA") müssen nicht weiter beachtet werden.

Zertifikat X
Allgemein Details Zertifizierungspfad
Zertifizierungspfad
1-Root-CA
Zertifikat anzeigen
Zertifizierungsstatus:
Dieses Zertifikat ist gültig.
OK

Abb. 3: Das Root-Zertifikat auswählen und anzeigen.

2) Auf dem Detaildialog für das Zertifikat "1-Root-CA" kann nun über den Button "In Datei kopieren" ein Zertifikatsexport angestoßen werden.

Zertifikat X	z Zertifikat X
Zertifikat       Allgemein       Details       Zertifizierungspfad       Incontended       Incontended    <	Zertifikat       X         Allgemein       Details       Zertifizierungspfad         Anzeigen:        ×         Feld       Wert       ^         Öffentlicher Schlüssel       RSA (2048 Bits)       ×         ØZertifikatvorlagenname       CA       ×         ØSchlüsselkennung des Antra       2e fe 39 43 e6 d4 4d 00 of 94       ×         ØVersion der Zertifizierungsst       V0.0       Schlüsselverwendung       Digitale Signatur, Zertifikatsign       =         ØRasiseinschränkungen       Typ des Antragstellers=Zertifi       =       =       Fingerabdruckalgorithmus       sha1       =         ØFingerabdruck       6f 24 05 6a 0f b3 3c 46 35 6a       ×
Zertifizierungsstatus: Dieses Zertifikat ist gültig. OK	Eigenschaften bearbeiten In Datei kopieren

Abb. 4: Auf dem geöffneten Root-Zertifikat einen Zertifikatsexport starten.

3) Das Zertifikat "Base 64 codiert X.509 (.CER)" z.B. in die Datei "adroot.cer" exportieren.



Abb. 5: Zertifikatsexport Base-64-codiert veranlassen.

4) Die Datei adroot.cer in adroot.pem umbenennen (das Base-64-codiert X.509 (.CER) Format entspricht dem PEM-Format).

Die adroot.pem muss dann dem DOCUMENTS -Server so zur Verfügung gestellt werden, dass dieser darauf zugreifen kann, indem man sie beispielsweise im Serververzeichnis ablegt.

#### Hinweis

Ein korrekt konfigurierter LDAPS – Server liefert mögliche Zwischenzertifikate beim TLS/SSL-Handshake implizit aus. Falls durch fehlerhafte Konfiguration dies nicht erfolgt, können in der pem-Datei weitere Zwischenzertifikate miteingefügt werden.

### 3. DOCUMENTS-LDAPS-Konfiguration

Zur Prüfung Zunächst muss das Testskript "otrTestLdapConnection.xml" importiert werden. Die Datei wird mit ausgeliefert und befindet sich im Verzeichnis "\server\scriptlibs\Ldap\".

nwendu	ng Servereinstellungen Administration	ocuments Hilfe	
🍃 Neu	serverseitiger Datenexport (jex) XML-Export	öschen 📇 Drucken 🧬 Anpassen 🗲 Zurück -> Vorwärts 🏠 Startseite	
Mapp	e XML-Import	D Öffnen Jc ◯◯ ♥ 📜 « Documents5 → server → scriptlibs → Ldap 💌 4→ Ldap dur	rchsuchen
	Server-Logs herunterladen	a Organisieren   Neuer Ordner	i≕ <b>-</b> [] @
8	Outbars 0	🖫 Zuletzt besucht 🔹 Name 🏠 Änderungsdatu	m Typ
	öffentliche Ordner 0 Mappentypen 0	☐ 01_LDAP_Scripts          18:10.2018 15:59                 ☐ 02_LDAP_ConfigurationFiletype          07.06.2018 15:54	XML-Dokument XML-Dokument
	📄 Mappentyp-Kategorien 0 🟯 Mappenverknüpfung 0	■ Bilder         ⊡ 03_LDAP_ConfigurationFolder         07.06.2018 15:54           ■ Dokumente         □ Ldap TestScripts         18.10.2018 15:59	XML-Dokument XML-Dokument
	Suchkategorien 0 Suchkategorien 0	Independent of the second secon	XML-Dokument
7	ぷ Workflows 0 寝 Aktenpläne 0 # Nummernkreise 0	: Computer	
.JS	<ul> <li>Scripte 1</li> <li>Scripting-Kategorien 1</li> </ul>	Netzwerk	
	<ul> <li>Impanding</li> <li>Impanding</li> <li>Impanding</li> </ul>	Dateiname: otrTestLdapConnection	i –
	🔁 Textablage 0 ★ Favoriten 0	Öffner	Abbrechen

Abb. 6: XML-Import der openLdapSSLConnection.xml

Anschließend müssen die Verbindungsdaten als Script-Parameter konfiguriert und das Skript ausgeführt werden. (Bitte keine Änderungen am Script-Quelltext durchführen, da es signiert ist und damit auch ohne Scripting-Lizenz ausführbar ist.)

// #crypt 5250564f5c50357705565601064d31174201326e1b03134c25011340040c04004756693b5c17495508116d101f41202106590d0628155c5c4b564d0147413423184b190e0 95640616f70607a595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d091c09421e096a7a155b1458594060464f576278595a4c4f64485f1d292c004756693b5c17495b18022a020c0e2a260059090d3a1 1520d04594b1c471f4a5d57024b5b18092c1b4c162021d1915073a115c4557545601524922770555551a1304232f2c41425f1b03134c250113400a5d4b085a4a33324b02 Skript ausführen Extern bearbeiten			
Skript-Parameter			O ⋈ ★ ⊕ ↓ 0
Name	Тур	Aufzählungswerte	Wert / Voreinstellung E
host	String		w12dopaag.dopaag.local
port	String		636
enableSSL	String		true
caCertFile	String		C:\Program Files\Documents5\server\w12dopaagCA.pem
IdapBaseDN	String		DC=dopaag,DC=local
loginDN	String		CN=Idapsync,CN=Users,DC=dopaag,DC=Iocal
password	String		ldapsync
filter	String		
٠ III			•
<u>O</u> K <u>Ü</u> bernehme	en <u>N</u> eu <u>A</u> bbr	echen XML Export	

Abb. 7: Verbindungsdaten für den SSL-Zugriff

Wenn die Verbindung geöffnet werden konnte, so wird im Serverfenster und auf dem Client die folgende Meldung ausgegeben:

Verbindung hergestellt mi
---------------------------

Kann die Verbindung nicht hergestellt werden, so wird die Fehlermeldung angezeigt, die aus der openLdap-Schnittstelle an den Server weitergereicht wurde.

#### Hinweis

Wenn Änderungen am caCertFile vorgenommen wurden, kann es notwendig sein den DOCUMENTS-Server neu zu starten, da die openLdap-Schnittstelle die Zertifikate cached.

Wenn der Verbindungstest erfolgreich war, so müssen für den LDAP-Job und das LDAP-Logon im Weiteren die SSL-spezifischen Parameter als Eigenschaften am Mandanten oder optional in dem Skript "LdapParamDomain" angepasst werden.

Wenn die Konfiguration mit Hilfe des LDAP Wizards im DOCUMENTS Manager durchgeführt wurde, empfiehlt es sich am Mandanten die Eigenschaften LdapPort, LdapEnableSSL und LdapCaCertFile zu setzen (in zukünftigen Versionen von DOCUMENTS kann diese Konfiguration im LDAP Wizard durchgeführt werden).

loginScript	Ldap.LdapLogon
singleSignon	false
LdapSwitchingGroupDN	CN=DocumentsUsers,CN=Users,DC=dopaag,DC=local
LastDayPageHits	0
OverallPageHits	0
LdapPort	636
LdapEnableSSL	true
LdapCaCertFile	C:\Program Files\Documents5\server\w12dopaagCA.pem
QK Übernehmen Abbrechen	

Abb. 8: LDAP-SSL Eigenschaften am Mandanten

Optional kann die Konfiguration im Script "server\scriptlibs\Ldap\LdapParamDomain.js" vorgenommen werden (z.B., wenn mehrere LDAPS-Server angesprochen werden müssen) oder falls die LDAP-Scripte in den DOCUMENTS-Manager importiert wurden (XML-Import: 01\_LDAP\_Scripts.xml), dann muss die Konfiguration im DOCUMENTS-Manager im PortalScript "LdapParamDomain" erfolgen.

📔 C:\P	rogram Files\Documents5\server\scriptlibs\Ldap\LdapParamDomain.js - Notepad++ [Administrator]		
Datei	Bearbeiten Suchen Ansicht Kodierung Sprachen Einstellungen Werkzeuge Makro Ausführen Erweiterungen Fenster ? X		
6	) 🗄 🖕 💫 🖧 🐘 🖍 🍃 🙋 🗰 🍇 👒 👒 📴 🚰 🗉 📲 🖉 🖉 🖘 🖉		
🔚 LdapParamDomain js 🗵			
43	// ldapConfig.cutPrefix = false; // set to true in case your ADS groups have cuttable prefixes		
44	<pre>// ldapConfig.groupPrefix = ""; // define the prefix here</pre>		
45	// ldapConfig.withSuperior = true; // true, if superiors are maintained in AD and should be synchronized as we		
46	// ldapConfig.withSupervisor = true; // true, if group supervisors are maintained in AD and should be synchron		
47	<pre>// ldapConfig.withTranscode = false; // ELC 3.60 requires to transcode UTF-8 input from MS ADS</pre>		
48	// ldapConfig.useLdapBaseDN = false; // allows to use one common basic BaseDN for all configurable DNs		
49	// ldapConfig.noPasswdChange = true; // if this is set to true the user will not be able to change his passwor		
50			
51	<pre>ldapConfig.enableSSL = true;</pre>		
52	<pre>ldapConfig.tcpPort = 636;</pre>		
53	ldapConfig.caCertFile = "C:\\Program Files\\Documents5\\server\\w12dopaagCA.pem"		
54			
•	₩ <b>•</b>		
JavaScri	pt file length : 3.229 lines : 54 Ln : 47 Col : 4 Sel : 0   0 Windows (CR LF) UTF-8 INS		

Abb. 9: Skript "LdapParamDomain" mit den SSL-Parametern "enableSSL, tcpPort, caCertFile"

# Abbildungsverzeichnis

Abb. 1: Über ldp -> Verbinden -> SSL	. 4
Abb. 2: SSL - Zertifikat des LDAP-Servers	. 5
Abb. 3: Das Root-Zertifikat auswählen und anzeigen.	. 6
Abb. 4: Auf dem geöffneten Root-Zertifikat einen Zertifikatsexport starten	. 6
Abb. 5: Zertifikatsexport Base-64-codiert veranlassen	. 7
Abb. 6: XML-Import der openLdapSSLConnection.xml	. 8
Abb. 7: Verbindungsdaten für den SSL-Zugriff	. 8
Abb. 8: LDAP-SSL Eigenschaften am Mandanten	. 9
Abb. 9: Skript "LdapParamDomain" mit den SSL-Parametern "enableSSL, tcpPort, caCertFile"	. 9