



LDAP Channel Binding

Channel-Binding:

Für die Umsetzung von „LdapEnforceChannelBinding“ auf einem DomainController benötigt man das SecGuide.admx und SecGuide.adml, wenn man über eine GPO realisieren möchte.

Administrative Vorlagen			Ausblenden
Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher abgerufen.			
MS Security Guide			Ausblenden
Richtlinie	Einstellung	Kommentar	
Extended Protection for LDAP Authentication (Domain Controllers only)	Aktiviert		
Configure LdapEnforceChannelBinding	Enabled, always (recommended)		
Benutzerkonfiguration (Aktiviert)			Ausblenden
Keine Einstellungen definiert			

Registry-Eintrag:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\parameters]

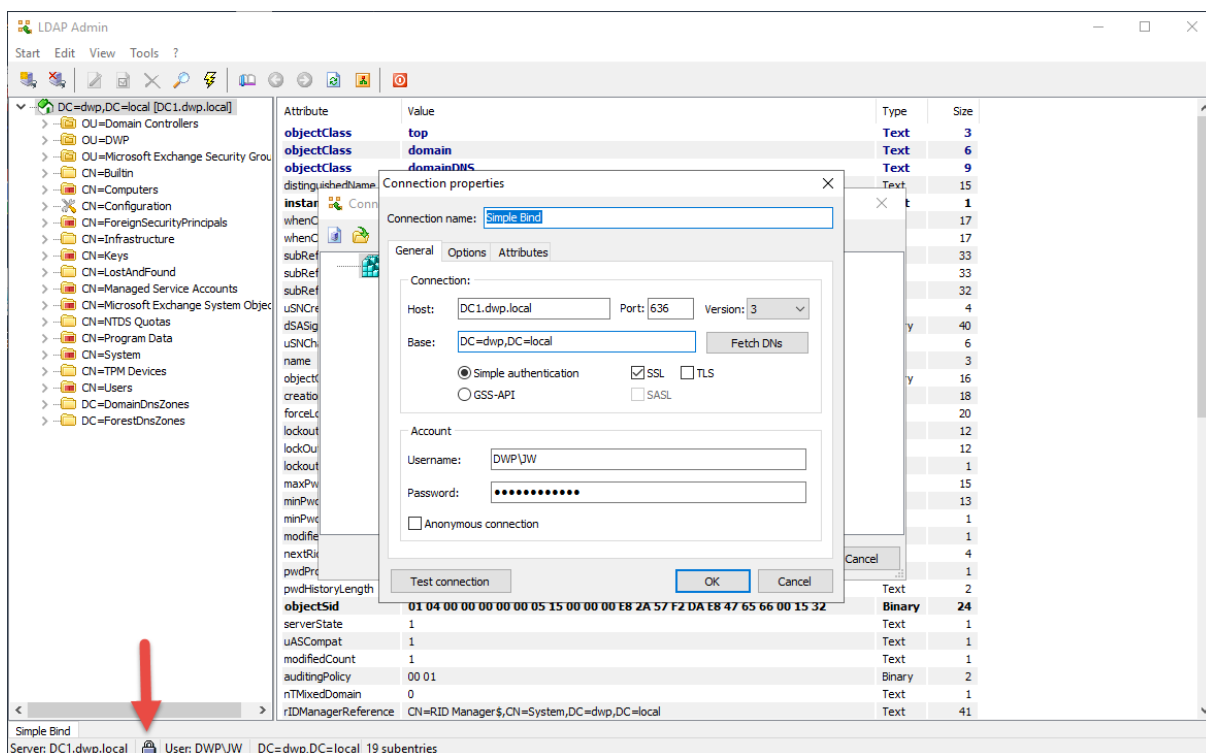
"ldapserverintegrity"=dword:00000002

"LdapEnforceChannelBinding"=dword:00000002

2 = erzwingen 1 = wenn möglich 0 = deaktiviert

Simple Authentication with SSL:



Für ein SSL-Binding benötigt man auf einem Domain-Controller ein Zertifikat.





LDAP Channel Binding

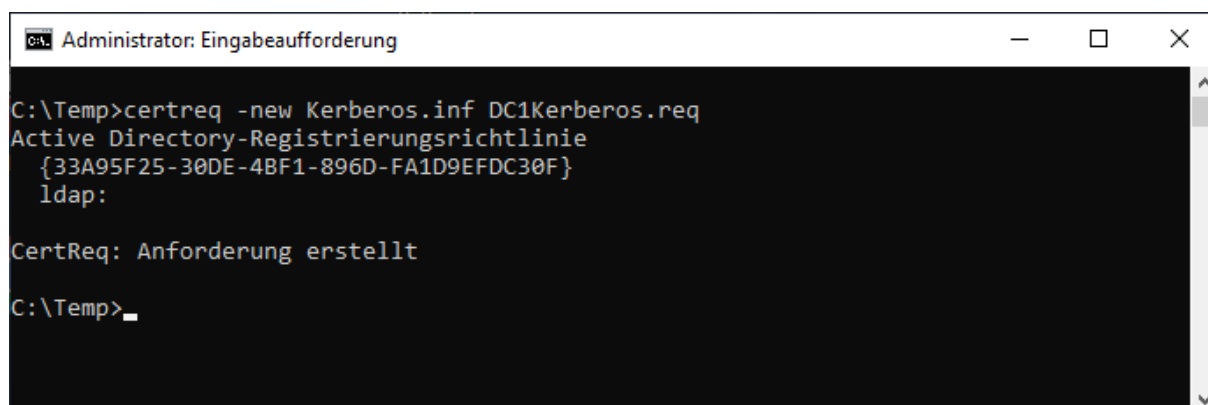
Falls die Zertifikatsvorlage „Kerberos Template“ im AD nicht veröffentlicht wurde, so kann man lokal auf der Maschine einen Request erstellen und dem CA-Admin den Request zum Signieren übergeben.

 Kerberos.inf	12.01.2020 16:38	Setup-Informatio...	1 KB
 Request.txt	12.01.2020 16:02	Textdokument	1 KB

```
; ----- Kerberos.inf -----  
[Version]  
Signature="$Windows NT$"  
[NewRequest]  
Subject = "CN=dc1.dwp.local" ; Anpassen  
FriendlyName = "Secure Binding"  
KeySpec = 1  
KeyLength = 2048  
Exportable = TRUE  
MachineKeySet = TRUE  
SMIME = False  
PrivateKeyArchive = FALSE  
UserProtected = FALSE  
UseExistingKeySet = FALSE  
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"  
ProviderType = 12  
RequestType = PKCS10  
KeyUsage = 0xa0  
[EnhancedKeyUsageExtension]  
OID=1.3.6.1.5.5.7.3.1  
[RequestAttributes]  
CertificateTemplate = Kerberos; Name anpassen  
SAN="dns=dc1.dwp.local" ; Anpassen  
; ----- Kerberos.inf -----
```

Über eine administrative CMD wird folgender Befehl ausgeführt.

```
certreq -new Kerberos.inf DC1Kerberos.req
```



```
C:\Temp>certreq -new Kerberos.inf DC1Kerberos.req  
Active Directory-Registrierungsrichtlinie  
  {33A95F25-30DE-4BF1-896D-FA1D9EFDC30F}  
  ldap:  
  
CertReq: Anforderung erstellt  
  
C:\Temp>
```

Den Request nur noch signieren lassen und das Zertifikat in den lokalen Computer Speicher importieren.



LDAP Channel Binding

Auf einem Client sieht die Konfiguration wie folgt aus:

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ldap\Parameters]  
"LdapClientIntegrity"=dword:00000002
```

2 = erzwingen 1 = wenn möglich 0 = deaktiviert

Parameter = 2 setzt aber die Installation eines Updates voraus:

<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8563>