

# LDAP Security: LdapEnforceChannelBinding

X [msxfaq.de/windows/sicherheit/ldapenforcechannelbinding.htm](https://msxfaq.de/windows/sicherheit/ldapenforcechannelbinding.htm)

Frank Carius

[Home](#) [Windows](#) [Safety](#) LdapEnforceChannelBinding



Digital technologies help against falsification of LDAP actions. Signatures and encryption. Since 2017, Microsoft has via an update of the clients and servers, the function for this provided but not yet forced. With the Windows Update in March 2020, domain controllers will now at least Force LDAP signing. Check your surroundings before something is no longer possible.

Update:

On Aug 18, 19, Microsoft announced for the first time about an upcoming tightened security setting. On 28.2 update that the implementation was not already available in Jan 2020 or March 2020 but only in the 2nd half of 2020 will be active ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing  
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023>

## What works after the change?

There are various articles and many are not quite clear or misleading. Microsoft actually only wants to ensure that "man in the middle" attacks are no longer possible. Today, if a client uses LDAP just like that, connects to the DC and logs in, it can be used via LDAP also change settings within the scope of its permissions. If this communication is not encrypted or signed, then an "evil part" can get into the Hook in the connection and adjust the commands. They want to as an admin, e.g. add a user to a group and the attacker simply rewrites the package so that his user is included in the Domain Administrators group. You don't want that. The best way to prevent this is to an end-to-end encrypted and signed connection via LDAP over SSL. But that doesn't have to be the case, because even with a LDAP connection without encryption can be "signed". All Windows clients already do that, but not all LDAP clients. A multi-IO device that can handle documents scans and sends by e-mail and creates an address book via LDAP doesn't do that.

Application procedure	Port LDAP/GC	Hitherto	LdapServerIntegrity active from autumn 2020
Simple Bind	389/3268	 Yes	 No
Simple Bind with TLS	636/3269	 Yes	 Yes
Unsigned SASL	389/3268	 Yes	 No
SASL over TLS	636/3269	 Yes	 Yes
SASL + LDAP Encryption	389/3268	 Yes	 Yes

Of the five registration procedures listed here, the two accesses that have neither TLS nor LDAP signing benefit.

Unfortunately, it is precisely the first procedure that is the most commonly used by 3rd party programs when You have entered an LDAP server somewhere just like that have

Any way via TLS encryption works problem- However, this also means "work" with certificates on the domain controllers.

## .. but control

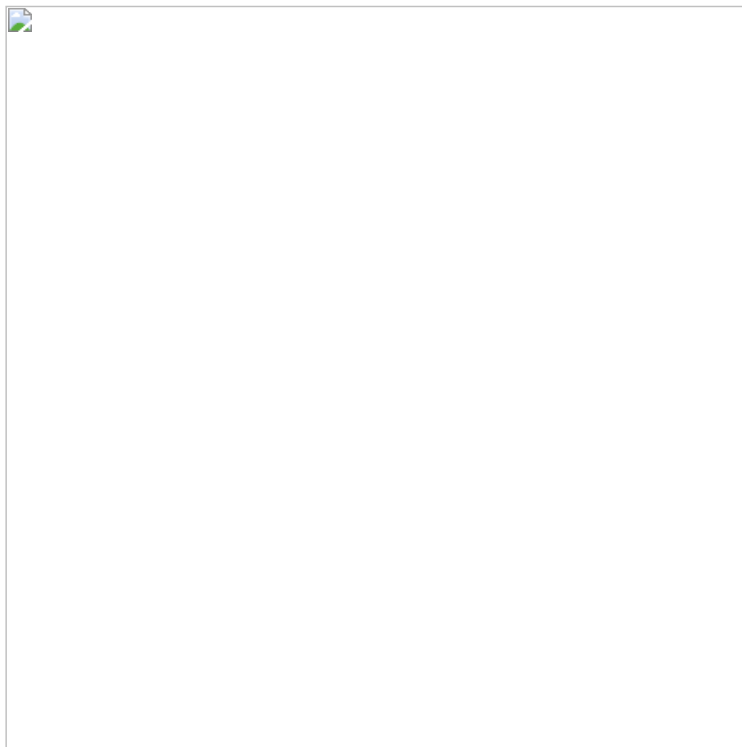
Not only Exchange Servers use LDAP to request the domain controller for the recipient's e-mail address, but LDAP is the protocol for managing an Active Directory. Administrators and domain administrators can use it to user, reset passwords, manage Group memberships and much more.

This makes LDAP connections an interesting target for these to hijack. It is in the same LAN through "ARP spoofing" and . a techniques not so difficult to combine a Clients to a server via a relay station Redirect. If data is not encrypted, they can be read along. If a signature is missing, you can the packages can even be changed in both directions. For an attacker here is

the write access to a Active Directory is very interesting to create your own accounts or change group memberships. These In 2017, this opportunity prompted Microsoft to publish its own security advisory.

- CVE-2017-8563 | Windows Elevation of Privilege Vulnerability (REQUIRED):  
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8563>
- LDAP Channel Binding and LDAP Signing Requirements - March update NEW behaviour  
<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ldap-channel-binding-and-ldap-signing-requirements-march-update/ba-p/921536#>
- Frequently asked questions about changes to Lightweight Directory Access Protocol  
<https://support.microsoft.com/en-us/help/4546509/frequently-asked-questions-about-changes-to-ldap>

The advisory also states that Microsoft does not "Workarounds".



But no workarounds are required either, because the Windows components already contain all functions. It is just a matter of configuration that allows the clients and Server encrypted or at least signed Communicate.

By Jan 2020, the default settings in such a way that clients and servers can use the Signings, but did not have to. Through the Update in Jan 2020, this Changed the default setting.

Of course, you could simply change the new default to the old behavior via Group Policy or REGEDIT. But I advise against that, because actually they could have can implement the safer variant and have it easy not done.

- 4034879 Use the LdapEnforceChannelBinding registry entry to make LDAP authentication over SSL/TLS more Secure  
<https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry>
- LDAP signing  
<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941832%28v%3dws.10%29>
- Use the LdapEnforceChannelBinding registry entry to make LDAP authentication over SSL/TLS more secure  
<https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry>

## **Affected systems and risks**

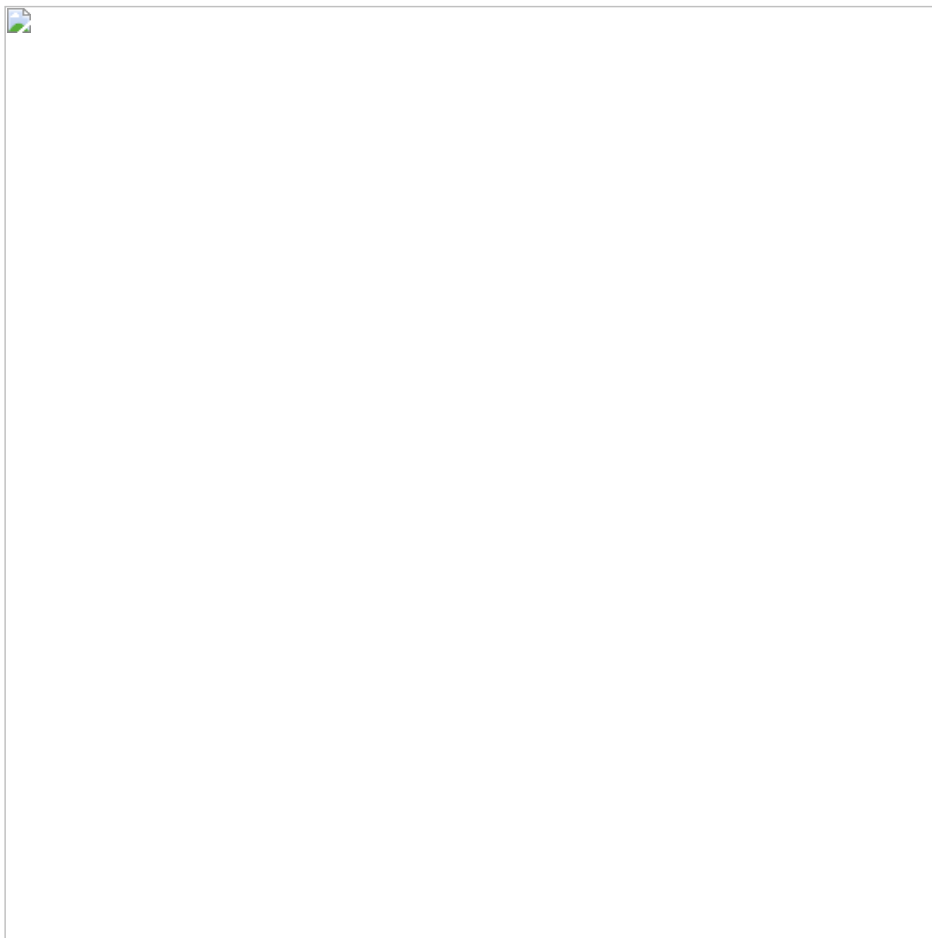
At first glance, you might feel relaxed because all halfway updated Windows Clients and servers should not be a problem at all. But but you can't be quite sure, because in almost in every heterogeneous environment, there is one or the other Service that addresses the domain controllers via LDAP and if necessary. then gets a problem. I think only in my own network.

- AntiSpam Products  
Actually, every company has one or two other spam filter between the Internet and mail server, which of course has a List of valid email addresses required. This is the only way he can immediately detect invalid addresses. and saves himself NDRs possibly fake senders. The most products read about this of course by LDAP the email addresses of your Exchange services and use LDAP against the Domain Controller.
- VoIP Session Border Controller  
Use VoIP gateways or session border Controllers that can be used e.g. via LDAP from the domain controller search for the phone number and based on the call to Skype for Business, Teams Trunk or the old telecommunications technology routes?. Then you should make sure that this will continue to be the case after January 2020 Works as expected
- Scan2Mail  
Any copier/printer that's worth its salt can also scan documents and use them Forward mail as PDF/TIFF. And of course, the user can use the Company Directory search for people. The most printers use a configured service account with read rights and LDAP. Without encryption or Signing will at least be the address book no longer work.
- Reverse Proxy PreAuth/WebApp Auth  
It's not that uncommon for services from the user to obtain login data via a form or Basic Authentication in the Asking for plain text and then using the access data in exchange for an "LDAP login" DC. If the registration then the application of validity and grants access. I have used such techniques with proxy servers (Apache), but also firewall (e.g. Sophos. See also [Azure ATP](#)) and there are certainly many other applications
- Provisioning, 3rd Party Apps, ...  
LDAP is a simple and universal usable protocol and so it can be assumed that that there are many other services in their network.

My list can't be complete, otherwise I would have to I check all the customers of the last one and they are a Quantity.

Microsoft itself has an extensive description on published on the following page

Client, service, and program issues can occur if you change security settings and user rights assignments  
<https://support.microsoft.com/hr-ba/help/823659>.



Currently, the default should be "Signing offered", i.e. the domain controller offers and accepts signing also such connections. But he also doesn't accept it yet signed connections. This will change by January 2020 unless we override this manually.

## **Evaluate**

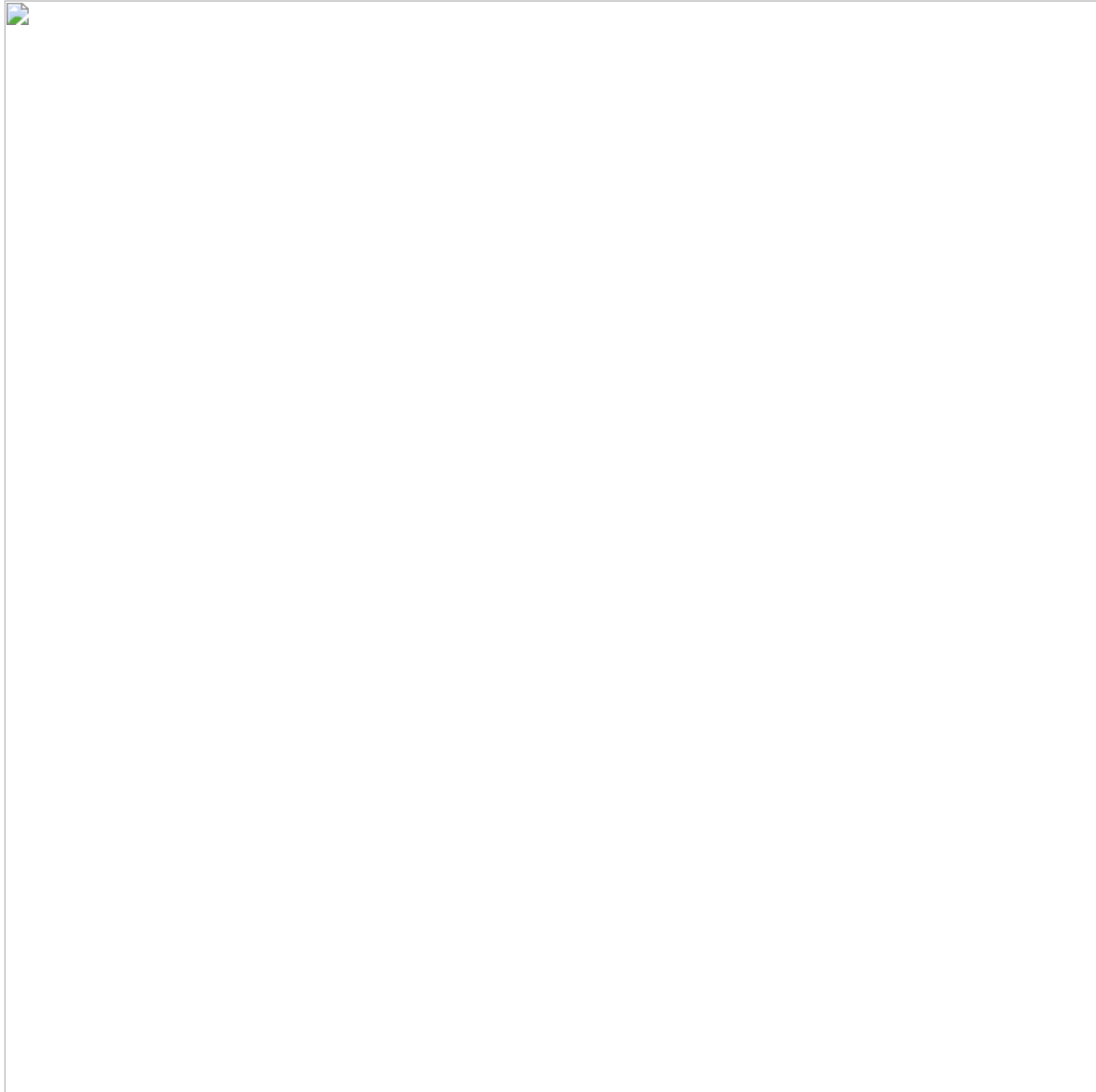
---

Time is ticking, because the update on January 2020 for stopping for long periods of time is not an option. I also advise refrain from configuring the old behavior again. and thus move the topic and ultimately to forget. However, in order to minimise the risk, we must know which clients can be connected to the domain controllers via LDAP and which of these clients still have the weak Leverage authentication. This data has been Windows 2008 in the event log.

Event ID 2886 — LDAP signing

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941829\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941829(v=ws.10)).

This will give you a first impression of whether there are such devices.



The message should come once in 24 hours, if a client "insecure". Already in this example but they see the problem that here between two Reports are also available for a few days, weeks or months can. So you will only find clients that regularly use the "weak way". Here is an event in detail:

Log Name: Directory Service  
Source: Microsoft-Windows-ActiveDirectory\_DomainService  
Date: 19.09.2019 00:08:11  
Event ID: 2886  
Task Category: LDAP Interface  
Level: Warning  
Keywords: Classic  
User: ANONYMOUS LOGON  
Computer: DC1.msxfaq.de  
Description:

The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection. Even if no clients are using such binds, configuring the server to reject them will improve the security of this server.

Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds.

For more details and information on how to make this configuration change to the server, please see <http://go.microsoft.com/fwlink/?LinkID=87923>.

You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher.

The link in the description goes to:

How to enable LDAP signing in Windows Server 2008

<http://go.microsoft.com/fwlink/?LinkID=87923>

<https://support.microsoft.com/en-us/help/935834/how-to-enable-ldap-signing-in-windows-server-2008>

But they don't yet know which end devices they are. At to obtain this information, you must use the Raise the diagnostic function on the DCs slightly. Per Regedit, via command line or REG file

```
Reg Add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics /v "16 LDAP Interface Events" /t REG_DWORD /d 2
```

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics]  
"16 LDAP Interface Events"=dword:00000002
```

The changes will take effect without restarting!

Now just wait for events with the number 2888 and 2889.

- [Event 2887, Event 2889 and LDAP Signing](#)
- [LDAP Tracing](#)
- Event ID 2888 — LDAP signing  
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941863\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941863(v=ws.10))  
Reports clients that have been signed without signing or without TLS have connected
- Event ID 2889 — LDAP signing  
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941849\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941849(v=ws.10))
- Identifying Clear Text LDAP binds to your DC's  
<https://blogs.technet.microsoft.com/russell/2016/01/13/identifying-clear-text-ldap-binds-to-your-dcs/>

This logging can be a bit more demanding on the server And they should consider how they can use this Evaluate information as quickly as possible. You can participate in eventlogs simply connect a "scheduled task" that and sends them an e-mail, for example. Anyone who has so far already carries out an evaluation of event logs, can be found in his historical logs retrospectively or perform more powerful opportunities.

Theoretically, you could also use [NetFlow/sFlow/IPFix/cFlow](#) to detect who is using port 389 connects what can be undesirable per se. With [Wireshark](#) (formerly [Ethereal](#)) you could even use the negotiated packages. But that's not all expedient.

But after the analysis, don't forget to debug by setting the value to "0"

```
Reg Add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics /v "16 LDAP Interface Events" /t REG_DWORD /d 0
```

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics]
"16 LDAP Interface Events"=dword:00000000
```

Access via LDAP is also possible via the "Global Catalog" possible. However, a GC is only "Read Only" achievable and thus a less rewarding destination. Nevertheless they should also require the switch to SSL here, because in Passwords transmitted in plain text could also be read here become.

LDAP Channel Binding and LDAP Signing Requirements - March update NEW behaviour

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ldap-channel-binding-and-ldap-signing-requirements-march-update/ba-p/921536#>

## **Implement**

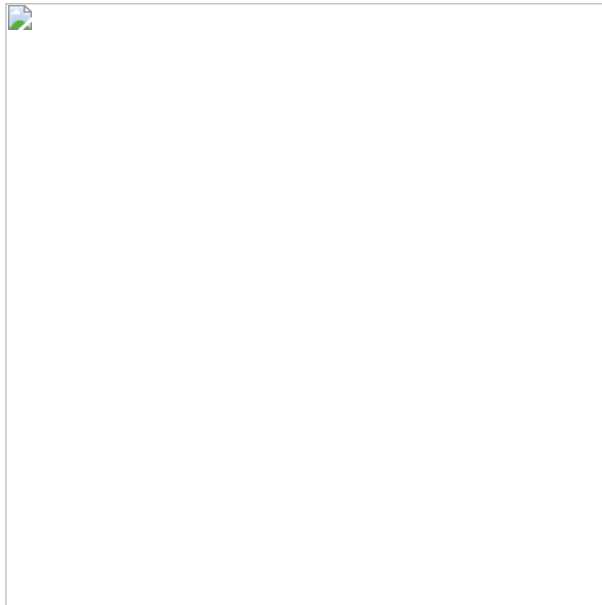
---

We can only hope that you make the logging as much as possible. quickly and in the few weeks until the release of the update at least the critical services in the protocol appear, which they must still change must. Usually it is enough to switch to LDAPS. Due to Due to the large number of clients and products, I can unfortunately do not provide a general description. Products that on the ADSI interface are usually uncritical and should work on their own. Here it can be problems are more likely to arise if they are protected by Group Policy have banned LDAP signing.

Über Gruppenrichtlinien können Sie das Verhalten der Clients als auch der Server kontrollieren. Wenn hier nichts konfiguriert ist, dann kommen die Defaults zu tragen.



Bis Januar bedeutet dies, dass jeder kann aber niemand muss. Ab Januar 2020 interpretiert ein Domain Controller die "rote Zeile" nicht mehr als "kann" sondern "muss". Sie können die Einstellung natürlich überschreiben. Zur Wahl steht aber nur "None" oder "Require Signing" aber nicht das "kann aber muss nicht". Das Bild ist von einem DC im Dezember 2019 und es könnte sein, dass das Update hier die Vorlage noch um ein "optional" erweitert.



Ansonsten können Sie den Wert ganz ohne Gruppenrichtlinie natürlich auch mit REGEDIT setzen. So setzen Sie für den Server als auch den Client ein "muss signieren"

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters]
"LDAPServerIntegrity"=dword:00000002
"LdapEnforceChannelBinding"=dword:00000002
```

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

Die Werte für einen AD LDS-Server, früher ADAM genannt, sind unter "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Parameters" zu finden.

Alternative Werte sind 0=Keine Signierung oder 1=Optional (Default)

- Use the LdapEnforceChannelBinding registry entry to make LDAP authentication over SSL/TLS more secure  
<https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry>.
- Aktivieren von LDAP-Signaturen in Windows Server 2008  
<https://support.microsoft.com/de-de/help/935834/how-to-enable-ldap-signing-in-windows-server-2008>

LDAP Signing Group Policy - No Downtime After installing ADV190023 both settings (even None and Not Defined) will enforce Require Signature Only 0 (OFF) will not enforce Require Signatu

- LDAP Signing auf Domänencontrollern erzwingen  
<https://www.gruppenrichtlinien.de/artikel/ldap-signing-auf-domainencontrollern-erzwingen/>
- Aktivieren von LDAP-Signaturen in Windows Server 2008  
<https://support.microsoft.com/de-de/help/935834/how-to-enable-ldap-signing-in-windows-server>

## **LdapEnforceChannelBinding**

Im Titel und einigen Webseiten wird aber auch der Parameter "LdapEnforceChannelBinding" genannt. Der Wert kann per Regedit oder Gruppenrichtlinie auf den Domain Controllern eingetragen werden. Er bestimmt, wie der LDAP Server eines Domain Controllers oder ADAM-Service mit dem Thema Signierung bei der Anmeldung umgeht. Die wesentlichen Informationen stehen auf:

Use the LdapEnforceChannelBinding registry entry to make LDAP authentication over SSL/TLS more secure  
<https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry>.

Er kann drei Werte annehmen oder nicht vorhanden sein.

Wert	Bedeutung
------	-----------



Nicht gesetzt (Default)	Normalerweise ist der Wert nicht vorhanden und der LDAP-Server setzt die im Code hinterlegten Defaults ein. Bis zum Januar 2020 entsprach das der "0" und mit dem Update wurde ein "2" draus
0 (Disabled, Default)	Funktion ist deaktiviert, dass der Server aktiviert kein "Channel binding" und ist der Default bei allen Servern, die nicht aktiviert wurden.
1 (Enabled)	Channel Binding Tokens (CBT) sind für alle Clients erforderlich, die diese Funktion unterstützen. Normal verbindet sich ein Client per LDAP und meldet mit, welche Funktionen er unterstützt. Das ist natürlich kein echter Schutz, da ein Angreifer auch diesen ersten Handshake unterbinden kann.
2 (Enforced)	In dieser Einstellung werden alle Clients gezwungen, Channel Binding Tokens (CBT) zu nutzen.

Damit ist klar, dass Sie mit einem Setzen des Werts auf "0" das alte aber unsichere Verhalten wieder aktivieren.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters]
"LdapEnforceChannelBinding"=dword:00000000
```

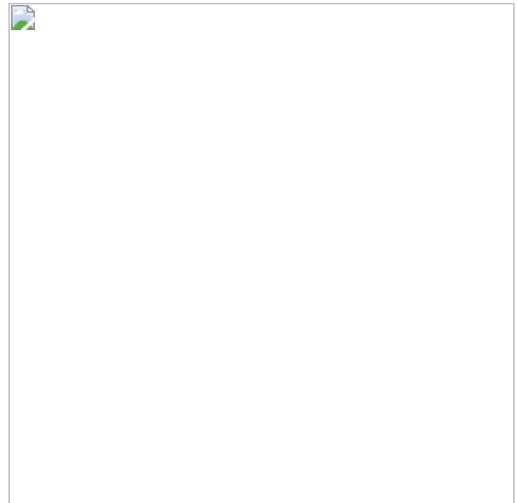
Ich würde diese Einstellung im Hinterkopf haben, um Sie im Notfall, und wirklich nur dann, auf den DCs nach dem Januar 2020 Update temporär wieder zu aktivieren.

## **Verifikation mit LDP.EXE**

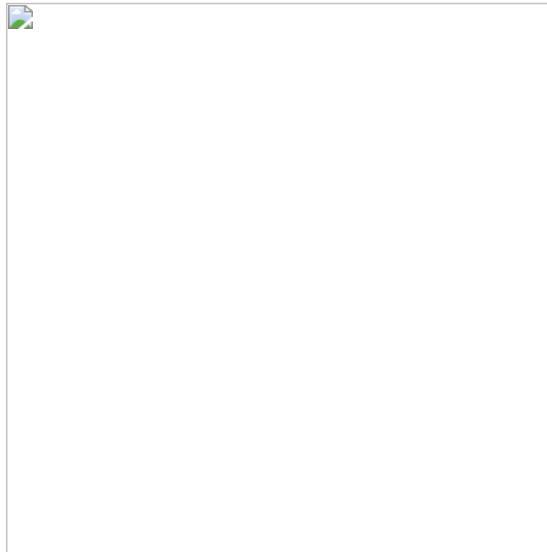
Ein möglicher Weg die verschiedenen Anmeldungen an einem LDAP-Server zu testen ist das Programm LDP.EXE. Dieses recht rudimentäre Programm erlaubt doch allerlei Einstellmöglichkeiten bei LDAP-Verbindungen.

- TCP oder SSL beim Connect  
Zuerst müssen Sie eine Verbindung mit dem Server herstellen. Neben dem Port können Sie hier auch manuelle SSL aktivieren

Wir können also gezielt uns per 389/TCP oder 636/TLS verbinden



- Authentifizierung  
Nach der anonymen Verbindung kommt dann die Anmeldung. Auch hier gibt es unterschiedliche Verfahren und eine optionale Verschlüsselung.



Mit diesen verschiedenen Optionen kann man spielen und am Ende folgende Tabelle erstellen. Die erste Anmeldung erfolgt anonym als 'NT-AUTORITÄT\ANONYMOUS-ANMELDUNG', die zweite Anmeldung nutzt explizit "Simple Bind" und die dritte Anmeldung dann die "integrierte" Anmeldung.

LdapEnforceChannelBinding	Connection	Anonym	Simple Bind	Unsigned SASL	Integriert	Beschreibung
0 (Kein Signing)	389	OK	OK	OK	OK	Ohne Zwang und ohne Verschlüsselung ging bislang alles. Kritisch sind die beiden gelben Felder, da hier Zugangsdaten abgegriffen oder Aktionen verändert werden könnten
	636	OK	OK	OK	OK	Mit LDAPS lösen sich die beiden kritischen Fälle, da die Verbindung nun verschlüsselt und signiert ist.
1 (Signing optional)	389	OK	OK	OK	OK	Wenn der Server ein Signing anbietet, dann erzwingt er es nicht. Die Clients sollten es nutzen
	636	OK	OK	OK	OK	Über LDAPS sorgt die Verschlüsselung dafür, dass Inhalte nicht verändert werden können.
2 (Signing erforderlich)	389	OK	Error 0x2028	Error 0x2028	OK	Sobald der Server eine Signierung erfordert, sind die einfachen Anmeldeverfahren aus dem Rennen. Nur die besseren Anmeldeverfahren, die auch eine LDAP-Signierung unterstützen funktionieren weiter
	636	OK	OK	OK	OK	Erst durch den Wechsel zu LDAPS sind auch wieder die einfachen Verfahren möglich.

Die graue "anonyme Anmeldung" geht immer. Hier ist aber auch keine Gefahr, da keine Anmeldedaten oder Aktionen übertragen werden. Interessanter sind die gelben Zugriffe, die heute schon ein Risiko darstellen. Solche unsicheren Zugriffe sind bislang möglich. Nachdem der Wert für "LdapEnforceChannelBinding" auf 2 gesetzt wurde, werden diese Zugriffe mit dem folgenden Fehler verweigert:

Error 0x2028 Eine sicherere Authentifizierungsmethode wird für diesen Server benötigt.

Sie sehen aber auch, dass mit einer entsprechend "sicheren" Anmeldung und LDAP Signierung der Pakete auch weiterhin ein Zugriff über Port 389 möglich ist. Nur schwache Anmeldeverfahren sind ausgesperrt.

Am Besten fahren sie also mit einer LDAPS-Verschlüsselung. Allerdings müssen dann nicht nur die Clients LDAPS unterstützen. Als Admin müssen Sie auf den Domain Controllern entsprechende Zertifikate vorhalten und regelmäßig aktualisieren.

- Understanding LDAP Security Processing  
<https://docs.microsoft.com/en-s/archive/blogs/askds/understanding-ldap-security-processing>
- Troubleshooting LDAP Over SSL  
<https://docs.microsoft.com/en-us/archive/blogs/askds/troubleshooting-ldap-over-ssl>
- LDAPS ist nicht LDAP Signing + Channel Binding  
<https://cusatum.de/ldaps-ist-nicht-ldap-signing-channel-binding/>
- Domain controller: LDAP server signing requirements and Simple Binds  
<http://setspn.blogspot.com/2016/09/domain-controller-ldap-server-signing.html>
- Strong Authentication: Error message "Server requires binds to turn on integrity checking if SSL/TLS are not already active on the connection"  
<https://www.dirwiz.com/kb/346>

## **Zertifikate für Domaincontroller**

Ich bin sicher, dass bei den meisten Firmen irgendwelche Client mit "Simple Bind" arbeiten. Auf der anderen Seite wird die IT Security die höhere Sicherheit anfordern. Dann bleibt ihnen nur die Option diese Geräte auf LDAPS umzustellen. Sollten die wenigen Clients das aber nicht unterstützen, dann können Sie diese nur abschalten, ersetzen oder sie lassen weiterhin einen LDAP-Server mit schwacher Absicherung laufen, der dann aber nur noch von diesen Geräten erreicht werden kann. Dazu eignen sich Firewalls und VPNs. Ziel muss aber der Wechsel auf LDAPS sein.

Dafür brauchen Sie aber Zertifikate auf dem Domain Controller. Natürlich könnten Sie nun öffentliche Zertifikate für jeden DC kaufen oder sogar ein "Wildcard" für die Domain. Das geht aber nur, wenn ihr DNS-Name der Domäne auch öffentlich ist. Sie müssen ja den Besitz nachweisen. Das ist aber mit Zeit und Kosten verbunden aber hat den Vorteil, dass fast alle Clients der ausstellenden PKI vertrauen.

Eine Alternative ist die Nutzung einer eigenen PKI für die Ausstellung von Computerzertifikaten. Da ist einfacher und nicht unsicherer, wenn Sie ein paar Dinge beachten. In Kurzfassung:

- AD integrierte RootCA installieren  
Sie suchen sich einen Member-Server oder wegen mir auch einen Domain Controller, auf dem Sie die Windows Zertifikatsdienste installieren.
- Sie passen die CA so an, dass sie NUR DomainController-Zertifikate ausstellt  
Sie entfernen dazu einfach alle anderen Templates. Aufgabenstellungen wie Key-Archiv, Key Recovery etc. umgehen Sie elegant. Später können Sie die PKI noch erweitern, dass Sie auch noch allgemeine Computerzertifikate ausstellt. So können Sie dann später ihr VPN oder 802.1x noch auf Zertifikate umstellen und die Sicherheit erhöhen
- Autoenrollment  
Über das Template und eine Gruppenrichtlinie können Sie steuern, dass die Domain Controller automatisch ein Zertifikat anfordern und nach einem Jahr auch wieder verlängern

Damit sollten die Domain-Controller ein gültiges Zertifikat für ihren Namen haben und der LDAP-Dienst dieses auch nutzen. Eine umfangreichere Beschreibung finden Sie auf den weiteren Links

- [Die Zertifikatsstelle in der eigenen Firma](#)
- [Private CA](#)
- [CA Templates](#)
- Troubleshooting LDAP Over SSL  
<https://docs.microsoft.com/en-us/archive/blogs/askds/troubleshooting-ldap-over-ssl>

## **Weitere Links**

- [Event 2887, Event 2889 und LDAP Signing](#)

- LDAP Security  
Bewerten sie die Risiken eines LDAP-Servers und nutzen sie z.B. TLS
- LDAP Tracing
- Checkliste Active Directory Absicherung  
Keine Liste ist komplett aber fangen Sie heute an und hören sie nie auf
- LDAP Channel Binding and LDAP Signing Requirements - March update NEW behaviour  
<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ldap-channel-binding-and-ldap-signing-requirements-march-update/ba-p/921536#>
- ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing  
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023>
- Frequently asked questions about changes to Lightweight Directory Access Protocol  
<https://support.microsoft.com/en-us/help/4546509/frequently-asked-questions-about-changes-to-ldap>
- Microsoft erzwingt ab Januar sichere Verbindungen zum Domain Controller  
<https://www.nospamproxy.de/de/microsoft-erzwingt-ab-januar-sichere-verbindungen-zum-domain-controller/>
- LDAP Channel Binding and LDAP Signing Requirements - JANUARY 2020 Updates  
<https://techcommunity.microsoft.com/t5/Core-Infrastructure-and-Security/LDAP-Channel-Binding-and-LDAP-Signing-Requirements-JANUARY-2020/ba-p/921536>
- CVE-2017-8563 | Windows Elevation of Privilege Vulnerability (REQUIRED):  
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8563>  
Erforderliches Update auf allen Clients, damit diese mit dem Server-Updates im Jan 2020 weiter arbeiten können.
- Identifying Clear Text LDAP binds to your DC's  
<https://blogs.technet.microsoft.com/russellt/2016/01/13/identifying-clear-text-ldap-binds-to-your-dcs/>
- Use the LdapEnforceChannelBinding registry entry to make LDAP authentication over SSL/TLS more secure  
<https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry>
- How to enable LDAP signing in Windows Server 2008  
<https://support.microsoft.com/en-us/help/935834/how-to-enable-ldap-signing-in-windows-server-2008>
- Domain controller: LDAP server signing requirements and Simple Binds  
<http://setspn.blogspot.com/2016/09/domain-controller-ldap-server-signing.html>
- Client, service, and program issues can occur if you change security settings and user rights assignments  
<https://support.microsoft.com/hr-ba/help/823659>
- LDAPWiki: LDAPServerIntegrity  
<https://ldapwiki.com/wiki/LDAPServerIntegrity>
- LDAP Signing  
<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941832%28v%3dws.10%29>
- LDAP Signing auf Domänencontrollern erzwingen  
<https://www.gruppenrichtlinien.de/artikel/ldap-signing-auf-domainencontrollern-erzwingen/>

Tags: LDAP Security Update ManInTheMiddle