

Wissensdatenbank > Produkte > HiOS > So richten Sie die LDAP-Authentifizierung auf HiOS-Geräten ein

# So richten Sie die LDAP-Authentifizierung auf HiOS-Geräten ein

- 2023-12-18 - HiOS

In dieser Lektion wird beschrieben, wie Sie die LDAP-Authentifizierung auf HiOS-Geräten konfigurieren.

Nützliche Tools: LDAP-Browser, z. Softerra LDAP Browser

Installation eines Active Directory Server

Informationen zur Installation von Windows AD Server 2012 finden Sie unter folgendem Link:

http://social.technet.microsoft.com/wiki/contents/articles/12370.windows-server-2012-set-u p-your-first-domain-controller-step-by-step.aspx

Informationen zur Installation von Windows AD Server 2016 finden Sie unter folgenden Link:

https://ittutorials.net/microsoft/windows-server-2016/setting-up-active-directory-ad-in-windo ws-server-2016/

Anweisungen zum Einrichten des Microsoft AD-Zertifikatdienstes finden Sie hier:

https://www.virtuallyboring.com/setup-microsoft-active-directory-certificate-services-ad-cs/

Durchsuchen Sie den LDAP-Server



Verwenden Sie einen LDAP-Browser und durchsuchen Sie die Struktur Ihres AD-Servers.

L.	- 0 A	ministrator: Windows PowerShell		- 0 X					
€ • Server Manaç	Pladent Fund Harli Courtight (C) 2004 Placesoft Corporation, All ( PE ConversionAdministrations and PE ConversionAdministrations	ights reserved.						•@  <b>r</b>	Manage Tools
E Danhboard									
Local Server									
Al Servero									
W ADDS	The Atlan View Samilar No.	Ci tur Mala	neole I - (Console Root	Cartificates (Local Comput	er((Personal)Cen	Piceter)			
A DHS	•• 20 X 0 X 0 0								
RE File and Storage Semices (#	Constraints	haved To *	Insured By	Expiration Date	Intended Purgenes	Friendly Hanne	Salus Cell Acts	ine .	
	a E Periord	TOWNED DRY AND ABAN	Open PCA	22121	Owd Authentical	-Monar-	·	oficios	
	<ul> <li>Cardware</li> <li>Trate/Root Certification Author</li> </ul>	. 📫	All Taola +	lper			140	CANNOR SEV-CA	
	<ul> <li>Drappie Turt</li> <li>Drappie Turt</li> <li>Drappie Turt</li> </ul>		Cepy	laness Cartoficate with New Key				Mart Actions	•
	<ul> <li>TruttaciPublishers</li> <li>Unitvalied Cartillusies</li> </ul>		Delete	lanage Private Keys					
575 51 m	<ul> <li>Trind-Party Real Cardination Autor</li> <li>Trintati Datale</li> </ul>	norities	Properties	dranced Operations					
4	<ul> <li>Clerk Indiversation Issues</li> <li>Recent Institute</li> </ul>			4000					
	<ul> <li>Carificale Insultrant Reputs</li> </ul>								
	<ul> <li>Smart Ced Hutsd Kell</li> <li>Trutel Delets</li> </ul>								
	e								
40 M									
N									
		1					-		
	Epot a catilicate								

## So rufen Sie das Active Directory-CA-Zertifikat vom Server ab

1. Stellen Sie eine Remote-Desktop-Verbindung her oder melden Sie sich an der Konsole eines DC an.

2. Starten Sie über Powershell die Microsoft Management Console, indem Sie MMC eingeben

und die Eingabetaste drücken

- 3. Wählen Sie im Menü FILE die Option ADD/REMOVE SNAP-IN
- 4. Wählen Sie CERTIFICATES und klicken Sie auf die Schaltfläche ADD
- 5. Wählen Sie COMPUTER ACCOUNT
- 6. Wählen Sie LOCAL COMPUTER
- 7. Klicken Sie auf FINISH
- 8. Klicken Sie auf OK
- 9. Erweitern Sie die CERTIFICATES
- 10. Erweitern Sie PERSONAL
- 11. Wählen Sie den DC im rechten Fenster.
- 12. Klicken Sie mit der rechten Maustaste auf den DC
- 13. Wählen Sie ALL TASKS EXPORT
- 14. Klicken Sie auf NEXT (2 mal).
- 15. Wählen Sie Base-64-codiertes X.509 (.CER) aus und klicken Sie auf NEXT
- 15. Benennen Sie die Zertifikatsdatei (befindet sich auf dem DC )
- 16. Kopieren Sie die Datei und importieren Sie sie bei Bedarf

#### So rufen Sie das Active Directory-CA-Zertifikat von einem Client ab

File Action View Favorites Window Help	•								- 0 3
Init Action: View Facultas: Window Help     the Consult Root     Soft     Consult Root     Soft     Consult Root     Soft     Consult Root     Soft     Consult Root     Soft     Consult Root     Consult Ro	Invest To     Construction     Cons	Insued By     AddYout Tesmal CA Root     AddYout Tesmal CA Root     AddYout Tesmal CA Root     Ro	Expiration Due 5/10/2020 5/10/2020 5/17/2020 5/17/2020 5/17/2020 5/17/2020 5/17/2020 5/2/2020 1/17/2020 5/2/2020 1/17/2020 5/17/2020 1/17/2020 5/16/2020 1/17/2000 1/17/2000 1/17/2000	Intended Purposes Serve Authenticati- eAllo Server Authenticati- eAllo Server Authenticati- Server Authenticati- S	Friendly Name Section (AddToxt) «Nonce DigiCet Bahimore Nonce DigiCet Bahimore Nonce DigiCet Bahimore Section (Isman Put. Section (Isman) Put. Section (Isman) Put. DigiCet Isman Put. DigiCet Calabel Roo DigiCet Calabel Roo Nonest Root Calabel Root C	Status	(^	Actions Cetificates More Actions Relates Global Root CA More Actions	- ( 0 ) = 

To retrieve the AD server certificate from a client device:

- 1. open the Microsoft Management Console Window-key+R and type mmc
- 2. Select File Add/Remove Snap-in (CRTL+M) and add 'Certificates' for Computer account

3. Select Certificates (Local Computer) - Trusted Root Certification Authorities - Certificates from the tree structure

4. Highlight the Belden-Global-Root-CA certificate and select All Tasks - Export from the context menu (right click)

5. In the certificate export wizard select Base-64 encoded X.509 (.CER) format to export in file.

#### Authentifizierungsliste

Navigation 4								
S	Authentication List							
Authentication List 🔹 🗙	Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated applications	Active
Device Security	defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	8
	defaultLoginAuthList	local	Idap	reject	reject	reject	SSH,Teinet,WebInterface	8
Authentication List	defaultV24AuthList	local 🚽	reject	reject	reject	reject	Console(V.24)	8

Ändern Sie die Richtlinien für die Authentifizierungsliste in LDAP.

Zum Testen setzen Sie LDAP an zweiter Stelle, bis Sie Ihre Konfigurationsarbeiten überprüft haben.

## **LDAP-Konfiguration**

Navig	ation	•											
] چ	<b>L</b> (A (F 200) - (	D	LDAP Configura	ation									Â'
Filter	¥	×	Operation	Configuration									
Ø	Basic Settings	^		Client cache timeout [min]	10		Bind user pas	sword			User name attribute	userPrincipalName	
0	Time			Bind user			Base DN	1	=Users,ou=Necka	rtenzlingen,ou=DE,dc=eu,dr	Default domain	eu.gad.local	
$\square$	Device Security	4	CA certificate										
	User Management		URL										
	Authentication List		Boldon@lobal	and a second									_
L	LDAP		BeidenGiobal	+ Copy -									
	Configuration		Start	1001000000									
	Role Mapping	1	Index	Description	Address	Destination	Connection	Server status	Active				_
L .	<ul> <li>Management Access</li> </ul>	_				TCP port	secunty			1			
	Pre-login Banner	9	□ 1	Belden-Server	DCNEC1SRV003.eu.GAD.local	636	ssi	ok	¥	J			
A state	Network Security												
\$⊄	Switching						$\checkmark$ 3	. 📰 🖽	} ≡ -				
iavascripte	undefined;	~											

## Operation: On Konfiguration:

- 1. Base DN
- 2. User Name Attribute
- 3. Default domain
- 4. CA Certificate: Laden Sie das Serverzertifikat hoch, wenn Sie SSL oder TLS verwenden

 Geben Sie den AD server, die Portnummber(normalerweise 389 or 636) an. In diesem Beispiel verwenden wir aufgrund des verwendeten Zertifikats einen Servernamen. Stellen Sie sicher, dass Sie auch den DNS-Client aktivieren (nächster Schritt)



#### **Enable DNS Client**

Aktivieren Sie den DNS-Client

#### **Role Mapping**

Navigation 4					
	LDAP Role Map	ping			
Role Mapping 👻 🗙	Configuration				
Device Security	Matching policy	highest	Ψ.		
	Index	Role	Туре	Parameter	Active
Role Mapping	1	administrator	attribute	userPrincipalName=cxs08151@eu.gad.local	R

Erstellen Sie eine neue Rollenzuordnung.

Auswählbare Rollen sind nicht unauthorized, guest, auditor, operator und administrator

Ordnen Sie diese Rollen AD-Attributen oder -Gruppen zu.