

Kennisbank > Products > HiOS > How to set up the LDAP authentication on HiOS devices

How to set up the LDAP authentication on HiOS devices - 2023-12-18 - HiOS

LDAP Authentication HiOS (SSL)

This lesson describes how to configure LDAP Authentication on HiOS devices.

Useful tools: LDAP browser e.g. Softerra LDAP Browser

Installation of an Active Directory Server

For the installation procedure of Windows AD Server 2012 please refer to the following knowledge base article:

http://social.technet.microsoft.com/wiki/contents/articles/12370.windows-s erver-2012-set-up-your-first-domain-controller-step-by-step.aspx

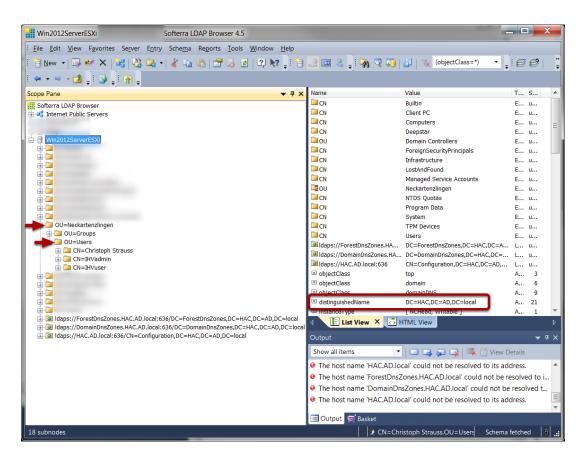
For the installation procedure of Windows AD Server 2016 please refer to the following article:

https://ittutorials.net/microsoft/windows-server-2016/setting-up-active-dire ctory-ad-in-windows-server-2016/

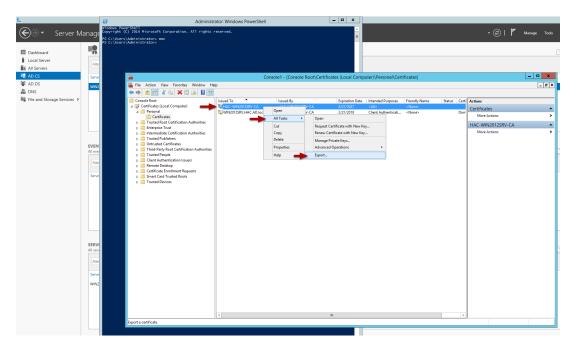
Instructions how to setup the Microsoft AD Certificate Service can you find here:

<u>https://www.virtuallyboring.com/setup-microsoft-active-directory-certificat</u> <u>e-services-ad-cs/</u>

Browse LDAP Server



Use a LDAP Browser and browse the structure of your AD server.



Retrieve the Active Directory CA certificate from server

1. Make a remote desktop connection or log onto the console of a DC.

2. Via powershell, launch the Microsoft Management Console by typing MMC and pressing enter

- 3. From the FILE menu choose ADD/REMOVE SNAP-IN
- 4. Choose CERTIFICATES and click the ADD button
- 5. Choose COMPUTER ACCOUNT
- 6. Choose LOCAL COMPUTER
- 7. Click FINISH
- 8. Click OK
- 9. Expand the CERTIFICATES
- 10. Expand PERSONAL
- 11. Select the DC in the RIGHT WINDOW PANE
- 12. Right Click on the DC
- 13. Choose ALL TASKS EXPORT
- 14. Click NEXT (2 times)
- 15. Select Base-64 encoded X.509 (.CER) and click NEXT
- 15. Name the certificate file (will be on the DC)
- 16. Copy the file and import it when needed

Retrieve the Active Directory CA certificate from a Client

Console1 - [Console Root\Certificates (Local Com File Action View Favorites Window He		ification Auth	onties(Certificates)						-	
🔿 🖄 📷 🤞 🐂 🗟 🖬										
Console Root	Issued To		Issued By	Expiration Date	Intended Purposes	Friendly Name	Status C	C^ A	ctions	
Certificates (Local Computer)	AddTrust External (A Root	AddTrust External CA Root	5/30/2020	Server Authenticati	Sectigo (AddTrust)		0	Certificates	
> 🧰 Personal	APGAD-RootCA		APGAD-RootCA	3/27/2023	<all></all>	<none></none>	F	R 🗖	More Actions	
Trusted Root Certification Authorities	Baltimore CyberTru	ist Root	Baltimore CyberTrust Root	5/13/2025	Server Authenticati	DigiCert Baltimore			More Actions	
Certificates	Belden-Global-Roc	t-CA	Belden-Global-Root-CA	10/7/2034	<all></all>	<none></none>		В	lelden-Global-Root-CA	
Enterprise Trust Intermediate Certification Authorities	BeldenRoot-CA	Open	toot-CA	10/29/2029	<all></all>	<none></none>			More Actions	
Trusted Publishers	Certum Trustec			12/31/2029	Server Authenticati	Certum Trusted Net				
Untrusted Certificates	Class 3 Public P	All Tasks	> Open	8/2/2028	Server Authenticati	VeriSign Class 3 Pu				
Third-Party Root Certification Authorities	COMODO RSA	Cut	Export th	1/19/2038	Server Authenticati	Sectigo (formerly C				
Trusted People	Copyright (c) 1	Сору	ht (c) 1997 Microsoft Cor	. 12/31/1999	Time Stamping	Microsoft Timesta				
Client Authentication Issuers	Deutsche Telek	Delete	e Telekom Root CA 2	7/10/2019	Secure Email, Serve	Deutsche Telekom				
Preview Build Roots	DigiCert Assure	Delete	t Assured ID Root CA	11/10/2031	Server Authenticati	DigiCert				
eSIM Certification Authorities	DigiCert Global	Properties	t Global Root CA	11/10/2031	Server Authenticati	DigiCert				
Homegroup Machine Certificates	DigiCert Global		t Global Root G2	1/15/2038	<all></all>	<none></none>				
PC-Doctor, Inc.	DigiCert Global	Help	Global Root G3	1/15/2038	Server Authenticati	DigiCert Global Roo				
Remote Desktop	DigiCert High Assu	rance EV Ro	DigiCert High Assurance EV Root		Server Authenticati	DigiCert				
Certificate Enrollment Requests	DST Root CA X3		DST Root CA X3	9/30/2021	Secure Email. Serve	DST Root CA X3				
Smart Card Trusted Roots	Entrust Root Certifi	cation Auth	Entrust Root Certification Authori		Server Authenticati	Entrust				
SMS	Entrust Root Certifi		Entrust Root Certification Authori	/	Server Authenticati	Entrust Root Certifi				
Trusted Devices	Entrust Root Certifi		Entrust Root Certification Authori		Server Authenticati	Entrust.net				
📔 Windows Live ID Token Issuer	Entrust.net Certific		Entrust.net Certification Authority		Server Authenticati	Entrust (2048)				
	GlobalSign		GlobalSign	3/18/2029	Server Authenticati	GlobalSign Root CA				
	GlobalSign		GlobalSign	12/15/2021	Server Authenticati	Google Trust Servic				
	GlobalSign Root C		GlobalSign Root CA	1/28/2028	Server Authenticati	GlobalSign Root CA				
	Go Daddy Class 2 (Go Daddy Class 2 Certification Au		Server Authenticati	Go Daddy Class 2 C				
	Go Daddy Root Ce		Go Daddy Root Certificate Author		Server Authenticati	Go Daddy Root Cer				
	Hotspot 2.0 Trust R		Hotspot 2.0 Trust Root CA - 03	12/8/2043	Server Authenticati	Hotspot 2.0 Trust R				
	konea-ci	001 CA - 03	konea-ci	11/10/2119	Server Authenticati	<none></none>				
	Microsoft Authenti	and a (terra) Rea	Microsoft Authenticode(tm) Root		Secure Email, Code					
	Microsoft ECC Pro				<all></all>	Microsoft ECC Prod				
	Microsoft Root Aut		Microsoft Root Authority	12/31/2020	<all></all>	Microsoft Root Aut				
	Microsoft Root Au		Microsoft Root Authority Microsoft Root Certificate Author		<all></all>	Microsoft Root Aut				
	Microsoft Root Cer		Microsoft Root Certificate Author Microsoft Root Certificate Author		<all></all>	Microsoft Root Cert				
			Microsoft Root Certificate Author Microsoft Root Certificate Author		<all></all>	Microsoft Root Cert				
			NO LIABILITY ACCEPTED, (c)97 W		Time Stamping	VeriSign Time Stam				
	QuoVadis Root CA		QuoVadis Root CA 2	11/24/2031	Server Authenticati	QuoVadis Root CA 2				
	QuoVadis Root CA	2 63	QuoVadis Root CA 2 G3	1/12/2042	Server Authenticati	QuoVadis Root CA		~		
	<						>			

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 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.

Authentication List

Navigation •									
😒 💄 🤙 <table-cell-rows> 🕄 🕕</table-cell-rows>	Au	thentication 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
Authentication List		defaultLoginAuthList	local	Idap	reject	reject	reject	SSH,Telnet,WebInterface	1
		defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	1

Change the authentication list policies to LDAP.

For testing put LDAP in second until you verified your configuration works.

LDAP configuration

DAP Configura	ition								(h) HIRSC	HMANN
Operation	Configuration									
	Client cache timeout [min]	10		Bind user past	sword			User name attribute	userPrincipalName	
	Bind user			Base DN	0	ou=Users,ou=Neckart	tenzlingen,ou=DE,dc=eu,dr	Default domain	eu.gad.local	
CA certificate										
URL										
BeldenGlobalE	COLCA 1 CHI X									
	100 C									
Start										
Index	Description	Address	Destination	Connection	Server statu	s Active				
7.4		DONEOLOGIANO OLO L				-				
	Deiden-Server	DENECTSRV003.e0.GAD.local	030	SSI	ox	×				
				✓ 3		¥ ≡ -				?
	Operation On Off CA certificate URL BeldenGkobalf Start	Client cache timeout (mm) Bind user CA certificate RR. BedenCliobalForce, 1 cer × - Terrier, 1 cer × - Terrier, 1 cer × - Terrier, 1 cer ×	Operation Operat	Operation Configuration Olient cache timeout 10 Bidd user 10 CA centricate Image: Cache timeout Biddewoldcate Cache timeout <th>Operation Configuration Clear cache innexit 10 Bind user 10 Bind user Base DN CA centricate Base DN Bedeexclobation 1 or × Bedeexclobation 1 or ×</th> <th>Operation Configuration Charl cache timeout 10 Bind user Base DN Concection Base DN Concection Concection State Description Index Description Addess Destrution ToP poet Executive</th> <th>Operation Contiguration One Officer cache timeod 10 Bed user password Image: Control of the cache timeod Bed user Base DN Cache cache timeod Control of the cache timeod Index Description Address Description Cache cache timeod Control of the cache timeod Index Description Address Description Cache timeod Control of the cache timeod I Belsen Server DCHECISRV003.eu. GAD.local Cache timeod Control of the cache timeod</th> <th>Operation Configuration Dear cache timeout 10 Bind user password eurolisers our-fleckasteroclingen our-DE, do-rea, do CA certificate eurolisers our-fleckasteroclingen our-DE, do-rea, do CA certificate eurolisers our-fleckasteroclingen our-DE, do-rea, do Case eurolisers our-fleckasteroclingen our-DE, do-rea, do Index Description Address Deladen-Server DC/ECISF/V02) au (ADI local 628</th> <th>Operation Contiguration 10 Bind user passood Image: Contiguration On: Other cache timeod 10 Bind user passood Image: Contiguration User name attribute Indicate Base DN Contiguration Contiguration Contiguration Contiguration CA certificate File Endeerdocation Contiguration Contiguration Contiguration Index Description Address Description Contending Contending Index Description Address Description Contending Contending Index Description Address Description Series status Active Index Description Address Description Series status Active Index Description Address Description Series status Active</th> <th>Operation Configuration One of the cach time of the cach time</th>	Operation Configuration Clear cache innexit 10 Bind user 10 Bind user Base DN CA centricate Base DN Bedeexclobation 1 or × Bedeexclobation 1 or ×	Operation Configuration Charl cache timeout 10 Bind user Base DN Concection Base DN Concection Concection State Description Index Description Addess Destrution ToP poet Executive	Operation Contiguration One Officer cache timeod 10 Bed user password Image: Control of the cache timeod Bed user Base DN Cache cache timeod Control of the cache timeod Index Description Address Description Cache cache timeod Control of the cache timeod Index Description Address Description Cache timeod Control of the cache timeod I Belsen Server DCHECISRV003.eu. GAD.local Cache timeod Control of the cache timeod	Operation Configuration Dear cache timeout 10 Bind user password eurolisers our-fleckasteroclingen our-DE, do-rea, do CA certificate eurolisers our-fleckasteroclingen our-DE, do-rea, do CA certificate eurolisers our-fleckasteroclingen our-DE, do-rea, do Case eurolisers our-fleckasteroclingen our-DE, do-rea, do Index Description Address Deladen-Server DC/ECISF/V02) au (ADI local 628	Operation Contiguration 10 Bind user passood Image: Contiguration On: Other cache timeod 10 Bind user passood Image: Contiguration User name attribute Indicate Base DN Contiguration Contiguration Contiguration Contiguration CA certificate File Endeerdocation Contiguration Contiguration Contiguration Index Description Address Description Contending Contending Index Description Address Description Contending Contending Index Description Address Description Series status Active Index Description Address Description Series status Active Index Description Address Description Series status Active	Operation Configuration One of the cach time

Operation: On Configuration:

- 1. Base DN
- 2. User Name Attribute
- 3. Default domain
- 4. CA Certificate: Upload the server certificate if you use ssl or TLS
- Specify the AD server, port number (usually 389 or 636). In this example we use a server name due to the used certificate. Make sure that you enable DNS client as well (see next step).

Enable DNS Client

Navigation 4					
📚 🛃 🐼 📭 300 🚍 💽	DNS Client Global				
DNS Client - 🗙	Operation				
	⊙ On ⊖ Off				
Advanced	Cache				
DNS	⊙ On ◯ Off				
L Client					
Global					
Current					
Static					

Enable the DNS-Client

Role Mapping

Navigation 4					
😒 👢 🙋 💕 300 🕢 🕄	LDAP Role Map	pping			
Role Mapping 🗾 🗙	Configuration				
Device Security	Matching policy	highest	~		
	Index	Role	Туре	Parameter	Active
Role Mapping	1	administrator	attribute	userPrincipalName=cxs08151@eu.gad.local	 ∠

Create a new role mapping.

Selectable roles are unauthorized, guest, auditor, operator and administrator

Map these roles to AD attribute or groups.