

ナレッジベース > 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:

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

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

File Action View Favorites Window Hel	puter) (indiced Koot Certification Autr	ionties (Certificates)							
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	c ^	Actions	
Certificates (Local Computer)	AddTrust External CA Boot	AddTrust External CA Boot	5/30/2020	Server Authenticati	Secting (AddTrust)			Cartificater	
> 🛗 Personal	APGAD-BootCA	APGAD-RootCA	3/27/2023	<all></all>	<none></none>		R	Continuous .	
Trusted Root Certification Authorities	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025	Server Authenticati	DigiCert Baltimore			More Actions	
Certificates	Belden-Global-Root-CA	Belden-Global-Root-CA	10/7/2034	<all></all>	<none></none>			Belden-Global-Root-CA	
> Enterprise Trust	BeldenRoot-CA Open	Root-CA	10/29/2029	<all></all>	<none></none>			More Actions	
Intermediate Certification Authorities	Certum Trustec		12/31/2029	Server Authenticati	Certum Trusted Net			- More Actions	
 Insteal Publishers Instructed Castificator 	Class 3 Public P All Tasks	> Open io	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 Copy	ht (c) 1997 Microsoft Corp.	12/31/1999	Time Stamping	Microsoft Timesta				
Client Authentication Issuers	Deutsche Telek Delete	ne Telekom Root CA 2	7/10/2019	Secure Email, Serve	Deutsche Telekom				
> Preview Build Roots	DigiCert Assure	t Assured ID Root CA	11/10/2031	Server Authenticati	DigiCert				
SIM 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		1/15/2038	Server Authenticati	DigiCert Global Roo				
Remote Desktop	DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root	11/10/2031	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 Certification Auth	Entrust Root Certification Authority	11/27/2026	Server Authenticati	Entrust				
SMS	Entrust Root Certification Auth	Entrust Root Certification Authori	12/18/2037	Server Authenticati	Entrust Root Certifi				
Trusted Devices	Entrust Root Certification Auth	Entrust Root Certification Authori	12/7/2030	Server Authenticati	Entrust.net				
Windows Live ID Token Issuer	Entrust.net Certification Author	Entrust.net Certification Authority	7/24/2029	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 CA	GlobalSign Root CA	1/28/2028	Server Authenticati	GlobalSign Root CA				
	Go Daddy Class 2 Certification	Go Daddy Class 2 Certification Au	6/29/2034	Server Authenticati	Go Daddy Class 2 C				
	Go Daddy Root Certificate Auth	. Go Daddy Root Certificate Author	1/1/2038	Server Authenticati	Go Daddy Root Cer				
	Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Server Authenticati	Hotspot 2.0 Trust R				
	🔄 konea-ci	konea-ci	11/10/2119	Server Authenticati	<none></none>				
	Microsoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root	1/1/2000	Secure Email, Code	Microsoft Authenti				
	Give State CC Product Root Ce	Microsoft ECC Product Root Certi	2/27/2043	<all></all>	Microsoft ECC Prod				
	GMicrosoft Root Authority	Microsoft Root Authority	12/31/2020	<all></all>	Microsoft Root Aut				
	GMicrosoft Root Certificate Auth	Microsoft Root Certificate Authori	5/10/2021	<all></all>	Microsoft Root Cert				
	GMicrosoft Root Certificate Auth	Microsoft Root Certificate Authori	6/23/2035	<all></all>	Microsoft Root Cert				
	Given State Auth	Microsoft Root Certificate Authori	3/22/2036	<all></all>	Microsoft Root Cert				
	NO LIABILITY ACCEPTED, (c)97 .	. NO LIABILITY ACCEPTED, (c)97 Ve	1/8/2004	Time Stamping	VeriSign Time Stam				
	QuoVadis Root CA 2	QuoVadis Root CA 2	11/24/2031	Server Authenticati	QuoVadis Root CA 2				
	QuoVadis Root CA 2 G3	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 •								
S L Q P 300 O	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	V
Authentication List	defaultLoginAuthList	local	Idap	reject	reject	reject	SSH,Telnet,WebInterface	1
	defaultV24AuthList	local	reject	reject	reject	reject	Console(V.24)	5

Change the authentication list policies to LDAP.

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

LDAP configuration

DAP Configura	ition								(n) 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									
	+ Copy -									
Start										
Index	Description	Address	Destination	Connection	Server statu	s Active				
7.4		DONEOLOGIANO OLO L	ror pon	security		-				
	Deiden-Server	DENECTSRV003.e0.GAD.local	030	SSI	ox	×				
				✓ 3		¥ ≡ -				?
	DAP Configura Operation On Of Of Article Relidence Stati	DAP Configuration Operation Chifguration	DAP Configuration Operation Operation Operation On O O O O O O O O O O O O O O O O O O	DAP Configuration Operation Operation Official Operation	DAP Configuration Operation Operatio	DAP Configuration Operation Operatio	DAP Configuration Operation Operati	DAP Cantiguration Operation Operatio	DAP Configuration Operation Configuration Image: Configuration Image: Configuration Image: Configuration Ima	DAP-Configuration Configuration Co

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.