

April 28th, 2021



Contents

Configure the authentication provider	3
Azure AD	3
Create the enterprise application in Azure AD	3
A. Creating the Netop Portal application Azure AD from the Application gallery	3
Add users and groups to the application	7
Configure single sign-on	9
Configure the application permissions	17
Configure Certificates & secrets	21
B. Creating the Netop Portal application Azure AD as a Non-gallery application	24
Add users and groups to the application	27
Configure single sign-on	29
Configure the application permissions	35
Configure certificates & secrets	39
Configure Azure AD in the Netop Portal	42
ADFS integration with the Netop Portal	47
Add Netop Portal as a Trusted Relying Party	47
Add Claim Rules for the Netop Portal Relying Party	55
Configure the Netop Portal	67
Remote session using ADFS	68
Managing the ADFS users	69

Configure the authentication provider

Azure AD

Create the enterprise application in Azure AD

There are two methods of creating the enterprise application in Azure AD:

- A. You can add the **Netop Portal** application from the Application gallery in the Enterprise applications section. Refer to the following <u>link</u> for additional information on how you can add and configure the application from the application gallery.
- B. You can create the Netop Portal application from the Non-gallery application section
- A. Creating the Netop Portal application Azure AD from the Application gallery

To create the Netop Portal application in Azure AD, proceed as follows:

1. Log in the <u>Azure Portal</u>.



2. Go to Azure Active Directory.

2.1. Click on the **More** button.

E Microsoft Azure	P Search resources, services	and docs (G+/)	E & + @ ? @ 😫
	Welcome to Azure! Don't have a subscription? Check out the following opti	ns.	
	Start with an Azure free trial Get \$200 free credit toward Azure products and service plus 12 months of popular free services.	Manage Azure Active Directory Access student benefits Manage access, set smart policies, and enhance security with Azure Active Directory. Get free software, Azure credit, or access for Teaching after you verify your acader	Azure Dev Tools nic status
	Eearn more B	View Learn more O' Explore Learn more O'	
	Azure services		
	+ 🚸 📮	😵 🖃 🗃 🐼 🌞	\rightarrow
	Create a Azure Active Virtual resource Directory machines	App Services Storage SQL databases Azure Database Azure Cosmos Kubernete accounts for PostgreSQ DB services	s More services
	Navigate		
	📍 Subscriptions 🛛 💓 R	source groups 👪 All resources 🖾 Dashboard	
	Tools		
	Microsoft Learn D [*] Learn Azure with free online training from Microsoft	ture Monitor Cost Manageme Secure your apps and infrastructure Cost Manageme Analyze and opt cloud spend for	nt imize your free

2.2. Click on Azure Active Directory.

=	\mathcal{P} :Search resources, services, and docs (G+ η)	
+ Hide portal menu		
A Home	Welcome to Azure!	
E Dashboard	Don't have a subscription? Check out the following options.	
All services		
* FAVORITES		
All resources		
() Resource groups		
S App Services		
🍜 Function App		
SQL databases		
S Azure Cosmos DB	Start with an Azure free trial Manage Azure Active Directory Access student benefits	
Virtual machines	Get \$200 free credit toward Azure products and services, Manage access, set smart policies, and enhance security Get free software, Azure credit, or access Azure Day Tools for the software access free security with Azure Azure Credit Contractions for resources for the software access for the s	
Load balancers	plot is monitor to popular tree services mini rusare Acure Directory, no readoning alter you reitry you readoning alters and an analysis and an	
Storage accounts		
Virtual networks		
Azure Active Directory	Azure services	
C Monitor		
Advisor	Carlas Arma Artise Virtual Ann Sanizer Steans SDI database Arma	
Security Center	esource Directory instance and accounts	
O Cost Management + Billing		
Help + support	Navigate	
	📍 Subscriptions 📦 Resource groups 🇱 All resources 🔤 Dashboard	
	Tools	
	Microsoft Learn 🖞 🛞 Azure Monitor 🙆 Security Center 🔥 Cost Management	
	Learn Azure with free online Monitor your apps and Secure your apps and Vanalyze and optimize your training from Microsoft infrastructure infrastructure cloud spend for free	

3. Go to Enterprise applications.

				d 🛱 🗘 🕲 ? 😊	
Home >					
Azure Active Directory	ew				×
	« 💿 Switch tenant 📋 Delete tenant 🕂	Create a tenant 🕜 What's new 🛛 🐱 Preview	features 🛛 🛇 Got feedback?		
Overview	·				
oetting started	Azure Active Directory can belo you enab	e remote work for your employees and partners Learn m	1078		×
Preview features		e remote more not your employees one pareness ceam m			
X Diagnose and solve problems	netop.es				
Manage					
🚨 Users	2 Search your tenant				
A Groups	Tenant information	Azure AD Connect			
External Identities	. New role				
Roles and administrators	Global administrator More info	Enabled			
Administrative units	License	Last even			
Enterprise applications	Azure AD Free	Less than 1 hour ago			
Devices					
App registrations	Primary domain				
Identity Governance	netop.es				
Application proxy					
🔓 Licenses	Sign-ins				
Azure AD Connect					
🔁 Custom domain names			Looke like the sign in data is uppusible. To again later		
Mobility (MDM and MAM)			cooks like the sign-in data is unavalique. Ity again later,		
Password reset					
Company branding					
User settings					
Properties	Create				
Security	& (i)	24	85		

4. Click on the **New application** button.

	Microsoft Azure	₽ Search resources, services, and docs (G+/)		E	I 🗣 🔎 🐵 ? 🐵	8
Hon	ne > Enterprise applicati	ons				
	Enterprise application	ons All applications …			>	ĸ
Over	« rview Overview	New application III Columns IIII Preview features ♥ Got feedback? Try out the new Enterprise Apps search preview. Click to enable the preview. →				
🗙 Man	Diagnose and solve problems	Application type Applications status Application visibilities Enterprise Applications V Any Any	Ny Apply Reset			
	All applications	\wp First 50 shown, to search all of your applications, enter a display name or the application ID				
5	Application proxy	Name Homepage U	JRL	Object ID	Application ID	
8	User settings	•				
Secu	urity	<u>6</u>				
•	Conditional Access					
٢	Consent and permissions					
Activ	vity					
Э	Sign+ins					
ai -	Usage & insights					
	Audit logs					
۵	Provisioning logs (Preview)					
	Access reviews					
Θ	Admin consent requests (Preview)					
Trou	bleshooting + Support					
1	Virtual assistant (Preview)					
2	New support request					

5. In the Search application entry field, specify Netop Portal.

E Microsoft Azure			e 💀 🖓 🎯 ? 😊	
Home > > Enterprise applications > Browse Azure AD Gallery				×
+ Create your own application () Request new gallery app	🛇 Got feedback?			
You're in the new and improved app gallery experience. Click here to	switch back to the legacy app gallery experience. $ ightarrow$			
Cloud platforms	n-on : All User Account Management : All Categories : All	de SAP		
On-premises applications				
Add an on-premises application Configure Azure AD Application Prony to enable secure remote access.	Learn about Application Proxy Learn how to use Application Proy to provide secure remote access to your on-premise applications.	Manage Application Proxy connectors Connectors are lightweight agents that sit on-premises and facilitate the outbound connection to the Application Provy service.		
➔ Federated SSO (2) Provisioning				

6. Click on the **Netop Portal** icon.

	∠ Search resources, service	ces, and docs (G+/)		E 🛱 🖓 🕸 ? ©	8
Home > > > > > > > > > > > > > > > > > > >					×
+ Create your own application 🕕 Request new gal	lery app 🛛 🛇 Got feedback?				
You're in the new and improved app gallery experience	e. Click here to switch back to the legacy app gallery experience. $ imes$				
retop portal X Federated SSO Provisioning	Single Sign-on : All User Account Management : All	Categories : All			
Showing 11 of 11 results					
Notop Portal Netop UC	Cocco Portal Coco Int ©©©©	Internap Portal Internap Retork Services Corporation.	Apex Portal APEX Anaylos @	Evenex ePortal Elevel	
IQN Developer Portal IQNavigator	TeleSign Portal Telegign Cop.	iserver Portal Cross Software D	ResLife Portal ResLife Portal Portal Texture Indexed Texture Index Texture Index Tex	RedHat Portal Login Red Hat, Inc.	
Kognitis Partner Portal Cognita					

7. If necessary, you can specify a different application name than Netop Portal in the Name entry field.



8. Click on the Create button to finish adding the Netop Portal application to the Azure Portal.

Microsoft Azure	℅ Search resources, service	is, and docs (G+/)			E 🗣 Q 🚳	? 🙂
Home > > Enterprise applications >				Netop Port	al	×
Browse Azure AD Gallery						
+ Create your own application ① Request new gallery app 🗢 Got feedba	ck?			Logo 🕕	Name * () Netop Portal	
You're in the new and improved app gallery experience. Click here to switch back to th	e legacy app gallery experience. $ ightarrow$			Remote Control	Publisher ()	Provisioning ① Automatic provisioning is not
					Netop Loc	supported
D netop X Single Sign-on : All	User Account Management : All	Categories : All			Single Sign+On Mode ①	URL ①
Federated SSO Provisioning					SAML-based Sign-on	https://www.netopportal.com/
Showing 21 of 21 results					Linked sign-on	
					Read our step-by-step Netop Po	rtal integration tutorial
Netop Portal Netros LC S	flagento, Inc.	NetProxy-S Dantelo Ap5 €	Netskope Administ Console Netskope 3		Remote Control of devices and c	computers
GameStop GameStop	llertOps lertOps	Nest Nest Labs	Xponent XPONENT Employer Solu			
	2					
Central Desitop Central Desitop Inc.	Dineteam Ineteam Inc.	NetSuite OpenAir NetSuite Inc.	Net vision Sea PTE LTD			
				Create		

The application is created successfully and added to the Enterprise applications section.

Add users and groups to the application

To add users and groups to the application, proceed as follows:

- 1. Go to Azure Active Directory.
- 2. Go to Enterprise applications.

3. Click on the newly created Netop Portal application.

■ Microsoft Azure	P Search resources, services, and docs (G+/)		D 🛱 Q 🐵 ? 👳	
Home > > Enterprise application	ons			
Enterprise application	ons All applications …			×
 Overview 	+ New application ≣≣ Columns Preview features ♡ Got feedback?			
0 Overview	✓ Try out the new Enterprise Apps search preview! Click to enable the preview. →			
Diagnose and solve problems Manage	Application type Applications status Application visibility Enterprise Applications Any Any Apply Reset			
All applications	P First 50 shown, to search all of your applications, enter a display name or the application ID.			
Application proxy	Name Homepage URL	Object ID	Application ID	
User settings	O Netop Portal			
Security	<u>6</u>			
Conditional Access				
Consent and permissions				
Activity				
Sign-ins				
📫 Usage & insights				
Audit logs				
Provisioning logs (Preview)				
E Access reviews				
 Admin consent requests (Preview) 				
Troubleshooting + Support				
🕎 Virtual assistant (Preview)				
New support request				

4. Click on Assign users and groups.

	${\cal P}$ Search resources, services, and docs (G+/)		₽	Q		\odot	
Home > Enterprise application	All applications > Netop Portal Overview						
Netop Portal Ov Enterprise Application	erview						
	«						
👪 Overview	Properties						
Deployment Plan	Name ①						
🗙 Diagnose and solve proble	ns Netop Portal						
Manage	Application ID ①						
H Properties	91389a0c-t01c-4d89-8/29 (C						
A Owners	Object ID ① 62f2bb4c-62e1-4820-8150 ①						
Users and groups							
Single sign-on	Getting Started						
Provisioning							
Application proxy	1. Assign users and groups 3. Set up single sign on						
Self-service	Provide specific users and groups access to the applications Enable users to sign into the	ir applica tials	tion				
Security	Assign users and groups Get started						
🐁 Conditional Access							

5. Click on the Add User/group button to add the allowed users or groups.

	P Search resources, services, an	i docs (G+/)		· □ @ ? ©	0
Home > > Enterprise application	ons > Netop Portal				
Netop Portal Users Enterprise Application	and groups				×
«	+ Add user/group 🖉 Edit 🔋 Remove 🖉 Update Credentials 🏥	Columns 🛛 💙 Got feedback?			
Deployment Plan	The application will appear on the Access Panel for assigned users. Set 'visible to u	sers?" to no in properties to prevent this. \rightarrow			
Manage	First 100 shown, to search all users & groups, enter a display name.				
Properties	Display Name	Object Type	Role assigned		
A Owners	65	User	Default Access		
& Roles and administrators (Preview)		User	Default Access		
Users and groups					
Single sign-on					
Provisioning					
Application proxy					
Self-service					
Security					
Conditional Access					
🔒 Permissions					
Token encryption					
Activity					
Sign-ins					
🕍 Usage & insights					
Audit logs					
Provisioning logs (Preview)					
E Access reviews					

NOTE: Make sure that the users that you add are from the Windows Server AD.

6. After you finish adding the users and groups, click on the Assign button.



Configure single sign-on

To configure the single sign-on, proceed as follows:

- 1. Go to Azure Active Directory.
- 2. Go to Enterprise applications.
- 3. Click on the newly created Netop Portal application.

4. Click on Set up single sign-on.

	<i>P</i> Search resources, services, and docs (G+/)	M 🛱 🔎 🕲 ? 🙄 🕴
Home > > Enterprise application	tions >	
Netop Portal Beta	Fest Overview …	×
«		
K Overview	Properties	
Deployment Plan	Ame O	
Manage	Netop Portal Beta Test	
Properties	Application ID ()	
🚑 Owners	Chiert ID. O	
👃 Roles and administrators (Preview)		
Users and groups	Gatting Started	
Single sign-on	Getting Started	
Provisioning		
Self-service	💂 1. Assign users and groups 🤤 2. Set up single sign on 🤌 3. Provision User Accounts	4. Conditional Access
Security	Provide specific users and groups access Enable users to sign into their application You'll need to create user accounts in to the applications using their Azure AD credentials the application	Secure access to this application with a customizable access policy.
🝨 Conditional Access	Assign users and groups Get started Learn more	Create a policy
remissions		
Token encryption		
Activity	⊘ 5. Self service	
Sign-ins	Enable users to request access to the application using their Azure AD	
📸 Usage & insights	credentials Get started	
Audit logs		
Provisioning logs (Preview)		
S Access reviews	What's New	
	. 🤊 Sion in charts have moved	

5. Click on SAML.

■ Microsoft Azure		i i i i i i i i i i i i i i i i i i i
Home > > Enterprise applicat	ions >	
	gle sign-on "	Х
Coerview Coerview Deployment Plan Manage Properties Coners Reserved administrators (Preview)	Select a single sign-on method Help me decide Disable SAML Control of the selection of application is not enabled. The user work to able to launch the app from My Apps. SAML Same Linked Linked Linke of the back of the observation of application using the SAML (Security Assertion Markup Language) protocol. Control of the back of the observation is not enabled. The user and or office 365 speciation launcher.	
Users and groups		
Single sign-on		
Provisioning		
Self-service		
Security		
Conditional Access		
nermissions		
Token encryption		
Activity		
Sign-ins		
📸 Usage & insights		
Audit logs		
Provisioning logs (Preview)		
E Access reviews		

6. In the Basic SAML Configuration group, click on the Edit button.



7. Verify the following settings:

Field name	Value
Identifier (Entity ID)	urn:portal:webservices
Reply URL	https://secure.netop.com/saml

8. Click on the Save button to save your changes.

Basic SAML Configuration				×
☐ Save				
Identifier (Entity ID) * 🕕				
The default identifier will be the audience of the SAML response for IDP-initiated SSO				
	Defa	ult		
urn:portal:webservices	\checkmark	(i)	Î	
Reply URL (Assertion Consumer Service URL) * 🕕				
The default reply URL will be the destination in the SAML response for IDP-initiated SSO				
	Defa	ult		
https://secure.netop.com/saml	\checkmark	(i)	Î	
Sign on URL ①				
Enter a sign on URL			~	
Relay State 🕕				
Enter a relay state				
Logout Url 💿				
Enter a logout url			~	

9. In the User Attributes & Claims group, click on the Edit button.



10. Verify the following claims:

Name	Namespace	Source	Source attribute
NRC-ACCOUNT-ID	https://secure.netop.com	Attribute	This is the domain identifier that you
			both specify here and in the Netop
			Portal ADFS/Azure AD configuration.
NRC-USERNAME	https://secure.netop.com	Attribute	user.userprincipalname
NRC-GIVEN-NAME	https://secure.netop.com	Attribute	user.givenname
NRC-SURNAME	https://secure.netop.com	Attribute	user.surname
NRC-EMAIL	https://secure.netop.com	Attribute	user.mail

NOTE: When adding the **Netop Portal** application from the Azure AD Browse Application gallery section, the above claims are created automatically. The default attributed value to the NRC-ACCOUNT-ID user is set to "adfs-demo". Modify this value as per your requirements.

The following steps apply only if you want to use the Azure AD groups in the Netop Portal:

11. Click on the Add a group claim button to add the following Group claim:



11.1. Select the **All groups** option from the Which groups associated with the user should be

returned in the claim section.

	𝒫 Search resources, services, a	and docs (G+/)	📕 🛛 🛱 🖓 🕲 ? 😊 🛛 🧶
Home > > SAML-based Sign-on >			Group Claims ×
User Attributes & Claims			Manage the group claims used by Azure AD to populate SAML tokens issued to your app
+ Add new claim + Add a group claim ≣≣ Columns			Which groups associated with the user should be returned in the claim? None
Required claim			All groups
Claim name	Value		O Directory roles
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for		Groups assigned to the application
https://secure.netop.com/NRC-EMAIL	user.userprincipalname		Source attribute *
https://secure.netop.com/NRC-GIVEN-NAME	user.givenname		Group ID 🗸
https://secure.netop.com/NRC-SURNAME	user.sumame		Advanced options
https://secure.netop.com/NRC-USERNAME	user.userprincipalname		Customize the name of the group claim
nameidentifier	user.userprincipalname		Name (required)
https://secure.netop.com/NRC-ACCOUNT-ID	"netop"		Harre (required)
Additional claims			Namespace (optional)
Claim name	Value		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail		Emit groups as role claims
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname		
			Save

11.2. Click on the **Customize the name of the group claim.**

- 11.3. Specify the required name and namespace of the claim:
 - Name: NRC-GROUPS
 - Namespace: https://secure.netop.com

	crosoft Azure	₽ Search resources, services,	and docs (G+/)	🛛 🛱 🖓 🚳 ? 🙂
new dain + Add a group dain E Columns Whice youps associated with the user should be returned in the dain? at dain Intervention sare Value sciencentop com/NRC-DNRAL useruserprincipalname [nameid for.] carenetop com/NRC-SURJAME useruserprincipalname [nameid for.] tare value useruserprincipalname [> SAML-based Sign-on > Attributes & Claims …			Group Claims Manage the group claims used by Azure AD to populate SAML tokens issued to your app
addim Security groups me Valve user identifier Name (D) userusseprincipalname (nameid-for are) excure.netop.com/NRC-EMUAL userusseprincipalname are excure.netop.com/NRC-GVUSN-NAME userusseprincipalname excure.netop.com/NRC-GVUSN-NAME userusseprincipalname excure.netop.com/NRC-GVUSN-NAME userusseprincipalname excure.netop.com/NRC-GVUSN-NAME userusseprincipalname userusseprincipalname *** excure.netop.com/NRC-GVUSN-NAME userusseprincipalname userusseprincipalname *** excure.netop.com/NRC-GVUSN-NAME userusseprincipalname excure.netop.com/NRC-GVUSN-NAME userusseprincipalname <	new claim + Add a group claim == Columns			Which groups associated with the user should be returned in the claim? None Alternative
value value value User determine (panne) user superprincipalmane (name) d-m ··· vieur-netop com/NRC- MAUL user superprincipalmane ··· secure-netop com/NRC- MAUL user superprincipalmane ··· and ware ··· and ware ··· chemas.unicopa.pris/2005/05/detertity/claims/claims/claims/claims/mane user superprincipalmane user superprincipalmane user superprincipalmane ··· chemas.unicopa.pris/2005/05/detertity/claims/claims/claim	d claim	11-h-r		Security groups Directory roles
u bar die	name	value		Groups assigned to the application
x//xecure.netop.com/NRC-GNLAL user.userprincipalmame *** x//xecure.netop.com/NRC-GNLALALE user.givenname Group ID x//xecure.netop.com/NRC-SUBNAAE user.userprincipalmame *** eidentifier user.userprincipalmame *** eidentifier user.userprincipalmame *** total claims *** Sucreations total claims *** Namespace (optional) //xehmas.mitoop.org/wr/2005/05/dienth/(claim/amealladfress) user.userprincipalmame *** //xehmas.mitoop.org/wr/2005/05/dienth/(claim/amealladfress) user.userprincipalmame ***	ue User Identifier (Name ID)	user.userprincipalname [nameid-for		
v//sc/ure netop.com/NRC-SUBNAME user.givmame *** v//scure netop.com/NRC-SUBNAME user.suremino *** v//scure netop.com/NRC-SUBNAME user.suremino *** user.suremino user.suremino *** user.suremino view.suremino *** user.suremino *** Advanced options user.suremino *** *** user.suremino *** *** ional claims *** *** //schemas.sumlosop.org/w/2000/05/(dentrity/claim/umameladdress) user.seprino/splaname *** //schemas.sumlosop.org/w/2000/05/(dentrity/claim/umameladdress) user.seprino/splaname *** //schemas.sumlosop.org/w/2000/05/(dentrity/claim/umameladdress) user.seprino/splaname ***	://secure.netop.com/NRC-EMAIL	user.userprincipalname		Source attribute *
kg/kgcurnetcp.com/NRC-SUBIAME user.summe *** Advanced options kg/kgcurnetcp.com/NRC-SUBIAME user.userprincipalmame *** kg/kgcurnetcp.com/NRC-VACCOUNT-ID 'netop' *** kg/kgcurnetcp.com/NRC-VACCOUNT-ID 'netop' *** total claims 'netop' *** mame Value *** kg/kgenamitopa.org/ws/2005/05/detthg/(daims/emailaddress) user.userprincipalmame *** kg/kemas.umitopa.org/ws/2005/05/detthg/(daims/emailaddress) user.userprincipalmame ***	is://secure.netop.com/NRC-GIVEN-NAME	user.givenname		Group to
Image: Marked poor (NRC-USERNAME) user.userprincipalname *** Nade refip.com (NRC-USERNAME) user.userprincipalname *** Name (required) *** Name (required) includians *** Name (required) mame Value *** //chemasumsloop.org/vs/2005/S/dethtly/claim/(shemame) *** user.umsloop.org/vs/2005/S/dethtly/claim/(shemame) *** //chemasumsloop.org/vs/2005/S/dethtly/claim/(shemame) *** //chemasumsloop.org/vs/2005/S/dethtly/claim/(shemame) ***	is://secure.netop.com/NRC-SURNAME	user.surname		Advanced options
neidentifier user_userprincipalmane *** ps://scure.netpp.com/NRC-ACCCUNT-ID *netp* *** intane Value *** intane Value *** //schemas.milscap.org/ws/2005/05/diettity/claim/yemaladdress user_userant *** //schemas.milscap.org/ws/2005/05/diettity/claim/yemaladdress user_userant *** //schemas.milscap.org/ws/2005/05/diettity/claim/yemaladdress user_userant *** //schemas.milscap.org/ws/2005/05/diettity/claim/yemane user_userant ***	ps://secure.netop.com/NRC-USERNAME	user.userprincipalname		Customize the name of the group claim
ps://scure.net.op.com/NRC-ACCOUNT-ID *net.op* itional claims *** im name Value //schemas.smlscap.org/w2005/05//dettify/claim/yemaldedress user.nall user.green.meter.ps.com/yand/op/05//dettify/claim/yemane user.green.meter //schemas.smlscap.org/w2005/05//dettify/claim/yemane user.userprincipalmame //schemas.mlscap.org/w2005/05//dettify/claim/yemane user.userprincipalmame user.userprincipalmame ***	neidentifier	user.userprincipalname		Name (required)
International claims Namespace (optional) inname Value p/Johenas.umitosop org/w/2005/05/jolentity/claims/yremane uer_unal uer_unamicop org/w/2005/05/jolentity/claims/uname uer_uname usr_uname uer_uname usr_uname uer_uname usr_uname uer_uname usr_uname uer_uname usr_uname uer_uname usr_uname uer_uname	ps://secure.netop.com/NRC-ACCOUNT-ID	"netop"		
immane Value p//schemas.xmlscap.org/wr/2005/05/identhly/claims/pianname user.mail p//schemas.xmlscap.org/wr/2005/05/identhly/claims/givenname user.givenname v//schemas.xmlscap.org/wr/2005/05/identhly/claims/yclaims/givenname user.givenname v//schemas.xmlscap.org/wr/2005/05/identhly/claims/yclaims/givenname user.sursenprincipalname user.givenname user.sursenprincipalname	ditional claims			Namespace (optional)
p://schemas.smlscap.org/w2/005/05/identity/claims/emailaddress user.mail ··· p://schemas.smlscap.org/w2/005/05/identity/claims/givenname user.givenname ··· p://schemas.smlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/05/identity/claims/schemas.mlscap.org/w2/005/identity/claims/schemas.mlscap.org/w2/005/identity/claims/schemas.mlscap.org/w2/005/identity/claims/schemas.mlscap.org/w2/005/identity/claims/schemas.mlscap.org/w2/005/identity/claims/schemas.mlscap.org/w2/005/identity/claims/schemas.mlscap.org/w2/005/identity/claims/schemas.mlscap.org/w2/005/identity/claims/schemas.mlscap.org/w2/005/identity/claims/schemas.mlscap.mlsca	aim name	Value		
p://schemas.umilsoap.org/wr/2005/05/identifiy/claims/givenname user.givenname ••• p://schemas.umilsoap.org/wr/2005/05/identifiy/claims/rumme user.user.principalname ••• p://schemas.umilsoap.org/wr/2005/05/identifiy/claims/rumme user.urmme •••	tp://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail		Emit groups as role claims ①
p://schemas.umisoap.org/wr/2005/05/dentitiy/claims/rvame useruserprincipalname *** z//schemas.umisoap.org/wr/2005/05/dentitiy/claims/sunname user.surname ***	tp://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname		
z//schemas.xmlsoap.org/ws/2005/05/identh/claims/sumame user.sumame ***	tp://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname		
	tp://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname		
				Save

12. Click on the Save button to save your changes.

Home > > SAML-based Sign-on > User Attributes & Claims ··· Marage the group claim used by Abure AD to populate SAML taken issued to your app + add new claim + add a group claim EE Columns ···· Required claim ···· Claim name Value Unique User identifier (hame ID) user userprincipaliname (namei-id-cr	■ Microsoft Azure	𝒫 Search resources, services, and	*/
User Attributes & Claims + dafa new daim + dafa new daim Required daim Caim name Vinique User steeting for NNRC- SURVAK Autor Survational Damain dama Vinique User steeting for NNRC- SURVAK Autor Survational Damain dama Vinique User steeting for NNRC- SURVAK Autor Survational Damain dama Vinique User steeting for NNRC- SURVAK Autor Survational Damain dama Vinique User steeting for NNRC- SURVAK Autor Survational Damain dama Vinique User steeting for NNRC- SURVAK Autor Survational Damain dama Vinique User steeting for NNRC- SURVAK Autor Survational Damain dama Inttp://score.netop.com/NRC- SURVAK Autor Survational Dama Inttp://score.netop.com/NRC- Survational	Home > > SAML-based Sign-on >		Group Claims
+ dd new dain + dd a group dain Required claim Claim name Unique User identifier (hame 10) user user principal name [nameid-for	User Attributes & Claims		Manage the group claims used by Azure AD to populate SAML tokens issued to your app
Required claim Image: Security claims	+ Add new claim + Add a group claim ≣≣ Columns		Which groups associated with the user should be returned in the claim?
Claim name Value Unique User identifiér (Name ID) user userprincipalname (nameid-sc	Required claim		All groups Security groups
Unique User identifier (Name (D) user susprincipalaname (maneid-for	Claim name	Value	Ground assigned to the application
http://scure.netop.com/NRC-SHARL user.useprincipalname ••• http://scure.netop.com/NRC-SHARL user.gename Intro-Structure http://scure.netop.com/NRC-SHARL user.gename ••• http://scure.netop.com/NRC-SHARLAME user.useprincipalname ••• intp://scure.netop.com/NRC-SHARLAME user.useprincipalname ••• intp://scure.netop.com/NRC-ACCOUNT-ID ••• Advanced options Additional claims ••• ••• Additional claims user.mail ••• http://scure.netop.com/NRC-ACCOUNT-ID valer ••• http://scure.netop.com/NRC-ACCOUNT-ID valer ••• Additional claims ••• ••• intp://scure.netop.com/NRC-ACCOUNT-ID user.mail ••• http://scure.netop.com/NRC-ACCOUNT-ID valer ••• Additional claims user.mail ••• http://scure.netop.com/Sci.destify/claims/jename user.mail ••• http://scure.netop.com/sci.destify.diams/jename ••• ••• http://scure.netop.com/sci.destify.diams/jename ••• •••	Unique User Identifier (Name ID)	user.userprincipalname [nameid-for **	
http://scure.netop.com/NRC-GVEN-VAME uar givenname ••• http://scure.netop.com/NRC-GVEN-VAME uars.umpane ••• http://scure.netop.com/NRC-GVEN-VAME uars.umpane ••• http://scure.netop.com/NRC-GVEN-VAME uars.umpane ••• http://scure.netop.com/NRC-GVEN-VAME uars.useprincipalname ••• http://scure.netop.com/NRC-ACCOUNT-ID •••top* ••• Additional claims ••• ••• http://scure.netop.com/NRC-ACCOUNT-ID value ••• http://scure.netop.com/NRC-ACCOUNT-ID ••• ••• Additional claims uars.maidentified uars.maidentified uars.maidentified http://scure.netop.com/NRC-ACCOUNT-ID value ••• ••• http://scure.netop.com/NRC-ACCOUNT-ID uars.maidentified ••• http://scure.netop.com/net	https://secure.netop.com/NRC-EMAIL	user.userprincipalname	Source attribute *
Intp://keure.neto.com/NRC-USERVAAME uars.umame *** http://keure.neto.com/NRC-USERVAAME uer.useprincipalname *** rameidentifier user.useprincipalname *** http://keure.neto.com/NRC-USERVAAME user.useprincipalname *** http://keure.neto.com/NRC-USERVAAME user.useprincipalname *** Additional claims *** Name tequined) Additional claims user.useprincipalname *** http://keure.neto.com/NRC-USERVAAME user.mail Name tequined) Linkmance variational of the group claim Name tequined) Intp://keure.neto.com/NRC-USERVAAME user.mail Name tequined) http://keure.neto.com/NRC-USERVAAME user.mail Name tequined) Intp://keure.neto.com/NRC-USERVAAME user.mail ***	https://secure.netop.com/NRC-GIVEN-NAME	user.givenname **	Group ID
http://kBcure.netop.com/NRC-USERNAME uar.userprincipalmame ••• namidentifier uar.userprincipalmame ••• http://kBcure.netop.com/NRC-USERNAME uar.userprincipalmame ••• Additional claims ••• Name (required) [mc::GROUPS Claim ame Vale ••• http://schemas.mitoop.org/wr/2005/05/dentity/claims/periame user gename ••• http://schemas.mitoop.org/wr/2005/05/dentity/claims/periame user gename •••	https://secure.netop.com/NRC-SURNAME	user.sumame **	Advanced options
nameidentifier user userprincipalname *** http://secure.netop.com/NRC-ACCOUNT-ID *netop* *** Additional claims	https://secure.netop.com/NRC-USERNAME	user.userprincipalname	Customize the name of the group claim
https://scure.netop.com/NRC-ACCOUNT-ID *netop* *netop* *netop* Additional claims Immergane (optional) Immergane (optional) Claim name Value Immergane (optional) http://schemas.mlioog.org/nrk/2005/05/identity/claims/guemame user.mail *** http://schemas.mlioog.org/nrk/2005/05/identity/claims/guemame user.user.mail *** http://schemas.mlioog.org/nrk/2005/05/identity/claims/guemame user.user.mail ***	nameidentifier	user.userprincipalname	line (main)
Additional claims value Interpret (optional) tip/schemss.mikosp.org/ws/2005/05/identity/claims/gename user mail Interpret (optional) http://schemss.mikosp.org/ws/2005/05/identity/claims/gename user givename Interpret (optional) http://schemss.mikosp.org/ws/2005/05/identity/claims/gename user givename Interpret (optional) http://schemss.mikosp.org/ws/2005/05/identity/claims/gename user givename Interpret (optional) http://schemss.mikosp.org/ws/2005/05/identity/claims/gename user superincipalme Interpret (optional)	https://secure.netop.com/NRC-ACCOUNT-ID	"netop"	NRC-GROUPS
Claim name Value Interprise Interprise http://schemas.mlikoap.org/ws/2005/05/identiti/claims/guemane user mail http://schemas.mlikoap.org/ws/2005/05/identiti/claims/guemane user guemane http://schemas.mlikoap.org/ws/2005/05/identiti/claims/unrame user guerincipalname http://schemas.mlikoap.org/ws/2005/05/identiti/claims/unrame user guerincipalname	Additional claims		Namespace (optional)
http://schemas.smlkoap.org/ws/2005/05/dentity/claims/genalladdress user.mail Image: Control of the second	Claim name	Value	https://secure.netop.com
http://schemas.xmliscap.org/ws/2005/05/identify/claims/givenname user givenname ••• http://schemas.xmliscap.org/ws/2005/05/identify/claims/name user userprincipalname ••• http://schemas.xmliscap.org/ws/2005/05/identify/claims/name user userprincipalname •••	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail **	Emit groups as role claims 💿
http://schemas.xmlscap.org/ws/2005/05/identify/claims/name useruserprincipalname ***	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname **	
http://chemas.vm/scan.org/asc/2005/05/deltiti//claims/sumame user.sumame ***	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.sumame ···	
			Save

NOTE: Make sure that you save the following information:

• The Federation Metadata XML file

Status	Active
Thumbprint	70F19DDC96EB823EEECD2E9BF8A750A961F0E0F6
Expiration	4/2/2023, 12:32:08 PM
Notification Email	andrei@nrcazuretest.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/cd5f608a-30
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

• The Login URL

/ou'll need to configure the appli	cation to link with Azure AD.
Login URL	https://login.microsoftonline.com/cd5f608a-30
Azure AD Identifier	https://sts.windows.net/cd5f608a-30a6-4ec3-b
Logout URL	https://login.microsoftonline.com/common/wsf

If you plan on using the Azure AD groups then it is necessary that you also save the Application ID

• Application ID

To retrieve the Application ID value from the Azure Portal, proceed as follows:

- 1.1. Go to the **Azure Portal**.
- 1.2. Go to Windows Active Directory.

- 1.3. Go to Enterprise Applications.
- 1.4. Select the Netop Portal application.
- 1.5. Go to **Overview**.
- 1.6. Click on the Copy to clipboard button.



Configure the application permissions

The following steps apply only if you want to use the Azure AD groups in the Netop Portal.

To configure the application permissions, proceed as follows:

- 1. Go to Azure Active Directory.
- 2. Go to App registrations.



3. Click on the Netop Portal application.



4. Click on the View API permissions button.



Configured permissic	ns			
Applications are authorize all the permissions the ap	d to call APIs when t plication needs. Lear	ney are granted permis n more about permissio	sions by users/admins as part of the consent process. The list of com	figured permissions should include
+ Add a permission	Grant admir	n consent for home		
	Add a permission			
API / Permissions r	name Type	Description	Admin consent req	Status
No permissions added				

6. Click on Microsoft Graph.



7. Click on Application permissions.

	∠P Search resources, services, and docs (G+/)		5 G 🖗 🤗 🐵 ? 🐵	0
Home > > >	API permissions 🛷 …	Request API permissions		×
Search (Ctrl+/) « Overview	🕐 Refesh 🗢 Got feedback?	Microsoft Graph https://graph.microsoft.com/ Docs 🔊		
🚳 Quickstart 💉 Integration assistant	The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permissio	Delegated permissions does your application requires Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a	
Manage Branding Authentication Certificates & secrets	Configured permissions Applications are authorized to all APIs when they are granted permissions by usery/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and content + Add a permission \checkmark Grant admin consent for netopue		agree in each	J
Token configuration	API / Permissions name Type Description Admin consent req			
 API permissions Expose an API 	No permissions added			
App rolesOwners	To view and manage permissions and user consent, try Enterprise applications.			
 Roles and administrators Preview Manifest 				
Support + Troubleshooting				
New support request				
		Add permissions Discard		

8. Search for Group in the Start typing a reply url to filter these results search field.

	∠ Search resources, services, and docs (G+/)		E & 🖓 🕸 ? 🙂 🛛 🙆
Home>>>	API permissions 🖋 …	Request API permissions	×
Search (Ctrl+/) W Overview	O Refresh ♥ Got feedback?	Microsoft Graph https://graph.microsoft.com/ Docs 💣 What type of permissions does your application require?	
 Quickstart Integration assistant 	The "Admin content required" column shows the default value for an organization. However, user consent can be outtomized per permissio	Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
Manage Branding Authentication	Configured permissions Applications are authorized to call APs when they are granted permissions by users/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and consent	Select permissions	expand all
Certificates & secrets Token configuration	Add a permission Grant admin consent for netopse API / Permissions name Type Description Admin consent req No supportione added	Start (yoing a reply on to nice mean results Permission AccessReview	Admin consent required
API permissions Expose an API App roles	To view and manage permissions and user consent, try Enterprise applications.	> AdministrativeUnit	
Owners Roles and administrators Preview Monifect		Agreement Agreement	
Support + Troubleshooting		APIConnectors	
New support request		AppRoleAssignment	
		ApprovalRequest	
		/ Audatog	

Add permissions Discard

9. Click on the Group.Read.All option.

	∠ Search resources, services, and docs (G+/)		_ E 🗣 🖉 🎯 ? 🙂 🛛 🐣
Home > > 	API permissions & ···· · · · · · · · · · · · · · · · ·	Request API permissions	×
 Overview Quickstart Integration assistant 	The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permissio	What type of permissions does your application require? Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
Manage Branding Authentication Certificates & secrets	Contigured permission all APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the permission we application needs. Learn more about permissions and consent + Add a permission \checkmark Grant admin consent for netop.se API / Permissions name Type Description Admin consent req.	Select permissions P Group Permission	erpand all ×
API permissions Expose an API App roles	No permissions added To view and manage permissions and user consent, try Enterprise applications.	Calls Coup Group Group	
 Owners Roles and administrators Preview Manifest 		Create arcurs Group.Read.All ① Read all groups Group.ReadWirte.All ①	Ves Ves Ves
Support + Troubleshooting Image: Troubleshooting Image: New support request		Kead and write all groups GroupMember PrivilegedAccess	
		Add permissions Discard	

10. Click on the Add permissions button to add your permission.

■ Microsoft Azure	P Search resources, services, and docs (G+/)		D 🖟 🖓 @ ? © 🛛 🙆
Home > >	API permissions 🖈 …	Request API permissions	×
Search (Ctrl+/) « Overview	🖒 Refresh 🗢 Got feetback?	Microsoft Graph https://graph.microsoft.com/ Docs c [*] What type of permissions does your application require?	
 Quickstant Integration assistant 	The 'Admin consent required' column shows the default value for an organization. However, user consent can be outomized per permission Conselferunced exempleciance	Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
Branding	Computer permissions Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and consent	Select permissions	expand all
Certificates & secrets Token configuration	Add a permission	Permission	Admin consent required
 API permissions 	No permissions added	> Calls	
 Expose an API App roles 	To view and manage permissions and user consent, try Enterprise applications.	Group (1)	
A Owners		Create groups	Yes
Manifest		Read all groups	Yes
Support + Troubleshooting		Read and write all groups	Yes
 P Troubleshooting New support request 		GroupMember PrivilegedAccess	
		Add permissions	

11. Click on the Grant admin consent for ... button to grant admin consent for the API permission.

Microsoft Azure	∠P Search resources, services, and docs (G+/)		D G G O C	. 0
Home > >				
-9-	\$ ² ···			\times
	🖒 Refresh 🛛 🗢 Got feedback?			
Uverview Overview	A You are editing permission(s) to your application, users will have to consent even if they've already done so	o previously.		
Quickstart				
💉 Integration assistant				U
Manage	1 The "Admin consent required" column shows the default value for an organization. However, user consent	t can be customized per permission, user, or app. This column may not reflect the value	in your organization, or in organizations where this app will be used. Learn more	^
Branding	Configured permissions			
Authentication	Applications are authorized to call APIs when they are granted permissions by users/admins as part of the	e consent process. The list of configured permissions should include		
📍 Certificates & secrets	all the permissions the application needs. Learn more about permissions and consent			
Token configuration	+ Add a permission 🗸 Grant admin consent for			
 API permissions 	API / Permissions name Type Description	Admin consent req Status		
Expose an API	Microsoft Graph (1)			
App roles	Group.Read.All Application Read all groups	Yes 🔥 Not granted for netop.se •••		
🚑 Owners				
Boles and administrators Preview	To view and manage permissions and user consent, try Enterprise applications.			
Manifest				
Support + Troubleshooting				
Troubleshooting				
New support request				

Configure Certificates & secrets

The following steps apply only if you want to use the Azure AD groups in the Netop Portal.

To configure the **Certificates & secrets** for the **Netop Portal** application in the **Azure Portal**, proceed as follows:

- 1. Go to Azure Active Directory.
- 2. Go to App registrations.
- 3. Click on the Netop Portal application.

4. Go to Certificates & secrets.

	$\mathcal P$ Search resources, services, and docs (G+/)		E 🗣 Q 🕸 ? ©	
Home > >				
*				\times
	🗴 Delete 🜐 Endpoints 🙃 Preview features			
Overview	∧ Essentials			^
📣 Quickstart	Display name : Netop Portal 2	Supported account types : My organization only		- 1
💉 Integration assistant	Application (client) ID : 0ddeaed9-3fe0-4a32-97ca-515ccb3d6d94	Redirect URIs : 1 web, 0 spa, 0 public client		
	Directory (tenant) ID : 82cdc9a9-7de3-42c9-ac33-4d0c848ba5d5	Application ID URI : Add an Application ID URI		- 1
Manage	Object ID : ea915fe8-a845-42b6-8e8f-10d51bf1533e	Managed application in I : Netop Portal 2		- 1
Branding	1 Starting June 30th. 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. Wi	e will continue to provide technical support and security updates but we will no	o longer provide feature updates. Applications will need to be	×
Authentication	upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more			
📍 Certificates & secrets				- 1
Token configuration	Call APIs	Documentation		- 1
 API permissions 		Microsoft identity platform		
Expose an API	📥 🙉 🛶 🏴 📧	Authentication scenarios		
App roles		Code samples		- 1
A Owners		Microsoft Graph Glossary		- 1
👃 Roles and administrators Preview		Help and Support		- 1
Manifest	Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.			- 1
Support + Troubleshooting	View API permissions			- 1
/ Troubleshooting				- 1
New support request				- 1
	Sign in users in 5 minutes			
	A CONTRACTOR			

5. Click on the **New client secret** button.

Microsoft Azure P Search resources, services, and docs (6+/)
Nome > >>
Certificates & secrets
P Search (Ctr(+)) ≪ ♥ Got feedback?
Overview Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS
Scheme). For a higher level of assurance, we recommend using a certificate (initead of a client secret) as a credential.
✓ Integration assistant Certificates
Manage Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.
E Branding
3 Authentication ↑ Upload certificate
Certificates & secrets Thumbprint Start date Expires ID
II Token configuration No certificates have been added for this application.
API permissions
👄 Expose an API
職 App roles Client secrets
Owners A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
a Roles and administrators Preview
Manifest Development accent accent Section Union
UPEX.rptuon capites value ID
Troubleshooting No client secrets have been created for this application.
R New support request

- 6. Specify a name for the client secret in the **Description** entry field.
- 7. Specify an expiry date for the client secret accordingly to your needs.

8. Click on the Add button.

	,P Search resources, services, and docs (G+/)	e 🗣 o 🎯 ? © 🛛 🧶
Home > > > Ce	tificates & secrets 👒 …	×
P Search (Ctrl+/) ≪	♥ Got feedback?	
Council of the second	Add a client secret Description Netop Portal Expires in 1 year in 2 years Never Add Cancel Cancel	
API permissions Expose an API	Add	
App roles Owners Roles and administrators Preview	Client secrets A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password. + New client secret	
Support + Troubleshooting	Description Expires Value ID No client secrets have been created for this application.	

 Save the client secret value in a text editor or copy it to the clipboard. It is necessary for you to do so, because once you leave this particular page the value will no longer be available for display in plain text.

			3+/)				7 🖓 🐵 ? © 🛛 🧶
Home > netop.se > Netop Portal Beta	Test Test Certificates & secrets	¢					Update application credentials 4:47 PM Successfully updated application Netop Portal Beta Test credentials
	♡ Got feedback?						
Overview	Copy the new client secret value. You won'	t be able to retrieve it after you perform another	operation or leave this b	ade.			
1 Integration assistant	Credentials enable confidential applications to scheme). For a higher level of assurance, we re	identify themselves to the authentication ser commend using a certificate (instead of a clie	vice when receiving tok ent secret) as a credenti	ens at a web addressab al.	le location (using an HTTPS		
Manage	Certificates						
Authentication	Certificates can be used as secrets to prove the	application's identity when requesting a tok	en. Also can be referred	to as public keys.			
📍 Certificates & secrets	Upload certificate						
 Token configuration API permissions 	Thumbprint	Start date	Expires	ID			
 Expose an API 	No certificates have been added for this applic	ation.					
K App roles							
Owners A Roles and administrators Preview	Client secrets						
Manifest	A secret string that the application uses to pro	ve its identity when requesting a token. Also	can be referred to as ap	pplication password.			
Support + Troubleshooting	+ New client secret			_			
Troubleshooting	Description	Expires Value		ID			
New support request	Netop Portal	3/24/2022 B		D	D 🔋		

B. Creating the Netop Portal application Azure AD as a Non-gallery application

To create the **Netop Portal** application in **Azure AD**, proceed as follows:

1. Log in the <u>Azure Portal</u>.

=	Microsoft Azure	,P: Search resources, services, and docs (G+)/	🖸 🕼 O	@ ? ©	
		Welcome to Azure! Don't have a subscription? Check out the following options.			ĺ
		Start with an Azure free trial Manage Azure Active Directory Access student benefits Get \$200 free credit toward Azure products and services, plus 12 months of popular free services. Manage access, set smart policies, and enhance security with Azure Active Directory. Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.			
		Start Learn more d' View Learn more d' Explore Learn more d'			
		Azure services			
		+ 🚸 📮 🕲 🖬 🖉 🐲 →			
		Create a Azure Active Virtual App Services Storage SQL databases Azure Database Azure Cosmos Kubernetes More services resource Directory machines accounts for PostgreSQ DB services			
		Navigate			
		🛉 Subscriptions. 😥 Resource groups 🇱 All resources 🔯 Dashboard			
		Tools			
		Microsoft Learn C2 Earn RAINE Azure Monitor Security Center Security Center Cold Management Learn Azure with free online training from Microsoft Monitor your apps and infrastructure Security Center Security Center Security Center Cold Management			

- 2. Go to Azure Active Directory.
 - 2.1. Click on the **More** button.

Microsoft Azure	(P) Search resources; services; and docs (G+/)	9 ? ©	8
	Welcome to Azure! Don't have a subscription? Check out the following options.		ĺ
	Start with an Azure free trial Manage Azure Active Directory Access student benefits Get \$200 free credit toward Azure products and services. Manage Azure Active Directory. Get free software, Azure credit, or access Azure Dev tools for Teaching after you verify your academic status.		
	Start Learn more D ⁴ View Learn more D ⁴ Explore Learn more D ⁴		
	Azure services		
	Navigate		
	🕈 Subscriptions. 🔘 Resource groups 🇱 All resources 🔯 Dashboard		- 1
	Tools		
	Microsoft Learn C* Azure Wonkor Azure Monitor Octom 200 Security Center Security Center <th></th> <th></th>		

2.2. Click on Azure Active Directory.

=	P Search resources, services, and docs (G+/)	5 6 4 0 7 C	
+ Hide portal menu			
A Home	Welcome to Azure!		
Dashboard	Don't have a subscription? Check out the following options.		
E All services			
* FAVORITES			
All resources			
(iii) Resource groups			
App Services			
🤣 Function App			
😇 SQL databases			
S Azure Cosmos DB	Start with an Azure free trial Manage Azure Active Directory Access student benefits		
Virtual machines	Get \$200 free credit toward Azure products and services, Manage access; set smart policies, and enhance security Get free software, Azure credit, or access Azure Dev Tools on the software access and the software access and the software access access and the software access a		
💠 Load balancers	plus to meaning aner you vering your exagenic status.		
Storage accounts	Cean more B Cean more B Cean more B		
Virtual networks			
Azure Active Directory	Azure services		
C Monitor			
Advisor	Create a Anure Artive Virtual Ann Senires Storane SOI databases Anure Database Anure Cosmos Kubernetes More senires		
Security Center	resource Directory machines accounts for Postgre5Q DB services		
O Cost Management + Billing			
Help + support	Navigate		
	📍 Subscriptions 🛛 😥 Resource groups 🗱 All resources 🛛 Dashboard		
	Tools		
	1995		
	🖬 Microsoft Learn 👌 🛞 Azure Monitor 👩 Security Center 😭 Cost Management		
	Learn Azure with free online Monitor your apps and Secure your apps and Analyze and optimize your training from Microsoft infrastructure infrastructure cloud spend for free		

3. Go to Enterprise applications.

=	Microsoft Azure		Search resources, services, and docs (G+/)		5 G 🗘 🖉 🐵 ? 😊	0
Hom						
0	Overview				>	<
	*	👁 Switch tenant 📋 Delete tenant 🕂 Cr	sate a tenant 🛛 What's new 🛛 💀 Preview	features 🛛 🛇 Got feedback?		
0 C	verview					^
🤊 G	etting started	 Azure Active Directory can help you enable re 	mote work for your employees and partners. Learn m	ore	×	
I P	review features					
× D	iagnose and solve problems	netop.es				
Mana	ge	Search your tenant				
Δ. υ	sers					
🎒 G	roups	Tenant information	💝 Azure AD Connect			
🕕 E	dernal Identities	Your role	Status			
🕹 R	oles and administrators	Global administrator More info	Enabled			
🙇 A	dministrative units	License Amure AD Free	Last sync			
👪 E	nterprise applications	Tenant ID	Less than 1 hour ago			
i	evices	C				
🔜 A	pp registrations	Primary domain				
🎒 lo	lentity Governance	netop.es				
₿ A	pplication proxy					
🔒 Li	censes	Sign-ins				
🔶 A	zure AD Connect					
P 0	ustom domain names			Looks like the sign-in data is unavailable. Try again later.		
(2) N	tobility (MDM and MAM)					
📍 P	assword reset					
II c	ompany branding					
🥭 U	ser settings					
P	roperties	Create				
🛡 s	ecurity		24			
https://p	ortal azure com/#blade/Microsoft ۵۵D 161	M/ArtiveDirecton/MenuRlade/EnternriseAnns	Conun Catamaira An	n rasistañan		

4. Click on the **New application** button.

■ Microsoft Azure		Search resources, services, and docs (G+/)		D & © ? O	
Home > > Enterprise applica	itions				
Enterprise applicat	ions All applications				×
« Overview	+ New application	Preview features 🛛 🛇 Got feedback?			
0 Overview	Try out the new Enterprise Apps search previ	ewl Click to enable the preview. \rightarrow			
X Diagnose and solve problems Manage	Application type Application Enterprise Applications Applications	ns status Application visibility Any Apply	Raset		
All applications	₽ First 50 shown, to search all of your applicat	ions, enter a display name or the application ID.			
Application proxy	Name	Homepage URL	Object ID	Application ID	
User settings	0				
Security	b				
Conditional Access					
Consent and permissions					
Activity					
Sign-ins					
🕍 Usage & insights					
Audit logs					
Provisioning logs (Preview)					
E Access reviews					
Admin consent requests (Preview)					
Troubleshooting + Support					
🖤 Virtual assistant (Preview)					
New support request					

5. Click on the **Create your own application** button.

Microsoft Azure	P Search resources, services, and docs (G+/)		E 🛱 🗳 🍏 ? 😳
Home > > Enterprise applications >			
Browse Azure AD Gallery			
+ Create your own application 🛈 Request new gallery app 📋 🛇 Got fe	edback?		
You're in the new and improved app gallery experience. Click here to switch back	to the legacy app gallery experience. $ ightarrow$		
Search application Single Sign-on : All	User Account Management : All Categories : All		
Cloud platforms			
Amazon Web Services (AWS) Ge	ogle Cloud Platform Oracle	SAP	
aws		SAP	
	Google Cloud		
On-premises applications			
Add an on-premises application Configure Azure AD Application Proxy to enable secure remote	Learn about Application Proxy Learn how to use Application Proxy to provide secure remote access	Manage Application Proxy connectors Connectors are lightweight agents that sit on-premises and facilitate	
access.	to your on-premises applications.	the outbound connection to the Application Proxy service.	
➔ Federated SSO ② Provisioning			

6. Specify a name for the application in the Input name entry field.

Microsoft Azure	₽ Search resources, services, and docs (G+/)		📃 🛛 💀 🖓 🎯 ? 🙄
e > > Enterprise applications > owse Azure AD Gallery			Create your own application
Create your own application ① Request new callery app	S Got feedback?		What's the name of your app?
You're in the new and immoved ann nallery experience Click he	re to switch hack to the lenary ann nallery evolutions		Input name
Search application Single	Sign-on ; All User Account Management : All Categories : All		What are you looking to do with your application? C Configure Application Proxy for secure remote access to an on-premises application Register an application to integrate with Azure AD (App you're developing) integrate any other application you don't find in the gallery (Non-gallery)
loud platforms			
Amazon Web Services (AWS)	Google Cloud Platform Oracle	le SAP	
aws	<u> </u>	SAD	
	Google Cloud		
)n-premises applications			
Add an on-premises application	Learn about Application Proxy	Manage Application Proxy connectors	
Configure Azure AD Application Proxy to enable secure remote access.	Learn how to use Application Proxy to provide secure remote access to your on-premises applications.	Connectors are lightweight agents that sit on-premises and facilit the outbound connection to the Application Proxy service.	2
Federated SSO (2) Provisioning			
•			
eatured applications			

7. Click on the **Create** button to finish adding the Netop Portal application the **Azure Portal**.

Microsoft Azure	P Search resources, services, a	and docs (G+/)		
rowse Azure AD Gallery				Create your own application
Create your own application 🛈 Request new gallery ap	op 🛛 🛇 Got feedback?			What's the name of your app? Netop Portal
You're in the new and improved app gallery experience. Click	: here to switch back to the legacy app gallery experience. $ imes$			What are you looking to do with your application?
P Search application Sing	gle Sign-on : All User Account Management : All	Categories : All		Configure Application Proxy for secure remote access to an on-premises appli Register an application to integrate with Azure AD (App you're developing) Integrate any other application you don't find in the gallery (Non-gallery)
Amazon Web Services (AWS)	Goode Cloud Platform	Orașle		We found the following applications that may match your entry We recommend using gallery applications when possible.
	Google cloud Platform	oracie		SAP
aws	Google Cloud			SAP returner Netop Portal COOP Octo Portal COOP Octo Portal
On-premises applications	Google Cloud			SAP extension Netop Portal Coeo Portal Coeo Portal
On-premises applications	Google Cloud		Manage Application Proxy connect	SAP exercise Netop Portal Coeo Portal Coeo Portal Coeo Portal Coeo Portal
On-premises applications Add an on-premises application Provy to enable secure rem Access.	Coogle Cloud Pations Google Cloud		Anage Application Proxy connector Connector are lightweight agents that shor the outdourd connection to the Application	SAP Interview Netop Portal Coes Portal Coes Portal Coes Portal Provide Statist

The application is created successfully and added to the **Enterprise applications** section.

Add users and groups to the application

To add users and groups to the application, proceed as follows:

- 1. Go to Azure Active Directory.
- 2. Go to Enterprise applications.

3. Click on the newly created **Netop Portal** application.

Microsoft Azure		℅ Search resources, services, and docs (G+/)		国 時 阜 〇 ? 〇
Home > Enterprise applica	ations			
Enterprise applicat	tions All applications			
« Overview	+ New application III Columns	B Preview features Office Got feedback?		
Overview	Try out the new Enterprise Apps search	a preview! Click to enable the preview. $ ightarrow$		
X Diagnose and solve problems	Application type App Enterprise Applications V	lications status Application visibility 1/2 Any Apply	Reset	
All applications	P First 50 shown, to search all of your a	oplications, enter a display name or the application ID.		
Application proxy	Name	Homepage URL	Object ID	Application ID
User settings	Netop Portal			
Security	6			
Conditional Access				
Consent and permissions				
Activity				
Sign-ins				
📫 Usage & insights				
Audit logs				
Provisioning logs (Preview)				
Access reviews				
Admin consent requests (Preview)				
Troubleshooting + Support				
🕎 Virtual assistant (Preview)				
New support request				

4. Click on Assign users and groups.

≡	Microsoft Azure		Search resources, services, and docs (G+/)	D 6 4 0 ? ©
Hon	me > > Enterprise applicati	ions >		
	Netop Portal Overv	view		×
- 15	Overview	Properties		
Ш	Deployment Plan	Name 💿		
Man	nage	Netop Portal		
8	Properties	Application ID () 490895eb+ee5d+4583-b9e8		
24	Owners	Object ID ①		
4	Roles and administrators (Preview)	ae5f65a5-69a9-4d51-9ecb 🗈		
24	Users and groups	Getting Started		
•	Single sign-on	o thing blan to a		
Ф	Provisioning			
-	Application proxy	1. Assign users and groups	2. Set up single sign on 3. Provision User Accounts	4. Conditional Access
0	Self-service	Provide specific users and group to the applications	ccess Enable users to sign into their application Automatically create and delete user using their Azure AD credentials accounts in the application	Secure access to this application with a customizable access policy.
Secu	urity	Assign users and groups	Get started Get started	Create a policy
•	Conditional Access			
4	Permissions			
۲	Token encryption	😔 5. Self service		
Activ	vity	Enable users to request access to application using their Azure AD		
•	Sign-ins	Get started		
άź.	Usage & insights			
	Audit logs			
2	Provisioning logs (Preview)	What's New		
£	Access reviews	Sign in charts have moved! The new Insights view shows sign in info	ong with other useful application data. View insights	
		Delete Application has moved to You can now delete your application from	roperties e Properties page. View properties	

5. Click on the Add User button to add the allowed users or groups.

■ Microsoft Azure	₽ Search resources, services, and d	ocs (G+/)	N 🛱 L 🐵 ? 👄	
Home > > Enterprise applicati	ons > Netop Portal			
Netop Portal Users Enterprise Application	and groups			×
« Overview Deployment Plan	Add user/group O Edit Remove O Update Credentials I III Co The application will appear on the Access Panel for assigned users. Set Visible to user	lumns │ ♥ Got feedback? s? to no in properties to prevent this. →		
Manage	First 100 shown, to search all users & groups, enter a display name.			
Properties	Display Name	Object Type	Role assigned	
Owners		User	Default Access	
& Roles and administrators (Preview)		User	Default Access	
Users and groups				
Single sign-on				
Provisioning				
Application proxy				
Self-service				
Security				
🝨 Conditional Access				
🖧 Permissions				
Token encryption				
Activity				
Sign-ins				
🕍 Usage & insights				
Audit logs				
Provisioning logs (Preview)				
E Access reviews				

NOTE: Make sure that the users that you add are from the Windows Server AD.

6. After you finish adding the users and groups, click on the **Assign** button.



Configure single sign-on

To configure the single sign-on, proceed as follows:

- 1. Go to Azure Active Directory.
- 2. Go to Enterprise applications.
- 3. Click on the newly created Netop Portal application.

4. Click on Set up single sign-on.

Microsoft Azure	J ^D Search (esources, services, and docs (G+/)	⊵ Ę \$ @ ? @ .
Home > > Enterprise applica	tions >		
Netop Portal Beta	Test Overview		
σ			
Sverview Cverview	Properties		
Deployment Plan	Ame 🛈		
Manage	Notop Portal Beta Test		
Properties	Application ID ()		
🎒 Gwners	Object ID O		
🚨 Roles and administrators (Preview)	Collection (C)		
Users and groups	Cardina Channel		
Single sign-on	Getting started		
Provisioning			
Sett-service	1. Assign users and groups	3. Set up single sign on	r Accounts 📜 4. Conditional Access
Security	Provide specific users and groups access to the applications	Enable users to sign into their application You'll need to creat using their Azuro 4D production the application	te user accounts in Secure access to this application with a customizable access to his application.
Conditional Access	Assign users and groups	Get started Learn more	Create a policy
- Fermissions			
Token encryption			
Artisty	S. Self service		
Signalar	Enable users to request access to the amplification using their Approx 47		
w agentis M those & includer	credentials		
and usage or insignity	Get started		
 Mouri rogi Braumanna loor (Braumu) 			
Access sectors	What's New		
- PALEN PROPERTY	• ? Sion in charts have moved!		

5. Click on SAML.

Select a single sign-on method Help me decide



6. In the Basic SAML Configuration group, click on the Edit button.



7. Specify the following settings.

Field name	Value
Identifier (Entity ID)	urn:portal:webservices
Reply URL	https://secure.netop.com/saml

8. Click on the **Save** button to save your changes.

Identifier (Entity ID) * ○ The default identifier will be the audience of the SAML response for IDP-initiated SSO urnportalwebservices Image: Comparison of the same service URL) * ○ The default reply URL (Assertion Consumer Service URL) * ○ The default reply URL will be the destination in the SAML response for IDP-initiated SSO Default https://secure.netop.com/saml Image: Comparison of URL ○ Enter a sign on URL ○ Enter a relay state Logout Url ○ Enter a logout url	Basic SAML Configuration				×
Identifier (Entity ID) * The default identifier will be the audience of the SAML response for IDP-initiated SSO	🔜 Save				
The default identifier will be the audience of the SAML response for IDP-initiated SSO	Identifier (Entity ID) * ①				
urnportal:webservices urnportal:webservices Reply URL (Assertion Consumer Service URL)* () The default reply URL will be the destination in the SAML response for IDP-initiated SSO Default Inters://secure.netop.com/saml Sign on URL () Enter a sign on URL Relay State Inter a relay state Logout Url () Enter a logout url	The default identifier will be the audience of the SAML response for IDP-initiated SSO				
urn:portal:webservices Reply URL (Assertion Consumer Service URL) * ③ The default reply URL will be the destination in the SAML response for IDP-initiated SSO Default https://secure.netop.com/saml Sign on URL ③ Enter a sign on URL Relay State ④ Enter a relay state Logout Url ④ Enter a logout url		Defa	ault		
Reply URL (Assertion Consumer Service URL) * () The default reply URL will be the destination in the SAML response for IDP-initiated SSO Default Mttps://secure.netop.com/saml Mttps:/	urn:portal:webservices	\checkmark	(i)	Î	
Reply URL (Assertion Consumer Service URL) * ① The default reply URL will be the destination in the SAML response for IDP-initiated SSO Default Methys://secure.netop.com/saml Sign on URL ① Enter a sign on URL Relay State ① Enter a relay state Logout Url ② Enter a logout url					
Reply URL (Assertion Consumer Service URL) * ① The default reply URL will be the destination in the SAML response for IDP-initiated SSO Default thttps://secure.netop.com/saml fittps://secure.netop.com/saml Sign on URL ① Enter a sign on URL Relay State ① Enter a relay state Logout Url ① Enter a logout url					
The default reply URL will be the destination in the SAML response for IDP-initiated SSO	Reply URL (Assertion Consumer Service URL) * 🕕				
Default https://secure.netop.com/saml Sign on URL Sign on URL Enter a sign on URL Relay State Enter a relay state Logout Url ③ Enter a logout url	The default reply URL will be the destination in the SAML response for IDP-initiated SSO				
https://secure.netop.com/saml Sign on URL ① Enter a sign on URL Relay State ① Enter a relay state Logout Url ② Enter a logout url		Defa	ault		
Sign on URL ③ Enter a sign on URL ✓ Relay State ④ Enter a relay state Logout Url ④ Enter a logout url ✓	https://secure.netop.com/saml		(i)	Ĩ	
Sign on URL ① Enter a sign on URL ✓ Relay State ① Enter a relay state Logout Url ① Enter a logout url ✓					
Sign on URL ① Enter a sign on URL ✓ Relay State ① Enter a relay state Logout Url ① Enter a logout url ✓					
Enter a sign on URL Relay State Enter a relay state Logout Url Enter a logout url	Sign on URL ①				
Relay State ① Enter a relay state Logout Url ① Enter a logout url ✓	Enter a sign on URL			\checkmark	
Relay State ① Enter a relay state Logout Url ① Enter a logout url ✓					
Enter a relay state Logout Url Enter a logout url	Relay State ①				
Logout Url ① Enter a logout url	Enter a relay state				
Enter a logout url	Logout Url 💿				
	Enter a logout url			~	

9. In the User Attributes & Claims group, click on the Edit button.

givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	

Name	Namespace	Source	Source attribute
NRC-ACCOUNT-ID	https://secure.netop.com	Attribute This is the domain identifier that	
			both specify here and in the Netop
			Portal ADFS/Azure AD configuration.
NRC-USERNAME	https://secure.netop.com	Attribute	user.userprincipalname
NRC-GIVEN-NAME	https://secure.netop.com	Attribute	user.givenname
NRC-SURNAME	https://secure.netop.com	Attribute	user.surname
NRC-EMAIL	https://secure.netop.com	Attribute	user.mail

10. Click on the Add new claim button to create the necessary claims.

The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**:

11. Click on the Add a group claim button to add the following Group claim:



11.1. Select the **All groups** option from the Which groups associated with the user should be returned in the claim section.

≡ Microsoft Azure		and docs (G+/)	e e e e e e e e e e
Home > > SAML-based Sign-on >			Group Claims
User Attributes & Claims			Manage the group claims used by Azure AD to populate SAML tokens issued to your app
+ Add new claim + Add a group claim ≣≣ Columns			Which groups associated with the user should be returned in the claim?
			All groups
Required claim			Security groups
Claim name	Value		O Directory roles
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for		Groups assigned to the application
https://secure.netop.com/NRC-EMAIL	user.userprincipalname		Source attribute *
https://secure.netop.com/NRC-GIVEN-NAME	user.givenname		Group ID
https://secure.netop.com/NRC-SURNAME	user.sumame		Advanced options
https://secure.netop.com/NRC-USERNAME	user.userprincipalname		Customize the name of the group claim
nameidentifier	user.userprincipalname		
https://secure.netop.com/NRC-ACCOUNT-ID	"netop"		Name (required)
Additional claims			Namespace (optional)
Claim name	Value		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail		Emit groups as role claims ①
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname		
			Save

- 11.2. Click on the **Customize the name of the group claim.**
- 11.3. Specify the required name and namespace of the claim:
 - Name: NRC-GROUPS
 - Namespace: https://secure.netop.com

Microsoft Azure	℅ Search resources, services, and docs (G+/)	N 💀 🗘 🕸 ? 😳
e > > > SAML-based Sign-on > er Attributes & Claims …		Group Claims Manage the group claims used by Azure AD to populate SAML tokens issued to your
+ Add new claim + Add a group claim ≡≣ Columns		Which groups associated with the user should be returned in the claim?
equired claim		All groups Security groups
Claim name	Value	Original Structure of the application
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for ***	
https://secure.netop.com/NRC-EMAIL	user.userprincipalname ***	Source attribute *
https://secure.netop.com/NRC+GIVEN+NAME	user.givenname •••	Group ID
https://secure.netop.com/NRC-SURNAME	user.surname ***	Advanced options
https://secure.netop.com/NRC-USERNAME	user.userprincipalname ***	Customize the name of the group claim
nameidentifier	user.userprincipalname ***	Name (required)
https://secure.netop.com/NRC-ACCOUNT-ID	"netop" ····	rearine (required)
dditional claims		Namespace (optional)
Claim name	Value	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ····	Emit groups as role claims ①
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname •••	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***	
http://schemes.vmlcoop.org/ws/2005/05/deptity/claims/surgame		

12. Click on the **Save** button to save your changes.

Microsoft Azure	₽ Search resources, services,	and docs (G+/)	E 🗣 🔎 🕲 ? 😊	0
Home > > SAML-based Sign-on > User Attributes & Claims			Group Claims Manage the group claims used by Azure AD to populate SAML tokens issued to your app	×
+ Add new claim + Add a group claim III Columns			Which groups associated with the user should be returned in the claim? None All groups Genuty groups	
Claim name	Value		O Directory roles	
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for		 Groups assigned to the application 	
https://secure.netop.com/NRC-EMAIL	user.userprincipalname		Source attribute *	
https://secure.netop.com/NRC-GIVEN-NAME	user.givenname		Group ID	\sim
https://secure.netop.com/NRC-SURNAME	user.sumame		Advanced options	
https://secure.netop.com/NRC-USERNAME	user.userprincipalname		Customize the name of the group claim	
nameidentifier	user.userprincipalname			
https://secure.netop.com/NRC-ACCOUNT-ID	"netop"		Name (required) NRC-GROUPS	
Additional claims			Nameroan (antional)	_
Claim name	Value		https://secure.netop.com	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail		Emit groups as role claims ①	_
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname			
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname			
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.sumame			
			Son	

Make sure that you save the following information:

The Federation Metadata XML file •



If you plan on using the Azure AD groups then it is necessary that you also save the Application ID

https://sts.windows.net/cd5f608a-30a6-4ec3-b..

https://login.microsoftonline.com/common/wsf...

L)

ւր

ቡ

Application ID •

To retrieve the Application ID value from the Azure Portal, proceed as follows:

1.1. Go to the Azure Portal.

Azure AD Identifier

View step-by-step instructions

Logout URL

- 1.2. Go to Windows Active Directory.
- 1.3. Go to Enterprise Applications.
- 1.4. Select the Netop Portal application.
- 1.5. Go to **Overview**.

1.6. Click on the Copy to clipboard button.

■ Microsoft Azure	P Search resources, services, and docs (G+/)	D 67 0 0 🧃
Home > > Enterprise applicat	ions >	
Enterprise Application	Overview	×
Uverview	Properties	
Deployment Plan	Name ()	
Manage	Netop Portal Beta Test	
Properties	Application ID () Copy to clipboard	
A Owners		
Boles and administrators (Preview)		
Users and groups	Getting Started	
Single sign-on	orting started	
Provisioning		
Self-service	1. Assign users and groups 🏐 2. Set up single sign on 🎇 3. Provision User Accounts	4. Conditional Access
Security	Provide specific users and groups access Enable users to sign into their application You'll need to create user accounts in to the applications using their Azure AD credentials the application	Secure access to this application with a customizable access policy.
Conditional Access	Assign users and groups Get started Learn more	Create a policy
4 Permissions		
Token encryption		
Activity	S. Self service	
3 Sign-ins	Enable users to request access to the application using their Azure AD	
🕍 Usage & insights	credentials Get started	
Audit logs		
Provisioning logs (Preview)		
≸ Access reviews	What's New	
	Sign in charts have moved! The new insights view shows sign in info along with other useful application data. View insights	
	Delete Application has moved to Properties You can now deter your application from the Properties page. View properties	

Configure the application permissions

The following steps apply only if you want to use the Azure AD groups in the Netop Portal.

To configure the application permissions, proceed as follows:

- 1. Go to Azure Active Directory.
- 2. Go to App registrations.



3. Click on the **Netop Portal** application.



4. Click on the View API permissions button.

5.

Call APIs
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources. View API permissions
Sign in users in 5 minutes
Use our SDKs to sign in users and call APIs in a few steps View all quickstart guides
Click on the Add a permission button to add the necessary permissions.

Configured permissions				
Applications are authorized t all the permissions the applic	o call APIs when they a ation needs. Learn mo	re granted permiss re about permissio	sions by users/admins as part of the consent process. The list of con ns and consent	figured permissions should include
+ Add a permission	Grant admin cor	isent for home		
	Add a permission			
API / Permissions nar	ne Type	Description	Admin consent req	Status
No permissions added				

6. Click on Microsoft Graph.



7. Click on Application permissions.

	∠P Search resources, services, and docs (G+/)		国际 🖗 @ ? @ 🧧
Home > >	API permissions 💉 …	Request API permissions	×
₽ Search (Ctrl+/) «	🕐 Refresh 🔰 🛇 Got feedback?	Microsoft Graph	
Overview		What type of permissions does your application require?	
 Quickstart Integration assistant 	The 'Admin consent required' column shows the default value for an organization. However, user consent can be customized per permission	Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a
Manage	Configured permissions		signed-in user.
Eranding	Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the parmissions the application panels, learn more about permissions and consent.		
Authentication	ин сле регладного иле вруповного пессо, кемп поле воско регладного иле сотретя.		
Certificates & secrets	+ Add a permission 🗸 Grant admin consent for netop.se		
Token configuration	API / Permissions name Type Description Admin consent req		
API permissions	No permissions added		
Expose an API			
App roles	To view and manage permissions and user consent, try Enterprise applications.		
A Owners			
Boles and administrators Preview			
Manifest			
Support + Troubleshooting			
Troubleshooting			
New support request			
		Add permissions Discard	

8. Search for Group in the Start typing a reply url to filter these results search field.

	∠P Search resources, services, and docs (G+/)	E 6 2 0 ? C		
Home > > >	API permissions 🖋 …	Request API permissions	×	
Search (Ctrl+/) « Overview	🖒 Refresh 🛛 🛇 Got feedback?	Microsoft Graph https://graph.microsoft.com/ Docs 3	Î	
 Quickstart Integration assistant 	The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission	What type of permissions does your application require? Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.	
Manage Branding Authentication	Contigured permissions Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and consent	Select permissions	espand all	
 Certificates & secrets Token configuration 	Add a permission V Grant admin consent tor hetepse APJ / Permissions name Type Description Admin consent req. No permissions defed	Permission AccessReview	Admin consent required	
API permissions Expose an API App roles	To view and manage permissions and user consent, try Enterprise applications.	> AdministrativeUnit		
 Owners Roles and administrators Proview 		AgreementAcceptance		
Manifest		Agreement APIConnectors		
2 Troubleshooting		> Application		
New support request		> AppRoleAssignment		
		ApprovalRequest AuditLog		
		Add permissions Discard		

9. Click on the Group.Read.All option.

■ Microsoft Azure	, P Search resources, services, and docs (G+/)		D & @ @ ? © 🧶
Home > >	API permissions 🖈 …	Request API permissions	×
Search (Ctrl+/) « Overview	○ Refresh ♥ Got feedback?	Microsoft Graph https://graph.microsoft.com/ Docs @*	
 Quickstart Integration assistant 	The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission.	What type of permissions does your application requirer Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
Manage Branding	Configured permissions Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of ca all the permissions the application needs. Learn more about permissions and consent	Select permissions	expand all
Authentication Certificates & secrets Token configuration	+ Add a permission \checkmark Grant admin consent for netopue API / Permissions name Type Description Admin consent req.	P Group Permission	X Admin consent required
API permissions Expose an API	No permissions added	Calls	
App roles	To view and manage permissions and user consent, try Enterprise applications.	Group.Create ③ Create groups	Yes
Roles and administrators Preview Manifest		Group.Read.All ① Read all groups	Yes
Support + Troubleshooting		Read and write all groups	Yes
New support request		PrivilegedAccess	
		Add permissions Discard	

10. Click on the Add permissions button to add your permission.

■ Microsoft Azure	, P Search resources, services, and docs (G+/)		🕞 🕞 🥵 ? 💿 adadmin@netop.se 🧶
Home > netop.se > Netop Portal Beta	r™et Test API permissions ≉ …	Request API permissions	×
Search (Ctrl+/) « Overview	🕐 Refresh 🗢 Got feedback?	Calleys Microsoft Graph Microsoft Graph http://graph.microsoft.com/ Docs c3* What type of permissions does your application require?	
 Quickstart Integration assistant 	The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission.	Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
Manage Branding Authentication	Configured permissions Applications are automated to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and consent	Select permissions	- expand all
Certificates & secrets Token configuration	+ Add a permission	Permission	Admin consent required
 API permissions 	No permissions added	> Calls	
Expose an API App roles Owners	To view and manage permissions and user consent, try Enterprise applications.	Group.Create O Create groups	Ves
Roles and administrators Preview Manifest		Group.Read.All ① Read all groups	Yes
Support + Troubleshooting		Group.ReadWrite.All ③ Read and write all groups	Yes
Troubleshooting New support request		GroupMember PrivilegedAccess	
		Add comining	

11. Click on the Grant admin consent for ... button to grant admin consent for the API permission.

Microsoft Azure		P	Search resources, services, and d	locs (G+/)		D 6	🖉 💿 ? 💿	
Home > >								
-	\$							\times
🔎 Search (Ctrl+/)	🕐 Refresh 🕴 🗢 Got feedback	a						
Cverview	A You are editing permission(s) to	your application, u	users will have to consent even if th	sey've already done so previously.				
 Quickstart Integration assistant 								
Manage	The "Admin consent required" of the consent required of the consent require	column shows the r	default value for an organization. H	lowever, user consent can be customized per permission,	user, or app. This column may not refle	ct the value in your organization, or in organizations when	e this app will be used. Learn more	×
Branding Authentication Certificates & secrets	Configured permissions Applications are authorized to call A all the permissions the application n	Pis when they are seeds. Learn more	granted permissions by users/a about permissions and consent	dmins as part of the consent process. The list of con	figured permissions should include			
Token configuration	+ Add a permission 🗸 Grant	admin consent fo	r					
API permissions	API / Permissions name	Туре	Description	Admin consent req	Status			
Expose an API	Microsoft Graph (1)							
R App roles	Group.Read.All	Application	Read all groups	Yes	A Not granted for netop.se ····			
A Owners								
Roles and administrators Preview	To view and manage permissions an	d user consent, tr	y Enterprise applications.					
Manifest								
Support + Troubleshooting								
Troubleshooting								
New support request								

Configure certificates & secrets

To configure the certificates & secrets for the Netop Portal application in the Azure Portal, proceed as follows:

- 1. Go to Azure Active Directory.
- 2. Go to App registrations.
- 3. Click on the Netop Portal application.

4. Go to Certificates & secrets.

	,P Search resources, services, and docs (G+/)		5 6 0 0 0	
Home > >				
*				\times
P Search (Ctrl+/) ≪	🔋 Delete 🕀 Endpoints 🖼 Preview features			
Soverview	∧ Essentials			i i
Quickstart	Display name : Netop Portal 2	Supported account types : My organization only		
💉 Integration assistant	Application (client) ID : Oddeaed9-3fe0-4a32-97ca-515ccb3d6d94	Redirect URIs : 1 web, 0 spa, 0 public client		
Manage	Directory (renant) ID : 82000999-7009-4209-4000848083005 Object ID : ea915fe8-8845-4266-8e8f-10d51bf1533e	Managed application in I : Netop Portal 2		
Branding Authentication	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. W upgraded to Microsoft Ruthentication Library (MSAL) and Microsoft Graph. Learn more	e will continue to provide technical support and security updates but we will	I no longer provide feature updates. Applications will need to be	×
Certificates & secrets Token configuration API permissions	Call APIs	Documentation		
Expose an API App roles App roles Annes Annes Annese Manifest Support + Troubleshooting Troubleshooting	Werk AP permission	Authentication screwids Authentication binaries Code samples Microsoft Gaph Glossary Help and Support		
New support request	Sign in users in 5 minutes			

5. Click on the New client secret button.

■ Microsoft Azure	P Search resources, services, and docs (G+)	
Home > >		
† C	ertificates & secrets 🤌 …	×
P Search (Ctrl+/)	♡ Got feedback?	
Overview	Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS	
📣 Quickstart	scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.	
💉 Integration assistant	Certificates	
Manage	Certificates can be used as servets to prove the application's identity when requestion a token. Also can be referred to as public laws	
Branding	чентовка чит не изна на лечена за рготе иле врртовнот а ластоту и пол терезлиту в точки лео чит не телетко то на разпо вери	
Authentication	↑ Upload certificate	
📍 Certificates & secrets	Thumbprint Start date Expires ID	
Token configuration	No certificates have been added for this application.	
 API permissions 		
🙆 Expose an API		
App roles	Client secrets	
A Owners	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.	
Roles and administrators Preview	+ New client servet	
Manifest	New costs accest New costs accest Description Expires Value ID	
Support + Troubleshooting	אינארוקאטירו האקורנע דעוועי וש	
Troubleshooting	No client secrets have been created for this application.	
New support request		

- 6. Specify a name for the client secret in the **Description** entry field.
- 7. Specify an expiry date for the client secret accordingly to your needs.

8. Click on the Add button.

	, P Search resources, services, and docs (G+/)	D & 0 % @ &
Home > > > Ce	tificates & secrets 👒 …	×
P Search (Ctrl+/) ≪	♡ Got feedback?	
Courriew Cuickstart C	Add a client secret Description Tetep Portal Expires O In 1 year Never Add Cancel Tete Tete Tete Tete Tete Tete Tete Tete	
 API permissions Expose an API 		
App roles Owners Roles and administrators Preview	Client secrets A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password. + New client secret	
Support + Troubleshooting Troubleshooting New support request	Description Expires Value ID No client secrets have been created for this application.	

 Save the client secret value in a text editor or copy it to the clipboard. It is necessary for you to do so, because once you leave this particular page the value will no longer be available for display in plain text.

		₽ Search resource.	s, services, and docs (G+	0				₽ 🖉 @ ? © 🛛 😫
Home > netop.se > Netop Portal Beta	Test Test Certificates & secr	ets 🖈 …						Update application credentials 4:47 PM Successfully updated application Netop Portal Beta Test credentials
	💙 Got feedback?							
Overview Ovidetart	Copy the new client secret value. Ye	u won't be able to retrieve it aft	er you perform another op	eration or leave this bl	ade.			
 Guickstart Integration assistant 	Credentials enable confidential applicat scheme). For a higher level of assurance	ons to identify themselves to , we recommend using a certi	the authentication servic ficate (instead of a client	e when receiving tok secret) as a credenti	ens at a web addres al.	sable location (using an HTTP	S	
Manage	Certificates							
Authentication	Certificates can be used as secrets to pr	ove the application's identity	when requesting a token	Also can be referred	to as public keys.			
📍 Certificates & secrets	Upload certificate							
Token configuration API permissions	Thumbprint		Start date	Expires	ID			
Expose an API	No certificates have been added for this	application.						
👪 App roles								
Owners	Client secrets							
Manifest	A secret string that the application uses	to prove its identity when req	uesting a token. Also ca	n be referred to as ap	plication password.			
Support + Troubleshooting	+ New client secret				_			
Troubleshooting	Description	Expires	Value		ID			
New support request	Netop Portal	3/24/2022	В		D		D 📋	

Configure Azure AD in the Netop Portal

To configure the ADFS/Azure AD authentication method in the Netop Portal, proceed as follows:

1. Log in to the <u>Netop Portal</u>.

NOTE: Make sure that you use an administrator account.

2. Go to Authentication.

Dashboard		Users: 42 / 1000 OnDemand user	s: 3 / 500 Devices: 74 / 300 John Doe 🔻
MANAGE			
📇 Users			
🖵 Devices	All authentication methods (8)		ৎ Add ADFS / Azure AD ৎ Add LDAP
요그 Groups	C Results can be filtered using the ▼ on each column		
Applications			
≔ Roles	▲ Name	Authentication type	Authentication method identifier
몹 Role assignments	ADFS (do not modifiy)	ADFS	my-identifier\
🗊 Downloads	Azure (do not modifiy)	Azure AD	nrcbeta\
SECURITY	AzureAD Test	Azure AD	nrcazuretestbeta\
Account security	• INTERNAL	INTERNAL	-
Authentication	Idap auth - 34.252.23.128	LDAP	domid\
🖹 Logs	NU STERGE	LDAP	domainSuperPuper\
ACCOUNT	• test	Azure AD	test
Configuration			
Netop	test-Idap	LDAP	test-Idap\ Activate Windows Go to Settings to activate Windows.

3. Click on the Add ADFS / Azure AD button.

Dashboard MANAGE		Users: 39 / 1000 OnDemand users: 3	30 / 1000 Devices: 70 / 300 John Doe 🔻
📇 Users		-	
🖵 Devices	All authentication methods (8)		ৎ Add ADFS / Azure AD ৭ Add LDAP
요구 Groups	C Results can be filtered using the ▼ on each column		,
Applications	▲ Name ₹	Authentication type	Authentication method identifier
≔ Roles		radionastion gpo	
器 Role assignments	ADFS (do not modifiy)	ADFS	my-identifier\
Downloads	Azure (do not modifiy)	Azure AD	nrcbeta\
SECURITY	AzureAD Test	Azure AD	nrcazuretestbeta\
Account security	• INTERNAL	INTERNAL	-
♣ Authentication	Idap auth - 34.252.23.128	LDAP	domid\
Logs	NU STERGE	LDAP	domainSuperPuper\
ACCOUNT	• test	Azure AD	testl

4. Specify a name for the authentication method in the **Name** entry field.

🔩 ADD ADFS / AZURE AD	Close X	
More information on how to integrate with ADFS and Azure AD is available here.		
Name		•
Enabled (This authentication method is enabled)		
Authentication type	~	0
The authentication type will be automatically filled in once you upload the FederationMedata xml file.		
Domain identifier		8
This will be used when logging in (domain identifier/username)		
IdP		0
Identity Provider's (IdP) URL		
Group (Optional)	~	
The user will become a member of this group on first login.		
ADFS / Azure AD FederationMetadata.xml file	owse	0
Q _t Save		

- 5. Click on the toggle button to enable or disable the authentication method.
- 6. In the **Domain identifier** entry field, specify the same value as the one specified in the NRC-ACCOUNT-ID user claim.

🔍 ADD ADFS / AZURE AD	Close 🗙
More information on how to integrate with ADFS and Azure AD is available here.	
Namo	
Azure AD	
Enabled (This authentication method is enabled)	
Authentication type	~
The authentication type will be automatically filled in once you upload the	
rederationMediata.xmi nie.	
Domain identifier <u>netopazure</u>	
reverauonmedaaa xini ine. Domain identifier netopazure This will be used when logging in (domain identifier/username)	
Domain identifier <u>netopazure</u> This will be used when logging in (domain identifier/username) IdP	
Domain identifier netopazure This will be used when logging in (domain identifier/usemame) IdP Identity Provider's (IdP) URL	
IdP Group (Optional)	~
Domain identifier Interconduction IdP Identity Provider's (IdP) URL Group (optional) The user will become a member of this group on first login.	~

7. In the **IdP** field, copy the **Login URL** from the **Set up Single sign on with SAML** page in the Azure AD portal.

🔍 ADD ADFS / AZURE AD	Close 🗙	
More information on how to integrate with ADFS and Azure AD is available here.		
Name Azure AD		•
Enabled (This authentication method is enabled)		
Authentication type	~	6
The authentication type will be automatically filled in once you upload the FederationMedata.xml file.		
Domain identifier netopazure		
This will be used when logging in (domain identifier/username)		
https://		
dentity Provider's (IdP) URL		
Group (Optional)	~	
The user will become a member of this group on first login.		
ADFS / Azure AD FederationMetadata.xml file	rowse	e

8. In the ADFS/Azure AD FederationMetadata.xml field, click on the Browse button.

ADD ADFS / AZURE AD	Close 🗙
More information on how to integrate with ADFS and Azure AD is available here.	
Name Azure AD	~
Enabled (This authentication method is enabled)	
Authentication type	~ 6
The authentication type will be automatically filled in once you upload the FederationMedata.xml file.	
Domain identifier netopazure	~
This will be used when logging in (domain identifier/username)	
https://	-
Identity Provider's (IdP) URL	
Group (Optional)	~
The user will become a member of this group on first login.	
ADFS / Azure AD FederationMetadata.xml file	owse 🛛
	_
a, Save	

9. Go to the file path where you saved the FederationMetadata.xml file, select it, and click on Open.

The following steps apply only if you want to use the Azure AD groups in the **Netop Portal**. 10. In the **Application ID** entry field, specify the Netop Portal **Application ID** from the **Azure Portal**.

B Remote Control			netoptest		-	T Purchase	Users: 497 1000	OnDemand users: 575	Devices 24/300
Dashboard Access			Enabled (This authentication method Authentication type Azure AD	is enabled)	0				Z Edit X Remove
⊕ _µ My sessions □ My devices	4 Authentication method info		The authentication type will be automatically FederationMedata.xml file.	filled in once you upload the					
My mobile devices	Name		Domain identifier						
MANAGE	Status	Enabled	This will be used when logging in (domain ide	intifier/usemame)					
All Users	Authentication type	Azure AD	IdP						
La Devices	Domain Identifier		Identity Provider's (IdP) URL						
Applications	IdP	https://login.microsofianline.com/a4/971	Group						
≡ Roles	Certificate validity	From 2020-06-11 19:12:17 To 2023-	new Group	an first Ionin					
7 Role assignments	Application ID	*	The user will become a memory of this group	on macrogen.					
Downloads	Client secret	*	ADFS / Azure AD FederationMeta	idata xml file Browse	0				
SECURITY	Group	new Group	Certificate valid from 2020-06-11 19:12:17	Certificate valid to 2023-06-11 19:12:17					
9, Authentication	Created	2020-06-11 19:21:21	Application ID (output)						
Logs	Created by	John Doc (ansignatup cam)	Fill in the Application ID and Client secret to u	εο Δαυτό ΔΩ ατομοί					
ACCOUNT	Modified	2021-03-22 09:25:57		an reaction groups.					
O ₆ Consultation	Modified by	TEAM Account Owner (devices, portal	Client secret (Optional)		×				
			Test configuration						
				_					
Netop			Q, Sav	•					

11. In the **Client secret** entry field, specify the client secret value from the **Certificates & secrets** page in the Azure Portal.

Remote Control			netoptest		-	T Purchase	Users: 497 1000	OnDemand users: 575	Devices: 24/300	*
Dashboard Access			Enabled (This authentication me Authentication type Azure AD	thod is enabled)	0				🖌 Edit 🛛 🗙 Remo	ve
⊕ My sessions □ My devices	& Authentication method info		The authentication type will be automatic FederationMedata xml file.	ally filled in once you upload the						
My mobile devices	Name		Domain identifier		0					
MANAGE	Status	Enabled	This will be used when logging in (domain	n identifierkusername)						
🛎 Users	Authentication type	Azuro AD	ШР		1					
BCI Generation	Domain identifier		Identity Provider's (IdP) URL		100					
Applications	IdP	Https://login.microsoftentine.com/a4/d97	Group		i l					
= Roles	Certificate validity	From 2020-06-11 19 12:17 To 2023-	new Group	roun on first lonin	1					
Role assignments	Application ID	283 2		and an and a gat						
Downloads	Client secret		ADFS / Azure AD FederationM	letadata xml file Browse	0					
SECURITY Account security	Group	new Group	Certificate valid from 2020-06-11 19:12:17	Certificate valid to 2023-06-11 19:12:17						
Authentication	Created	2020-06-11 19:21:21	Application ID restores							
🖻 Logs	Created by	John Doe (ansugnetup son)	Fill in the Application ID and Client secret	to use Azure AD arouns	*					
	Modified	2021-03-22 09:25:57		a oo a sa s	1					
W ₆ Consignation	Modified by	TEAM Account Owner Morteau, portail	Client secret (optional)		~					
			Test configuration							
Netop			٩	Save						

12. To test your configuration, click on the **Test configuration** button. "*The Azure AD configuration is correct.*" text message is displayed if the configuration is successful, or an error message is displayed if the configuration was unsuccessful.

Remote Control			4 EDIT ADFS / AZURE	AD	Close X	T Contact Netop	🗮 Purchase	Users: 49 / 1000	OnDomand users: 575	Devices: 24/300	
Dashboard ACCESS	AZURE AD		More information on how to integrate with	ADFS and Azure AD is available here.						🖌 Edit	* Remove
P _→ My sessions My devices	۹ Authentication method info		AZURE AD		0						
My mobile devices	Name	AZURE AD	Enabled (This authentication	method is enabled)							
MANAGE	Status	Enabled	Authentication type Azure AD		~ 0						
Devices	Authentication type	Azure AD	The authentication type will be automa FederationMedata.xml file.	tically filled in once you upload the							
B Groups	IdP		Domain identifier		θ						
≡ Roles	Certificate validity	From 2018-10-11 19:02:35 To 2021-10-11 19:02:36	This will be used when logging in (dom	nain identifier/username)							
 Role assignments Downloads 	Application ID		kd ^p		~						
SECURITY	Client secret		Identity Provider's (IdP) URL								
Account security	Group		Group		~						
 Authentication Logs 	Created	2021-03-24 17:28:30	The user will become a member of this	s group on first login.							
ACCOUNT	Created by		ADFS / Azure AD Federation	nMetadata.xml file Br	owse O						
Configuration	Modified	2021-04-19 12:21:80	Certificate valid from 2018-10-11 10-02-25	Certificate valid to							
	Modified by		2010-10-11 19.02.30	2021-10-11 15.02.30							
			Abherroute		~						
			Client secret	ret to use Azure AD groups.							
			Test configuration The Azur	re AD configuration is correct.							
				G. Save							
Noton											
ador.											

13. Click on **Save** to save your configuration.

Remote Control			Enabled (This authentication method is enabled)		Users: 147999 OnDemand users: 4725	Devices: 2030 / 10000	Andrei Cucos 💌
Dashboard Access	Netop Portal Test		Authentication type Azure AD The authentication type will be automatically filled in once you upload the FederationAdvidual and like.	0		🖌 Edit	X Remove
P My sessions	۹ Authentication method info		Domain identifier netoptest	0			
My mobile devices	Name	Nelop Portal Test	This will be used when logging in (domain identifier/username)				
MANAGE	Status	• Enabled	https://login.microsoftonline.com/82cdc9a9-7de3-	0			
Att Users	Authentication type	Azure AD	Identity Provider's (IdP) URL				
문 Groups	Domain identifier	netoptest	Group cfacrgi				
Applications	IdP	https://login.microso	The user will become a member of this group on first login.				
🗏 Roles	Certificate validity	From 2021-03-23 1	ADFS / Azure AD FederationMetadata.xml file Browse	0			
Role assignments	Application ID	246d20df-b630-4am	Cartificate valid from Cartificate valid to				
Townsaus .	Client secret	aCi	2021-03-23 15:57:07 2024-03-23 15:57:06				
Account security	Group	ctacrgi	Application ID 246d20df-b630-4ae9-b4c1-54413b1e65b5				
R _e Authontication	Created	2021-03-23 15:59-2	Fill in the Application ID and Client secret to use Azure AD groups.				
Logs	Created by	Andrei Cacos (mas	Client secret eCi*******************************				
Configuration	Modified	2021-03-24 12:48:2					
	Modified by	TEAM Account Ow	G, Save				
Netop							

ADFS integration with the Netop Portal

The ADFS integration with the **Netop Portal** requires setting up a two-way trust. ADFS requires to be configured to trust the **Netop Portal** as a relying party.

Pre-requisites

- ADFS 2.0 or later is installed (for more information on how to install ADFS 2.0, refer to the following link)
- The users that authenticate by using ADFS are required to have the following LDAP fields non empty:
 - o E-Mail-Addresses
 - o Given-Name
 - User-Principal-Name

NOTE: The following procedure uses the Windows Server 2012 R2 Operating System.

Add Netop Portal as a Trusted Relying Party

To add the **Netop Portal** as a Trusted Relying Party, proceed as follows:

- 1. Connect to your ADFS server.
- 2. Open the ADFS Management Console.

🕲 l 💽 📗 = l	Shortcut Tools			Administrative Tools			;	¢
File Home Shar	e View Manage						\sim	?
(⇒) → ↑ (⊕) + (Control Panel + System and Security + Administra	tive Tools			✓ C Search Adm	inistrative Tools	م	,
	Name	Date modified	Туре	Size				^
Desktop	Terminal Services	8/22/2013 3:39 PM	File folder					
Downloads	Active Directory Administrative Center	8/21/2013 11:50 PM	Shortcut	2 KB				
Recent places	Active Directory Domains and Trusts	8/22/2013 6:55 AM	Shortcut	2 KB				
	Active Directory Module for Windows Po	8/22/2013 6:55 AM	Shortcut	2 KB				
🌉 This PC	Active Directory Sites and Services	8/22/2013 6:55 AM	Shortcut	2 KB				
隆 Desktop	Active Directory Users and Computers	8/22/2013 6:55 AM	Shortcut	2 KB				
Documents	AD FS Management	8/22/2013 6:56 AM	Shortcut	2 KB				
🐌 Downloads	🛃 ADSI Edit	8/22/2013 6:55 AM	Shortcut	2 KB				
🚺 Music	Component Services	8/22/2013 6:57 AM	Shortcut	2 KB				=
崖 Pictures	🛃 Computer Management	8/22/2013 6:54 AM	Shortcut	2 KB				
📑 Videos	📸 Defragment and Optimize Drives	8/22/2013 6:47 AM	Shortcut	2 KB				
🏜 Local Disk (C:)	🛃 DNS	8/22/2013 6:55 AM	Shortcut	2 KB				
	📷 Event Viewer	8/22/2013 6:55 AM	Shortcut	2 KB				
📬 Network	📷 Group Policy Management	8/22/2013 6:56 AM	Shortcut	2 KB				
	🖹 Internet Information Services (IIS) Manager	8/22/2013 6:50 AM	Shortcut	2 KB				
	😹 iSCSI Initiator	8/22/2013 6:57 AM	Shortcut	2 KB				
	Local Security Policy	8/22/2013 6:54 AM	Shortcut	2 KB				
	📷 ODBC Data Sources (32-bit)	8/21/2013 11:56 PM	Shortcut	2 KB				
	📷 ODBC Data Sources (64-bit)	8/22/2013 6:59 AM	Shortcut	2 KB				
	Performance Monitor	8/22/2013 6:52 AM	Shortcut	2 KB				
	Resource Monitor	8/22/2013 6:52 AM	Shortcut	2 KB				
	👼 Security Configuration Wizard	8/22/2013 6:45 AM	Shortcut	2 KB				
	🕞 Server Manager	8/22/2013 6:55 AM	Shortcut	2 KB				
	Services	8/22/2013 6:54 AM	Shortcut	2 KB				L
	🔁 System Configuration	8/22/2013 6:53 AM	Shortcut	2 KB				2
33 items 1 item selecte	d 1.21 KB						8==	

3. Go to Trust Relationships.

4. Right-click on Relying Party Trust.

\$		AD FS		_ _ X
翰 File Action View Window Help				_ <i>=</i> ×
🗢 🔿 🙍 🖬 👔				
 AD FS Service Claims Provider Trusts Relying Party Trusts Attibute Stores Authentication Policies 	Relying Party Trusts Display Name secure-staging netop.com Device Registration Service AWS secure-beta netop.com	Frabled Type Yes WS-T Yes WS-T Yes WS-T Yes WS-T	Identifier um portal staging webservices um mar drs.adfs-test.netop.com um amazon.webservices um portal beta-webservices	Actions Relying Party Trusts. Add Relying Party Trust Add Non-Claims-Aware Relying Party Trust View New Window from Here Image: Complex and the state of t
	J			

5. Select the Add Relying Party Trust option. The Add Relying Party Trust Wizard is displayed.

\$ 1			AD FS			
翰 File Action View Wind	dow Help					_ <i>5</i> ×
🗢 🤿 🙎 📰 🛛 🖬						
AD FS		Relying Party Trusts				Actions
Service		Display Name		Enabled	Type Id	Relying Party Trusts
Claims Provider Trusts	s	secure-staging.netop.com secure-alpha.netop.com		Yes Yes	WS-T u WS-T u	Add Relying Party Trust
Relying Party A	dd Relying Part	y Trust		Yes	WS-T u	Add Non-Claims-Aware Relying Party Trust
Authoute Stor Authoute Stor Au	dd Non-Claims	-Aware Relying Party Trust		Yes	WS-T ur WS-T ur	View 🕨
Vi	ïew	•				New Window from Here
N	lew Window fro	m Here				Q Refresh
Re	efresh					P Help
H	lelp					secure-beta.netop.com
						Update from Federation Metadata
						Edit Claim Rules
						Disable
						Properties
						X Delete
						👔 Help
		< III			>	
Add a new relying party trust to th	Add a new relying party trust to the configuration database					

6. Click on Start.

Add Relying Party Trust Wizard					
Welcome					
Steps Welcome Select Data Source Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.	\$			
	< <u>P</u> revious <u>Start</u> Cancel				

- 7. Select the Import data about the relying party published online or on a local network option.
- 8. In the Federation metadata address (host name or URL specify the following: <u>https://secure.netop.com/saml/metadata.xml</u>). The XML metadata file is a standard SAML metadata document that describes the **Netop Portal** as a relying party.

\$	Add Relying Party Trust Wizard
Select Data Source	
Steps Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: () Ignot data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL): Inttps://secure.netop.com/sami/metadata.xmi Example: fs.contoso.com or https://www.contoso.com/app Impgrt data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has explored its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Browse Or Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.
	< <u>Previous</u> <u>N</u> ext > Cancel

9. Click on Next.

10. In the display name field, specify the **Display name** for the relying Party.

\$	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Portal Netop ADFS	
Specify Display Name	Notes:	
Configure Multi-factor Authentication Now?		^
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
🥃 Finish		Ľ
	< Previous Next > Cancel	

11. Click on Next.

12. Select the I do not want to configure... option.

\$	Add Relying Party Trust Wizard
Steps • Welcome • Select Data Source • Specify Display Name • Configure Multi-factor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	Add Relying Party Trust Wizard 2 Configure multifactor authentication settings for this relying party trust. Multifactor authentication is required if there is a match for any of the specified requirements. Multifactor Authentication Global Settings Multifactor Authentication Global Settings Requirements Users/Groups Not configured Device Not configured Location Not configured I do not want to configure multifactor authentication settings for this relying party trust at this time. O configure multifactor authentication settings for this relying party trust.
	You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u> .
	<pre></pre>

13. Click on Next.

14. Select the Permit all users to access this relying party option.

National Add Relying Party Trust Wizard							
Choose Issuance Authorization Rules							
Steps Welcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	 Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules. Permit all users to access this relying party The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access. Deny all users access to this relying party The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must later add issuance authorization rules for this relying party trust by selecting the relying party trust and claims Eff Chine Dube in the Actions area. 						
	and clicking Edit Claim Rules in the Actions pane.						

15. Click on Next.

16. Review your settings and click on Next.

Add Relying Party Trust Wizard								
Ready to Add Trust								
Ready to Add Trust Steps • Welcome • Select Data Source • Specify Display Name • Configure Multifactor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database. Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Note Specify the monitoring settings for this relying party trust. Relying party's federation metadata URL: https://secure.netop.com/samll/metadata.xml Monitor relying party Monitor relying party Automatically update relying party This relying party's federation metadata data was last checked on: 5/11/2017 This relying party was last updated from federation metadata on: 5/11/2017							
	< <u>P</u> revious <u>N</u> ext > Cancel							

17. Select the Open the Edit Claim Rules dialog for this relying part trust when the wizard

closes checkbox.

\$ #	Add Relying Party Trust Wizard
Finish	
Steps	The relying party trust was successfully added to the AD FS configuration database.
Welcome	You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.
Select Data Source	
Specify Display Name	
Configure Multi-factor Authentication Now?	✓ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes
 Choose Issuance Authorization Rules 	
Ready to Add Trust	
Finish	
	Close

18. Click on **Close** to finalize the setup. The Netop Portal is added as a relying party.

Add Claim Rules for the Netop Portal Relying Party

It is necessary that you add the Claim Rules so that the elements that the **Netop Portal** requires, which the ADFS does not provide them by default (Nameld, AccountId, Email, First name and Principal name), are added to the SAML authentication response.

To add the Claim Rules, proceed as follows:

1. Right-click on the relying party (in this case Netop Portal ADFS).

2. Select the Edit Claim Rules option.



3. In the Edit Claim Rules for <relying party> dialog box, click on the Add Rule button.

Q		Ed	it Claim	Rules fo	or Neto	p Portal /	ADFS	-		x
ls	suance 1	Fransform Rules	Issuanc	e Authoriza	tion Rules	s Delegatio	n Authoriza	ation R	ules	
	The follo	wing transform	rules speci	ify the claim	ns that will	be sent to th	ne relying p	arty.		
	Order	Rule Name				Issued Claim	15			
										_
									1	
										,
	Add F	Rule Edit	Rule	Remove	Rule					
L										
					0	ĸ	Cancel		Арр	у

4. Select Send Claims Using a Custom Rule option from the Claim rule template drop-down menu.

%	Add Transform Claim Rule Wizard
Select Rule Template	
Select Rule Template Steps Choose Rule Type Configure Claim Rule	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template. Claim rule template: Send LDAP Attributes as Claims Send Group Membership as a Claim Transform an Incoming Claim Pass Through or Filter an Incoming Claim Send Glaims Using a Custom Rule Multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
	< Previous Next > Cancel

- 5. Specify the following values:
 - Claim rule name: Account Id
 - Custom rule: => issue(Type = "https://secure.netop.com/NRC-ACCOUNT-ID", Value = "<Account identifier>");

Make sure that you replace the **<Account identifier>** with the account identifier that you use in the **Netop Portal** (in this example, the **"my-identifier")** is used as the account identifier.

\$	Add Transform Claim Rule Wizard
Configure Rule	
Steps • Choose Rule Type • Configure Claim Rule	You can configure a custom claim rule, such as a nule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom nule, type one or more optional conditions and an issuance statement using the AD FS claim nule language. [daim nule name: Account Id Rule template: Send Claims Using a Custom Rule Cystom nule: -> issue (Type = "https://secure.netop.com/NRC-ACCOUNT-ID", Value = "my-identifier");
	< <u>P</u> revious Finish Cancel

6. Click on **Finish**.

7. In the Edit Claim Rules for <relying party> dialog box, click on the Add Rule button.

\$	Edit Claim Rules for Netop Portal	- 🗆 X
lss	ssuance Transform Rules Issuance Authorization Rules Delegation Authority	orization Rules
	The following transform rules specify the claims that will be sent to the relyin	ng party.
	Order Rule Name Issued Claims	
	1 Account Id <see claim="" rule=""></see>	
	Add Rule Edit Rule Remove Rule	
	OK Cance	el Apply

8. Select Send Claims Using a Custom Rule option from the Claim rule template drop-down menu.

\$	Add Transform Claim Rule Wizard
Select Rule Template	
Steps Choose Rule Type Configure Claim Rule	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template. Gaim rule template: Send Claims Using a Custom Rule Caim rule template description: Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include: Sending claims from a SQL attribute store Sending claims from a CuStom attribute store using a custom LDAP filter Sending claims from a custom attribute store using a custom LDAP filter Sending claims only when a nincoming claim value matches a complex pattem Sending claims with complex changes to an incoming claim value (Creating claims for use only in later rules)
	< Previous Next > Cancel

- 9. Specify the following values:
 - Claim rule name: Name Id
 - Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname
"]
```

```
=> issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
ValueType = c.ValueType,
```

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent");

9	Add Transform Claim Rule Wizard	x
Configure Rule		
Steps Configure Rule Type Configure Claim Rule	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extract claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language. Qaim rule name: Name Id Rule template: Send Claims Using a Custom Rule Custom rule: c: [Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name"] => issue (Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format "] = "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent");]	s
	< Previous Finish Cancel	

10. Click on Finish.

11. In the Edit Claim Rules for <relying party> dialog box, click on Add Rule.

Ŷ		E	dit Claim Rul	es for Ne	etop Portal	-		x
Iss	suance T	Transform Rules	Issuance Authoriz	ation Rules	Delegation Authoriza	tion R	ules	
	The follo	wing transform n	lles specify the clai	ms that will t	be sent to the relying pa	arty.		
	Order	Rule Name			lssued Claims]	
	1	Account Id		•	<see claim="" rule=""></see>			
	2	Name iu			<see claim="" rule=""></see>			
								_
							1	
]	
	<u>A</u> dd R	Lule Edit F	Rule	e Rule				
				OF	Cancel		Арр	ły

12. Select Send LDAP Attributes as Claims from the Claim rule template drop-down menu.

\$	Add Transform Claim Rule Wizard				
Select Rule Template					
Steps Ghoose Rule Type	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.				
Configure Claim Rule	Gaim rule template:				
	< Previous Next > Cancel				

- 13. Specify the following values.
- Claim rule name: User details
- Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP attribute	Outgoing Claim Type
E-Mail-Addresses	https://secure.netop.com/NRC-EMAIL
Given-Name	https://secure.netop.com/NRC-GIVEN-NAME
Surname	https://secure.netop.com/NRC-SURNAME
User-Principal-Name	https://secure.netop.com/NRC-USERNAME

\$	Add Transform Claim Rule Wizard				x
Configure Rule					
Steps Choose Rule Type Configure Claim Rule	You c: which issued Qlaim I User d Attribu Active Mappi	an configure this rule to send the values of to extract LDAP attributes. Specify how the from the rule. rule name: letails emplate: Send LDAP Attributes as Claims te gtore: e Directory ng of LDAP attributes to outgoing claim typ LDAP Attribute (Select or type to add more) E-Mail-Addresses Given-Name Sumame User-Principal-Name		DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be v : Outgoing Claim Type (Select or type to add more) https://secure.netop.com/NRC-GIVEN-NAME https://secure.netop.com/NRC-SURNAME https://secure.netop.com/NRC-USERNAME]	
				< <u>P</u> revious Finish Cancel	

14. Click on Finish.

15. Click on OK.

\$ 1	E	dit Claim Rเ	ules for N	etop Portal	-		x
Issuance	Transform Rules	Issuance Autho	rization Rules	Delegation Authori	zation R	ules	
The foll	owing transform n	ules specify the c	laims that will	be sent to the relying	party.		
Order	Rule Name			Issued Claims			
1	Account Id			<see claim="" rule=""></see>			
2	Name Id			<see claim="" rule=""></see>			
3	User details			https://secure.netop	.com		
Add I	Rule	Rule	ove Rule			1	•
			0	K Cancel		Appl	y

16. You finished with the necessary configuration on the ADFS server.

Configure the Netop Portal

To configure the ADFS integration with the Netop Portal, proceed as follows:

- 1. Sign in the **Netop Portal** with an Account administrator type of user.
- 2. Go to **Dashboard**.
- 3. Go to Authentication.
- 4. Click on the Add ADFS / Azure AD button.
- 5. Specify a name for the Authentication type.
- 6. Toggle the **Enable** button, to enable or disable the authentication type. By default, it is set to **Enable**.
- 7. In the Domain Identifier field, specify the same value that you used in creating the Account Claim rule.
- 8. In the **IdP** entry field, specify the Identity Provider's (IdP) URL. This is the ADFS URL used for authenticating the user.

NOTE: The default value is

https://somedomain.com/adfs/ls/IdpInitiatedSignOn.aspx.

9. Specify a group for the authentication. This is an optional step.

10. Browse for the ADFS FederationMetadata.xml file. The ADFS FederationMetadata.xml file is specific to ADFS based on the various settings. It can generally be retrieved from https://somedomain.com/FederationMetadata.xml file. The ADFS FederationMetadata.xml file is specific to ADFS based on the various settings. It can generally be retrieved from https://somedomain.com/FederationMetadata.xml file. The ADFS FederationMetadata.xml file is specific to ADFS based on the various settings. It can generally be retrieved from https://somedomain.com/FederationMetadata/2007-06/FederationMetadata.xml.

NOTE: When uploading the FederationMetada.xml, the embedded certificate is parsed and its validity interval is displayed (Certificate valid from – Certificate valid to).

Remote Control	A ADD AUTHENTICATION METHOD Close ×	Logged in as Marius N
«		
.	Mame My ADFS	dd authentication method
M29 Dashboard	Enabled (This authentication method is enabled)	
ACCOUNT	ADFS V 0	hentication method identifier
Authentication	Domain identifier	
Deployments	This will be used when logging in (domain identifier/username)	e 1 1-1 of 1 < >
MANAGE		
🕰 Users	https:// /adfs/ls/ldplnitiated:	
i ⊂ Roles	Group V	
Role assignments	The user will become a member of this group on first login.	
ACCESS	ADFS FederationMetadata.xml file Browse	
	Certificate valid from 2017-03-10 11:33	
	More information on how to integrate with ADFS is available here	
	۹, Save	
Netop		

11. To save your modifications, click on **Save**.

Remote session using ADFS

Prerequisites:

- **Guest** and **Host** are version 12.60 or later
- Role assignments that are defined in the Netop Portal that allow ADFS based users to connect to the Host
- Make sure the Host is configured to Use Netop Portal access rights

Managing the ADFS users

8 Remote Control Chat with Netop 🐂 Purchase Seats: 14/999 Logged in as TEAM Account Admin « All Users (1) 1 Add user 🖶 Add group Dashboard Filter by name: some **x** Clear all the filters Name Ŧ Туре T Group T Authentication method Ŧ Modified Configuration Some User User ххх my adfs 2017-05-12 04:22:58 Authentication Show Rows 10 👻 1-1 of 1 < > Go to page 1 Deployments 🗥 Users 🖵 Devices \equiv Roles 6 몱 Role assignments 🖵 My devices

On the first login using ADFS, a user gets created into the Netop Portal. The user type is User.

The new user works like a regular user, except:

- The user cannot change his password, first name, and email from the **Netop Portal**, which are synced with the ADFS server
- The user cannot be set as an Account owner
- The user cannot be used for the phonebook as predefined credentials