

Powered by



FCS IaaS Tutorial FCS SAML auth. with Azure-AD (incl. Multi-Factor-Authentication)



#### INHALTSVERZEICHNIS

VORAUSSETZUNGEN	3
VORWORT	3
VORGEHEN	4
OPTIONAL: MULTI-FAKTOR-AUTHENTIFIZIERUNG (MFA) AKTIVIEREN	14



### Voraussetzungen

- aCMP Customer-Org-Global-Admin Login
- Azure AD Connect, falls On-Prem AD verwendet wird
- Azure AD Premium P1 (oder höher), falls Azure MFA verwendet wird

#### Vorwort

Wir freuen uns Ihnen hier das aCMP Feature "FCS SAML auth with Azure-AD" vorzustellen, welches es Ihnen ermöglicht Ihr ggf. bestehendes Azure-AD als zentrale Identitätsquelle für die Anmeldung an Ihrem FCS IaaS Tenant zu nutzen. Sollten Sie bisher MFA über "FCS VMWare Verify" genutzt haben, steht Ihnen die kostenfreie Umstellung auf "FCS SAML auth with Azure-AD" jederzeit offen, unser IOC unterstützt Sie gerne bei einer Migration.

Im Folgenden finden Sie eine Schritt-für-Schritt Anleitung zur Ersteinrichtung der Azure-AD Anbindung in Ihrem FCS IaaS Tenant. Dazu finden Sie ab sofort einen neuen Menüpunkt unter Administration:

Focusnet Cloud Servi	tes laaS Data Centers Applications Networking Libraries Administration Monitor More V
《 答 Access Control ~	SAML Configuration
Users	✓ Service Provider
Groups	Entity ID
Roles	Metadata
🕹 Identity Providers 🗸 🗸	Certificate Expiration 01/11/2022, 11:23:19 PM
SAML	✓ Identity Provider
🖾 Certificate Manage 🗸	SAML identity Provider enabled faise
Trusted Certificates	Metadata XIML -
Certificates Library	
⊗ Settings ∨	
General	
Pres e 3	



# Vorgehen

1. Erstellen Sie eine Gruppe (Azure AD oder On-Prem) mit einer passenden Bezeichnung.

Wichtig: On-Prem Gruppen müssen nach Azure AD synchronisiert werden.

igenschaf	iten von SG	_IT_FCS_aCM	P_CloudAdmins	?	×			
Allgemein	Mitglieder	Mitglied von	Verwaltet von					
SG_IT_FCS_aCMP_CloudAdmins								
Gruppenname (Prä-Windows 2000): SG_IT_FCS_aCMP_CloudAdmins								
Beschreit	bung: Fo	cusnet Cloud	Services laaS Administra	atoren				
E-Mail:								
Gruppe	nbereich		Gruppentyp					
O Lokal (in Domäne)			<ul> <li>Sicherheit</li> </ul>					
Global			◯ Verteilung					
		◯ Universal						

(Beispiel On-Prem)

Wichtig: Bei Azure AD Gruppen (Cloud Only) muss die Object-ID in Schritt 13 und 15 eingefügt werden anstatt des Namens:

6	SG_IT_FCS_aCMP_CloudAdmins								
	«	📋 Delete 🛛 💀 Preview features 🖤 Got feedback?							
0	Overview	🔗 This page includes province scalab							
×	Diagnose and solve problems	Inis page includes previews availab	te for your evaluation. View previews ->						
Manage		SG IT FCS	aCMP CloudAdmins						
0	Properties	SG							
24	<u>Members</u>								
24	Owners								
2	Administrative units	Membership type	Assigned						
<b>\$</b>	Group memberships	Source	Windows server AD	D					
	Applications	Туре	Security	D					
ů	<u>Licenses</u>	Object Id		D					



- 2. Melden Sie sich mit Ihrem lokalen Customer-Org-Global-Admin an der FCS aCMP an.
- **3.** Wechseln Sie zur Registerkarte «Administration» und wählen Sie unter «Identitätsanbieter» > «SAML». Klicken Sie unter SAML-Konfiguration auf «Bearbeiten».

Focusnet Cloud Services laaS Data Centers Applications Networking Libraries Administration Monitor More ~								
答 Access Control	~	SAML Configuratio	n					
Users		✓ Service Provider						
Groups		Entity ID						
Roles		Metadata						
🖧 Identity Providers	~	Certificate Expiration				01/11/	2022, 11:23:19 PM	1
SAML		V Identity Provider						
🖾 Certificate Manage	~	SAML Identity Provider er	nabled			false		
Trusted Certificates		Metadata XML				-		
Certificates Library								
Settings	~							
General								
E an a l								

4. Als Entitäts-ID wird die Metadaten URL kopiert und eingefügt

SAML Configuration	
EDIT	
✓ Service Provider	
Entity ID	https://iaas.cloud.focusnet.de/ /saml/metadata/alias/vcd
Metadata	https://iaas.cloud.focusnet.de/ /saml/metadata/alias/vcd
Certificate Expiration	04/27/2022, 11:40:08 AM

5. Generieren Sie ein neues Zertifikat, indem Sie auf «Neu Generieren» und danach «Speichern» klicken.

Service Provider	Identity Provider		
intity ID •	https://iaas.cloud.focusnet.de/	'saml/metadata/alias/vcd	
	Your service provider entity ID.		
Certificate	04/27/2022, 11:40:08 AM	REGENERAT	E
	This certificate is used to sign federation expired certificate might disable the fede	messages and is valid up to 1 year from the time of creation. An eration with the identity provider setup for this organization.	
	Entity ID ist die Metada	ta URL	



6. Laden Sie die XML-Datei «spring\_saml\_metadata.xml» herunter.

SAML-Konfiguration			
BEARBEITEN			
✓ Dienstanbieter			
Entitäts-ID	Download startet, sobald auf/den	https://	saml/metadata/alias/vcd
Metadaten		https://	saml/metadata/alias/vcd
Zertifikatablauf	Öffnen von spring_saml_metadata.xml X	04.11.2021, 11:10:23 AM	
∨ Identitätsanbieter	Sie möchten folgende Datei öffnen:		
SAML-Identitätsanbieter akt	<ul> <li>spring_saml_metadata.xml</li> <li>Vom Typ: Extensible Markup Language (XML) (4.1 KB)</li> </ul>		
Metadaten-XML			
	Wie soll Firefox mit dieser Datei verfahren?		
	○ <u>Ö</u> ffnen mit Applications\Code.exe (Standard) ∨		
	Datei speichern		
	<u>F</u> ür Dateien dieses Typs immer diese Aktion ausführen		
	OK Abbrechen		

7. Melden Sie sich im Azure AD an und erstellen Sie eine neue Enterprise Application.





8. Geben Sie Ihrer neuen Applikation einen sinnvollen Namen und klicken Sie auf «Create».

Create your own application	×
What's the name of your app? FCS_aCMP_SSO	
What are you looking to do with your application?         O Configure Application Proxy for secure remote access to an on-premises application         O Register an application to integrate with Azure AD (App you're developing)	n
Integrate any other application you don't find in the gallery (Non-gallery)	

9. Fügen Sie die im ersten Schritt erstellte AD-Gruppe hinzu (On-Prem AD oder Azure AD).

Ho	ome > Enterprise ap	pplications > FCS aCMP SSO							
	Erterprise Application								
Щ Ма 44 Э Ф	« Overview Deployment Plan anage Properties Owners Roles and administrators (Preview) Users and groups Single sign-on Provisioning	Add user/group     C Edit      Remove      Update Credentials     I      The application will appear for assigned users within My Apps. Set Visible to users     First 100 shown, to search all users & groups, enter a display name.     Display Name     SG IT FCS aCMP CloudAdmins	Columns ♡ Got feedback? ?' to no in properties to prevent this. →	Object Type Group					
-	Application proxy								
0	Self-service								
Se	curity								
•	Conditional Access								
÷	Permissions								
٢	Token encryption								
Ac	tivity								
Э	<u>Sign-ins</u>								
αá	Usage & insights								
	Audit logs								
÷	Provisioning logs (Preview)								
ŝ≡	Access reviews								



FocusNet Cloud Services / SAML auth. with Azure-AD 04/2021

10. Klicken Sie auf «Single sign-on» und wählen Sie als Authentifizierung SAML aus.

Ho	me > Enterprise	applications >	FCS aCMP SSO					
5	FCS_aCMP_SSO   Si	ngle sigr	n-on …					
-	Enterprise Application							
щ	« Overview	Select a	a single sign-on method	<u>Help</u>	<u>me decide</u>			
Ш	Deployment Plan				•		0	
Ма	nage	Disabled			{3	SAML	日	Password Password
10	Properties		won't be able to launch the app from My Apps			applications using the SAML (Security Assertion Markup Language) protocol		web brows
24	Owners		mj ripps.			Assertion markup canguage) protocol.		
2.	Roles and administrators (Preview)							
- 24	Users and groups			_				
Э	Single sign-on							
٢	Provisioning							
8	Application proxy							
0	Self-service							
Sec	curity							
•	Conditional Access							
4	Permissions							
٢	Token encryption							
Act	livity							
Э	<u>Sign-ins</u>							
άá	Usage & insights							
	Audit logs							
2	Provisioning logs (Preview)							
\$≡	Access reviews							

**11.** Im nächsten Schritt können Sie die XML Datei, welche Sie in Ihrem Tenant aus der aCMP heruntergeladen haben, in der neu erstellte Azure AD Enterprise App hochladen.

Home > Enterprise applications > FCS aCMP SSO >									
FCS_aCMP_SSO   SAML Enterprise Application	-based Sign-on								
«	$ar{\uparrow}$ Upload metadata file $$ Change single sign-or	n mode 🛛 i 🗮 Test this application 🛛 🛇 Got feedback?							
Deployment Plan	Upload metadata file. Values for the fields below are provided by FCS_aCMP_SSO. You may either enter those values manually, or upload a pre-con								
Manage									
Properties	Select a file								
A Owners	Add Cancel								
Roles and administrators (Preview)	Reply URL (Assertion Consumer Service URL)	Required							
Users and groups	Sign on URL	Optional							
	Relay State Logout Url	Optional Optional							
Provisioning									
B Application proxy	2 User Attributes & Claims	🖉 Edit							
Self-service	givenname	user.givenname							
Security	surname emailaddress	user.sumame user.mail							
Conditional Access	name	user.userprincipalname							
Permissions	onque oser reentiner	user user principalitative							
Token encryption	3 SAML Signing Certificate	A = v.							



**12.** Unter «User Attributes & Claims» können Sie nun einen neuen Claim hinzufügen.

Fügen Sie die folgenden Claims hinzu:

- Name: EmailAddress, Source attribute: user.mail
- Name: FullName, Source attribute: user.displayname
- Name: UserName, Source attribute: user.mail

Die automatisch durch Azure erstellten Claims können gelöscht werden.

Home > Enter	prise applications > FCS aCMP	SSO > SAML-based Sign-on	> User Attributes & Claims >
--------------	-------------------------------	--------------------------	------------------------------

Manage claim		Groß- und	Kleinschreibung mus	is
🔚 Save 🗙 Discard changes	4	beachtet v	verden	~
Name *	UserName			
Namespace	Enter a namespace URI			
Source *	<ul> <li>Attribute</li></ul>	formation		
Source attribute *	user.mail			
<ul> <li>Claim conditions</li> <li>Returns the claim only if all the conditions</li> </ul>	below are met.			
() Multiple conditions can be applied to	a claim. When adding condition	ons, order of operation is im	portant. <u>Read the documentation</u> for mo	re information.
User type	S	coped Groups	Source	
Select from drop down	✓ S	Select groups	Attribute	O Transformation



**13.** Fügen Sie nun einen Group Claim hinzu:

Group Claims	×
Manage the group claims used by Azure AD to p	oopulate SAML tokens issued to your app
Which groups associated with the user should l	be returned in the claim?
All groups	
Security groups	
<ul> <li>Directory roles</li> </ul>	
<ul> <li>Groups assigned to the application</li> </ul>	Bei On-Prem-AD Gruppen
Source attribute *	muss hier der Name
sAMAccountName	Verwendet werden, bei
This source attribute only works for groups using AAD Connect Sync 1.2.70.0 or above	expected by the synchronized from an on-premises Active Directory
Advanced options	
Customize the name of the group clain	n
Name (required)	
Groups	
Namespace (optional)	
Emit groups as role claims ①	

Sie erhalten danach eine Übersicht über alle Claims, alle zuvor automatisch erstellten Azure-Standard-Claims können gelöscht werden. Das Endergebnis sollte so aussehen:

Required claim		
Claim name	Value	
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for	***
Additional claims		
Claim name	Value	
EmailAddress	user.mail	•••
FullName	user.displayname	•••
Groups	user.groups	•••
UserName	user.mail	•••



# 14. Nun können Sie die erzeugte FCS\_aCMP\_SSO XML-Datei herunterladen.

	-			
Overview	<u></u> Υι	Ipload metadata file 7 Change single	sign-on mode 🛛 🗮 Test this application 🗌 🗸	Got feedback?
Deployment Plan	Set u	p Single Sign-On with SAM	L	
lanage	Read	the configuration guide 🗟 for help integr	rating FCS_aCMP_SSO.	
Properties	1	Basic SAMI Configuration		
<u>Owners</u>		basic shine configuration		🖉 Edit
Roles and administrators (Preview)		and the second se		
Users and groups		10 M 10		
Single sign-on				
Provisioning				
Application proxy	2	User Attributes & Claims		🖉 Edit
Self-service		EmailAddress	user.mail	
curity		FullName	user.displayname	
		Groups	user.mail user.groups	
Conditional Access		Unique User Identifier	user.userprincipalname	
Permissions				
Token encryption	3	SAML Signing Certificate		0
tivity				C Edit
Sign-ins		and the second s	CONTRACTOR OF THE OWNER.	
Usage & insights		the second se		
Audit logs				
Provisioning logs (Preview)		Certificate (Base64)	Download Download	
· · · · · · · · · · · · · · · · · · ·		Federation Metadata XML	Download	



**15.** Nach dem Download der XML-Datei aus dem Azure-AD-Portal müssen Sie diese nun in Ihrem aCMP-Tenant hochladen:

Focusnet Cloud Se				
魯 Access Control		EDIT	Edit SAML Configuration	×
Users		V Service Provider		
Groups		Entity ID	Service Provider	
Roles		Metadata	Use SAML Identity Provider: Your identity provider authenticates users in this organization. Enter the SAML v2.0 metadata for the service. The metadata	
ldentity Providers		Certificate Expiration	must include the location of the single sign-on service, the single logout service, and the X.509 certificate of the service. You can provide the metadata by pasting the XML in the field below or by uploading a file containing the XML.	
SAML		V Identity Provider	Browse:	
Certificate Manage		SAML Identity Provider enabled	Matadata VMI -	
Trusted Certificates		Metadata XML	metauata Amu.	
Certificates Library				
Settings				
General				
Email				
Guest Personalization				
Metadata				
Recent Tasks			·	
Task				
Disabled User (71271169-0047-416e-9bd6-3ce948ea65c6)		d6-3ce948ea65c6)	DISCARD SAVE	
Disabled User (16eb9822-ee98-		5b0-d79c445f3571)		



**16.** Als letzter Schritt steht noch der Import der initial erstellten On-Prem-AD-Sicherheitsgruppe(n) aus, welche zur Anmeldung über die Azure-AD Authentifizierung berechtigt ist/sind. Sollte es sich um reine Azure-AD Gruppen handeln, muss statt dem Namen die Group-ID hier eingetragen werden:

ervices laaS	Resources Libraries	Administration Monitor	More∨	
~ Gro	Import Groups			×
IMP	(i) No quota will be cr each of the import	eated for selected groups. You ed groups from the group list	u can create a quota for or group's details view.	
	Source	SAML	~	
	Enter the group		t & startin al	
<b>~</b> 0	names *	SG_II_FCS_aCMP_Cloud	IAdmins	AP
$\sim$				
~				
~				
			//	
		Group names must be in the nai supported by the SAML identity organization. Use a new line for	me identifier format v provider configured for this each group name.	
	Assign Role *	Select a role	~	
)-4f4d-8901-57d				r-adr
-416e-9bd6-3ce				/F
8-4f25-a5b0-d79			DISCARD	

Hinweis: Wenn sie unterschiedliche Berechtigungsgruppen in Ihrem FCS laaS Tenant nutzen, z.B. für den Zugriff auf unterschiedliche VDCs, müssen Sie diese Gruppen entsprechend im Azure-AD abbilden und die Berechtigungen an den VDCs anhand der Azure-AD-Gruppen setzen.



### Optional: Multi-Faktor-Authentifizierung (MFA) aktivieren

Optional können Sie die Multi-Faktor-Authentifizierung (MFA) aktivieren. Bitte beachten Sie, dass Sie dafür die Azure AD Premium P1 Lizenz benötigen.

1. Klicken Sie im Azure Portal unter «Enterprise applications > FCS\_aCMP\_SSO > Conditional Access» auf «New policy».

Home > Enterprise applications > FCS aCMP_SSO						
	ECS_aCMP_SSO   Conditional Access					
	Enterprise Application					
щ	Overview					
	Deployment Plan	Try out the new Conditional Access search, so	rt and filter preview!			
Ma	nage	What is conditional access?				
Ш	Properties	Conditional Access gives you the ability to enforce	e access requirements when specific conditions occur. Let's take a few examples	5		
24	Owners	Conditions	Controls			
2.	Roles and administrators (Preview)	When any user is outside the company network	They're required to sign in with multi-factor authentication			
24	Users and groups	When users in the 'Managers' group sign-in	They are required be on an Intune compliant or domain-joined device			
€	Single sign-on	Want to learn more about conditional access?				
æ	Provisioning	Get started				
	Application prove	Create your first policy by clicking "+ New     Specify policy Conditions and Controls	Create your first policy by clicking "+ New policy"			
	Application proxy	When you are done, don't forget to Enable	e policy and Create			
0	<u>Self-service</u>	Interested in common scenarios?				
Sec	curity					
•	Conditional Access					
Å	Permissions					
٥	Token encryption					
Act	livity					
Э	<u>Sign-ins</u>					
άá	Usage & insights					
	Audit logs					
Ľ	Provisioning logs (Preview)					
ś≡	Access reviews					



2. Benennen Sie die Policy und wählen Sie die User aus, die sich künftig mit MFA authentifizieren sollen.





3. Wählen Sie im nächsten Schritt unter «Cloud apps» die «FCS\_aCMP\_SSO» Applikation.

Home > Enterprise applications > FCS aCMP SSO >				
Control user access based on all or specific cloud apps or actions. <u>Learn more</u> Select what this policy applies to Cloud apps User actions				
Include Exclude				
<ul> <li>None</li> <li>All cloud apps</li> <li>Select apps</li> </ul>				
Select FCS_aCMP_SSO				
FCS_aCMP_SSO 6826a712-5fc5-42a1-b4fe-364a793b11				



4. Anschließend können Sie unter «Grant» die Option «Require multi-factor authentication» auswählen.

Home > Enterprise applications > FCS aCMP SSO >	Grant ×
New	
Conditional access policy	Control user access enforcement to block or grant access. <u>Learn more</u>
Control user access based on conditional access policy to bring signals together, to	Block access
make decisions, and enforce organizational policies. <u>Learn more</u>	• Grant access
Name *	Require multi-factor authentication ①
FCS_aCMP_MFA	Require device to be marked as compliant ①
Assignments	Require Hybrid Azure AD joined
Specific users included	device ①
 Cloud apps or actions ①	Require approved client app ① See list of approved client apps
1 app included	Require app protection policy ① See list of policy protected client apps
Conditions ①	Require password change
0 conditions selected	
Access controls	For multiple controls
Grant 🛈	<ul> <li>Require all the selected controls</li> </ul>
0 controls selected	Require one of the selected controls
Session ①	



5. Stellen Sie sicher, dass die Policy aktiviert ist (On) und klicken Sie auf «Create».

Home > Enterprise applications > FCS aCMP SSO >
New
Conditional access policy
Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. <u>Learn more</u>
Name *
FCS_aCMP_MFA ✓
Assignments
Users and groups ①
Specific users included
Cloud apps or actions ①
1 app included
Conditions ①
0 conditions selected
Access controls
Grant ①
1 control selected
Session ①
Enable policy Report-onl Off

"FCS SAML auth with Azure-AD" ist nun vollständig eingerichtet und Sie werden beim Aufrufen Ihres FCS IaaS Tenants zur Azure-Authentifizierung umgeleitet.





Bei Fragen stehen wir jederzeit gerne zur Verfügung und wünschen Ihnen nun viel Freude und Erfolg mit Ihrer hochverfügbaren Infrastruktur!

Ihre

