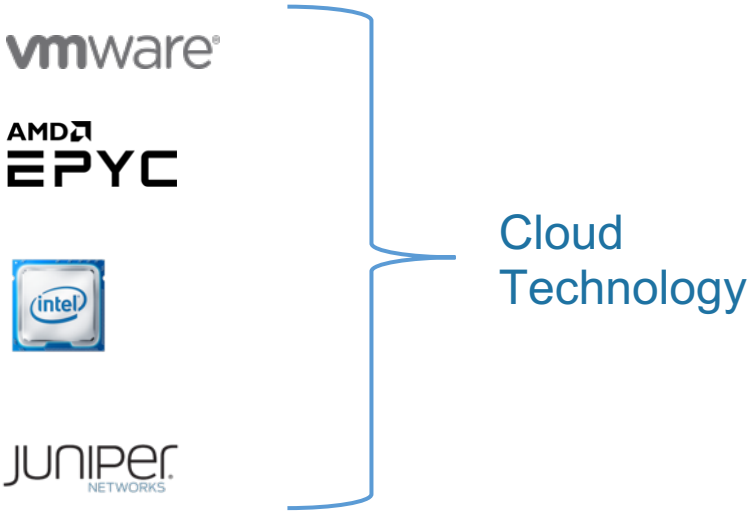
focusnet

CLOUD SERVICES

Powered by



FCS IaaS Tutorial

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

INHALTSVERZEICHNIS

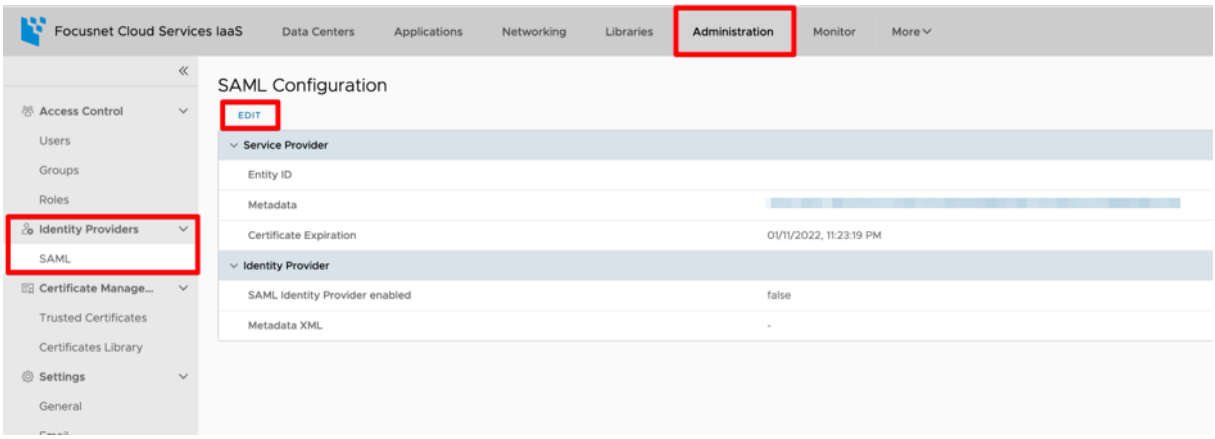
Voraussetzungen

- 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.

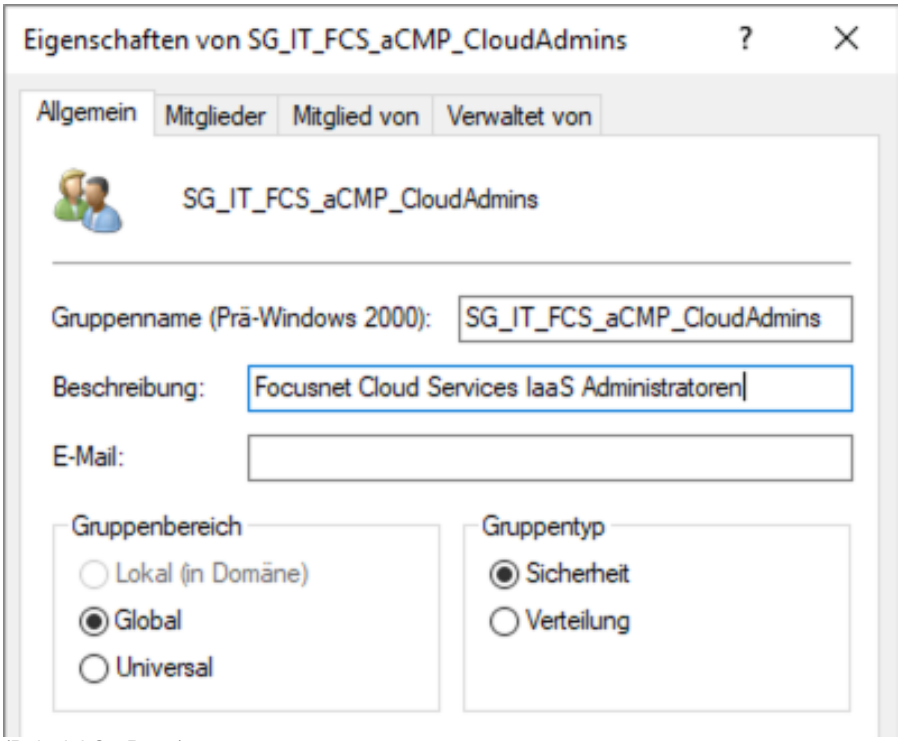
Im Folgenden finden Sie eine Schritt-für-Schritt Anleitung zur Ersteinrichtung der Azure-AD Anbindung in Ihrem FCS IaaS Tenant. Dazu finden Sie ab sofort einen neuen Menüpunkt unter Administration:



Vorgehen

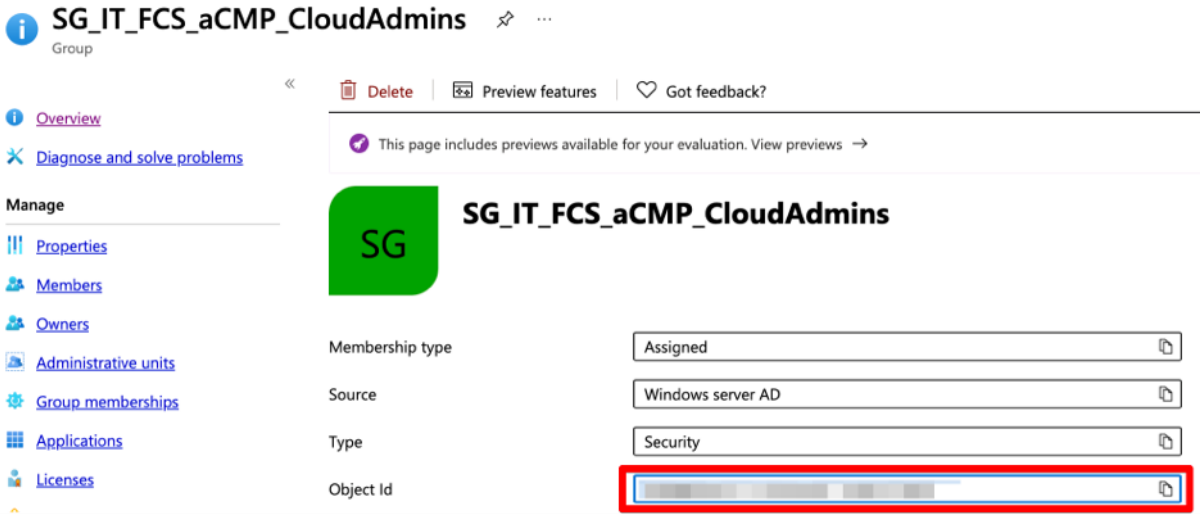
1. Erstellen Sie eine Gruppe (Azure AD oder On-Prem) mit einer passenden Bezeichnung.

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



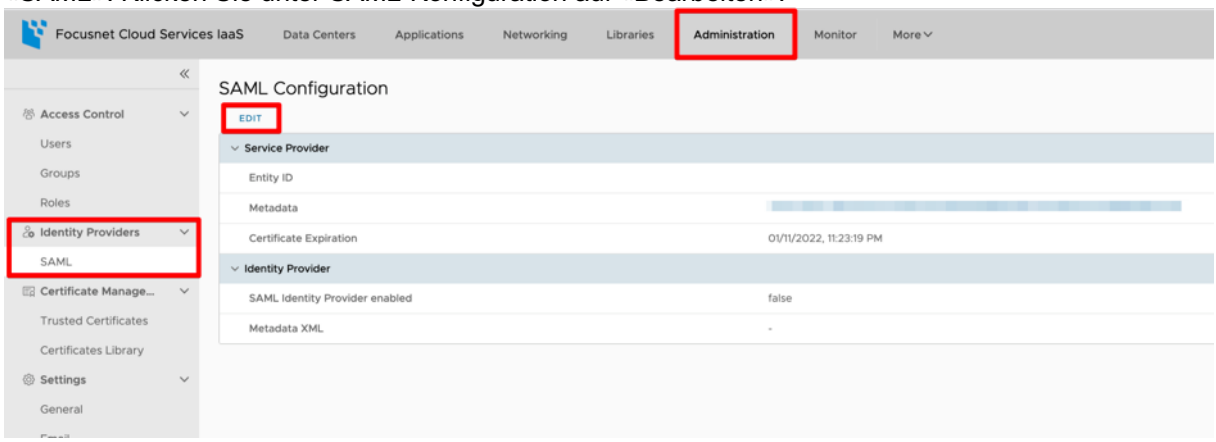
(Beispiel On-Prem)

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



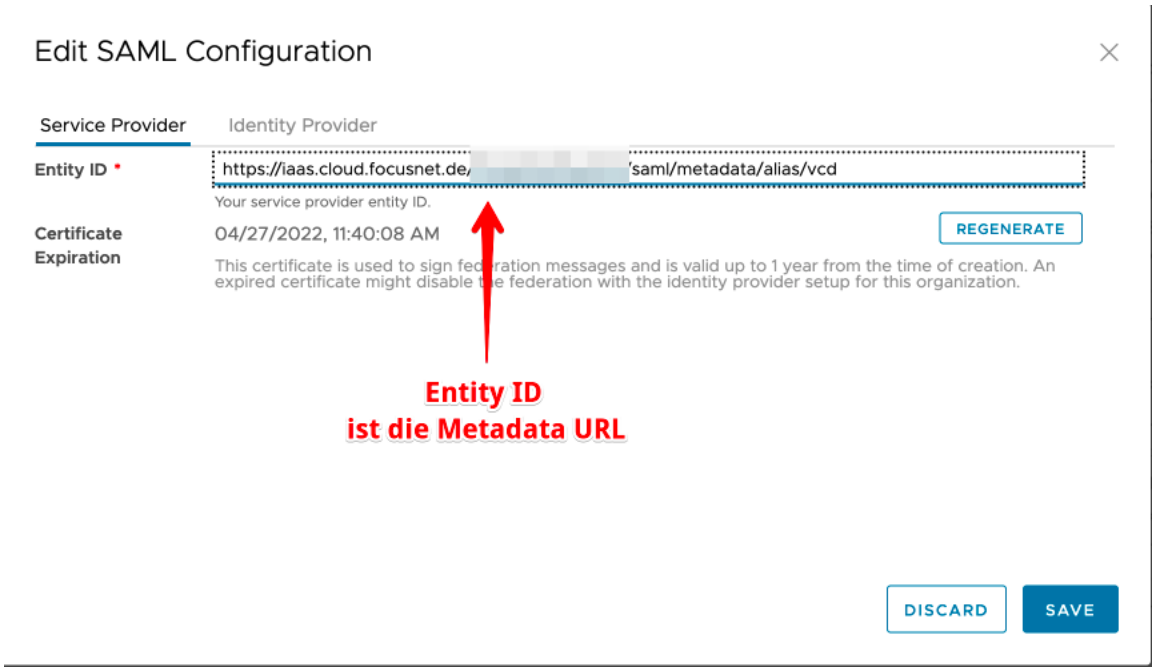
2. Melden Sie sich mit Ihrem lokalen Customer-Org-Global-Admin an der FCS aCMP an.

3. Wechseln Sie zur Registerkarte «Administration» und wählen Sie unter «Identitätsanbieter» > «SAML». Klicken Sie unter SAML-Konfiguration auf «Bearbeiten».

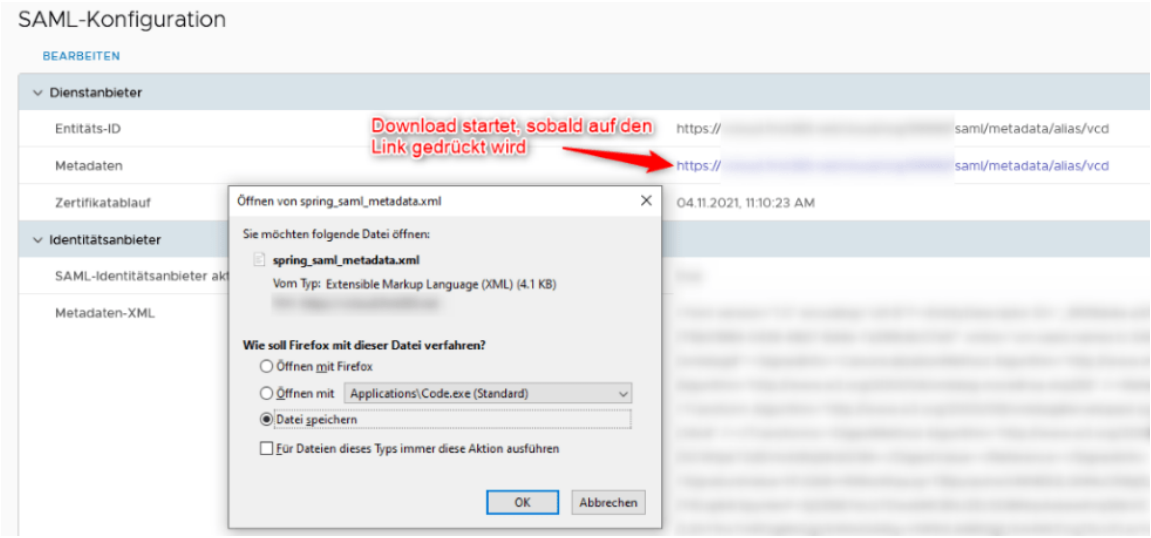


4. Als Entitäts-ID wird die Metadaten URL kopiert und eingefügt

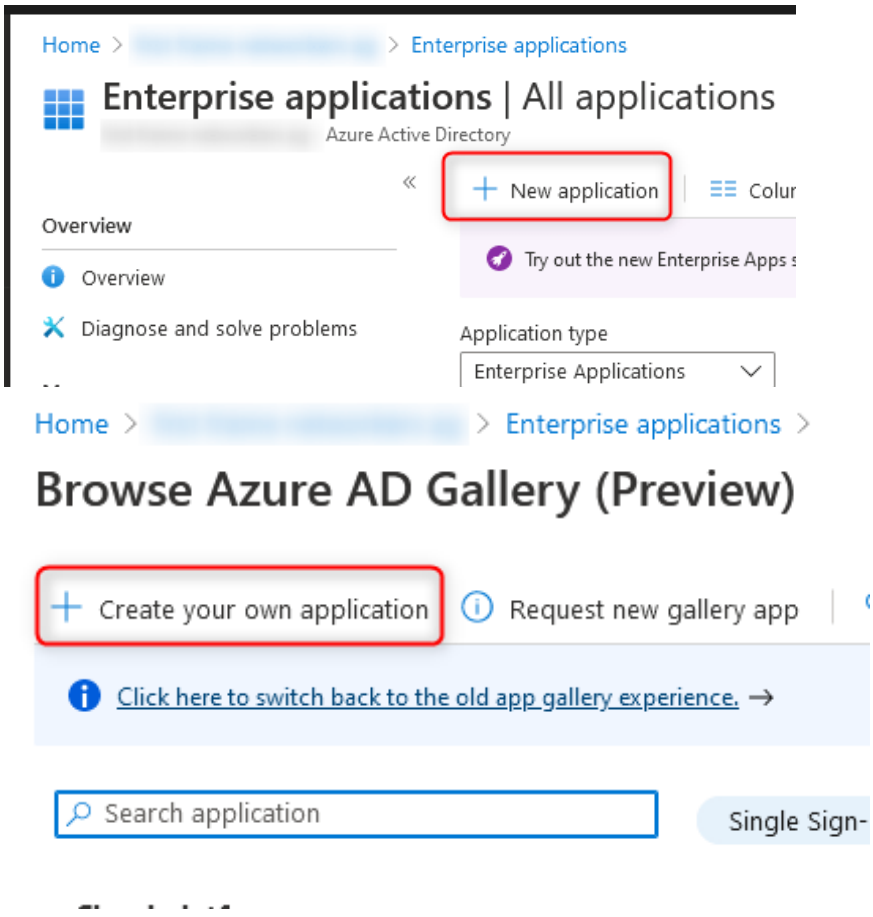
5. Generieren Sie ein neues Zertifikat, indem Sie auf «Neu Generieren» und danach «Speichern» klicken.



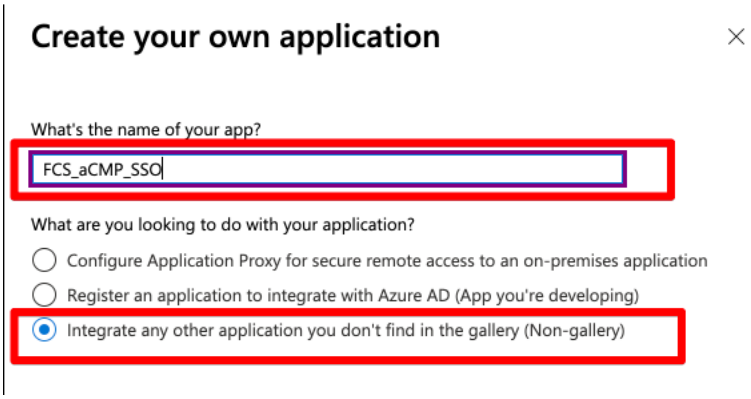
6. Laden Sie die XML-Datei «spring_saml_metadata.xml» herunter.



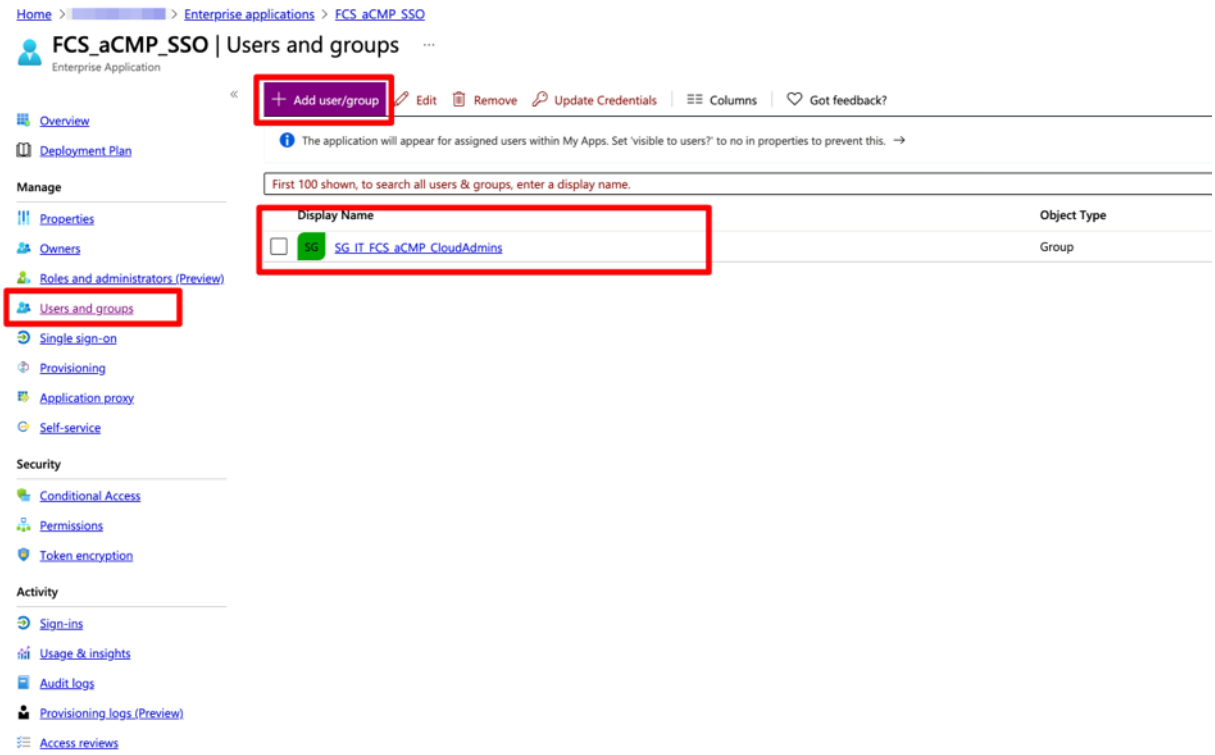
7. Melden Sie sich im Azure AD an und erstellen Sie eine neue Enterprise Application.



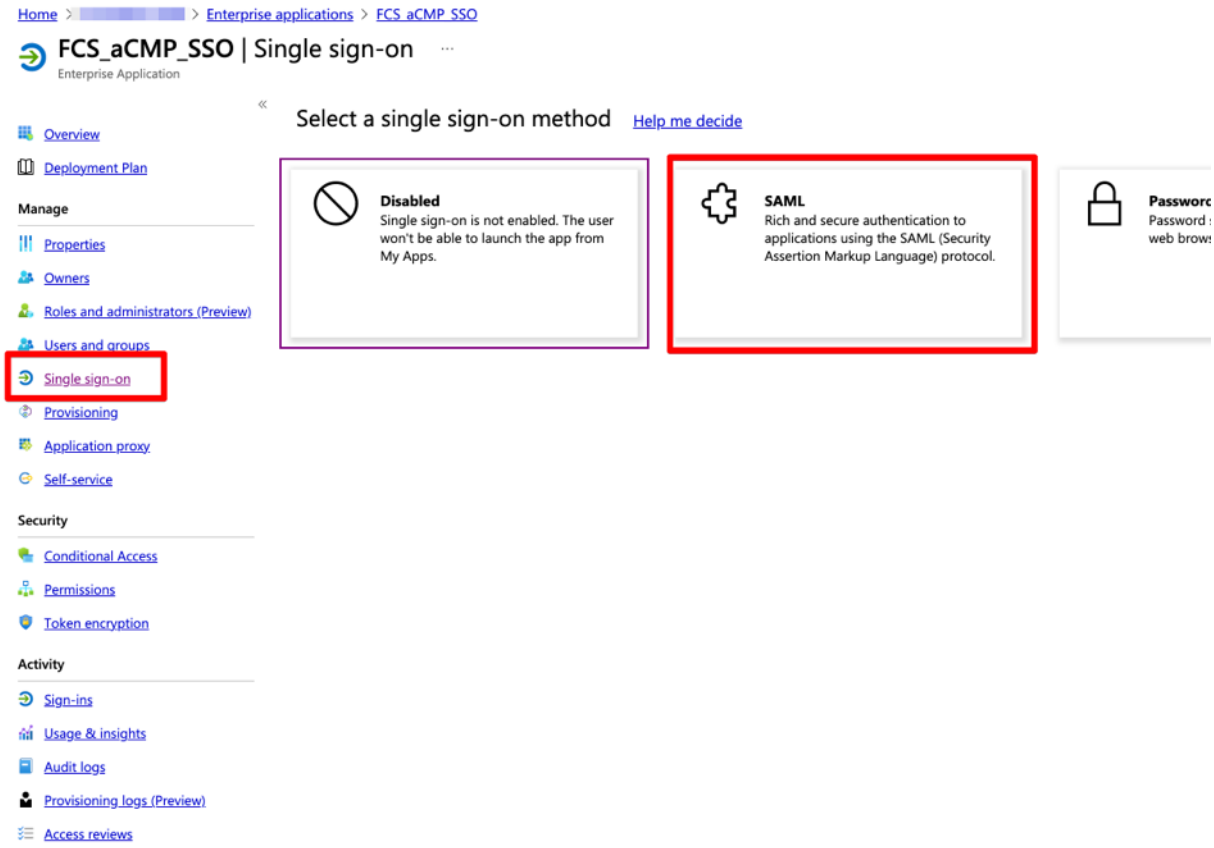
8. Geben Sie Ihrer neuen Applikation einen sinnvollen Namen und klicken Sie auf «Create».



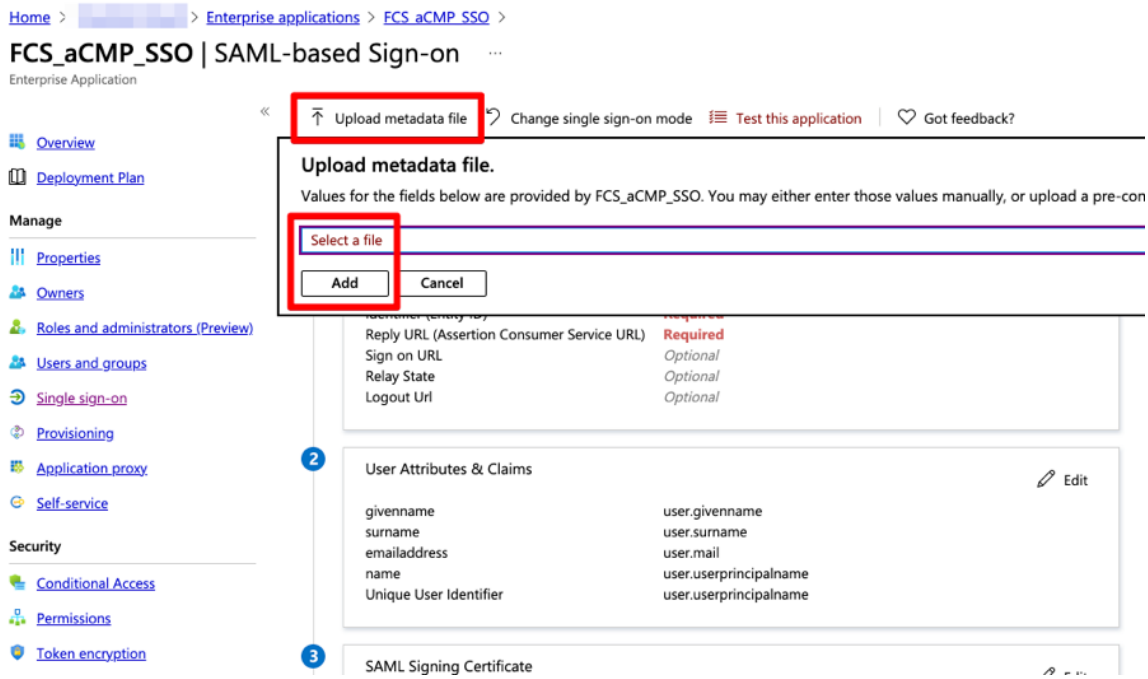
9. Fügen Sie die im ersten Schritt erstellte AD-Gruppe hinzu (On-Prem AD oder Azure AD).



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



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.

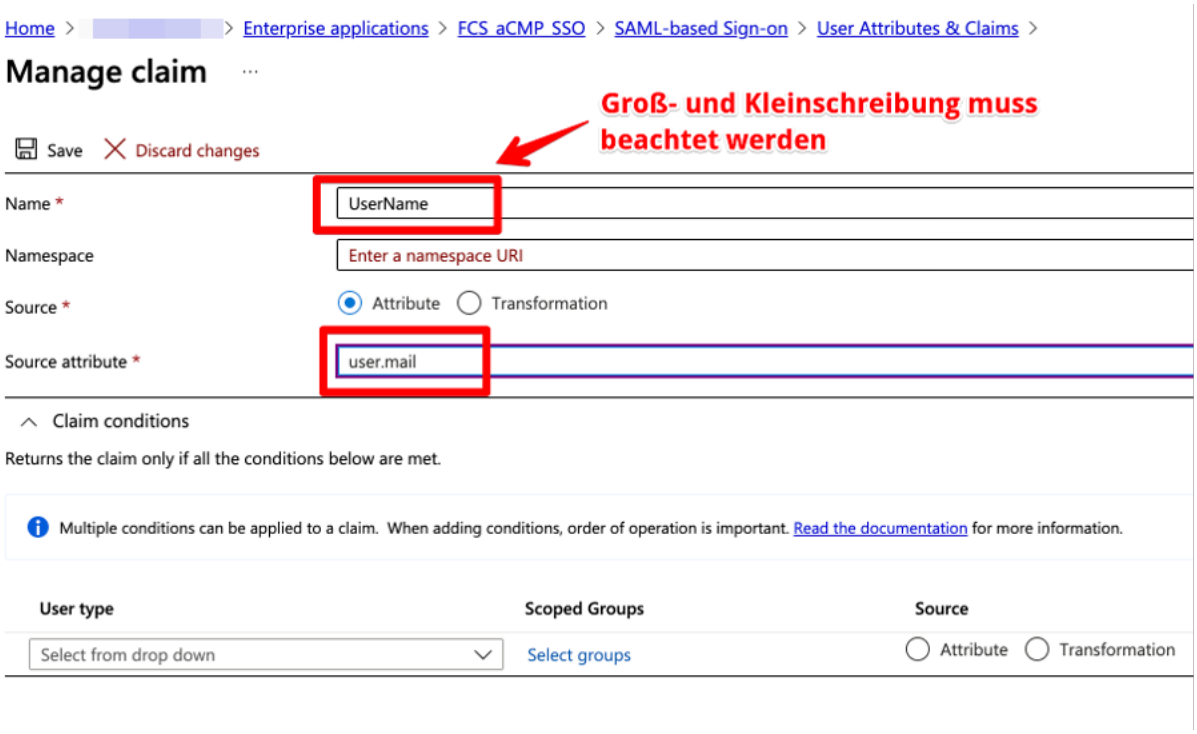


12. Unter «User Attributes & Claims» können Sie nun einen neuen Claim hinzufügen.

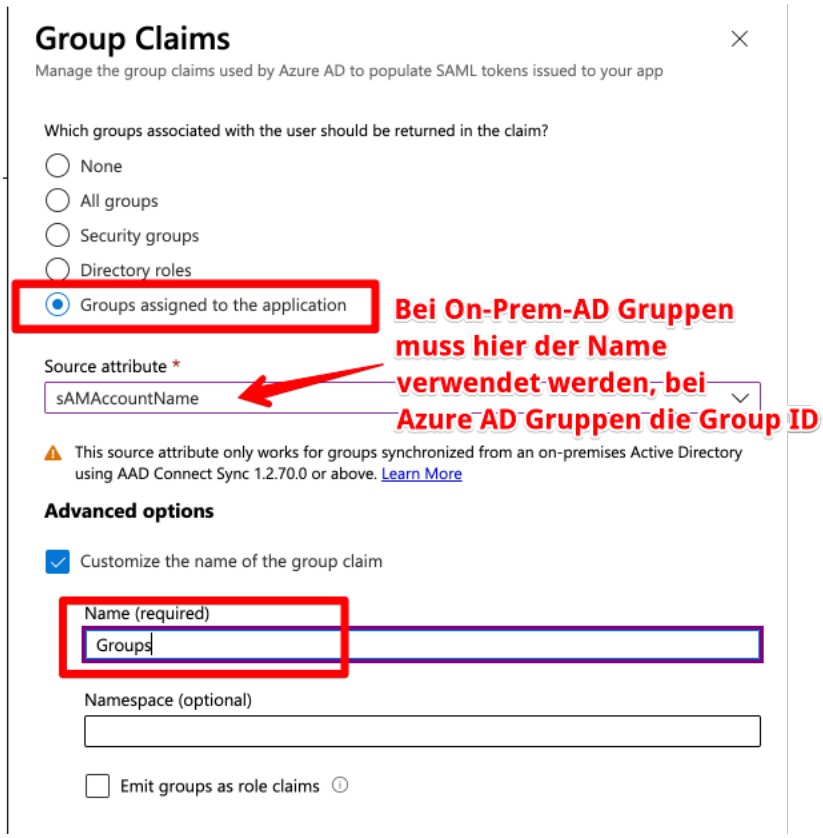
Fügen Sie die folgenden Claims hinzu:

- 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.



13. Fügen Sie nun einen Group Claim hinzu:



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

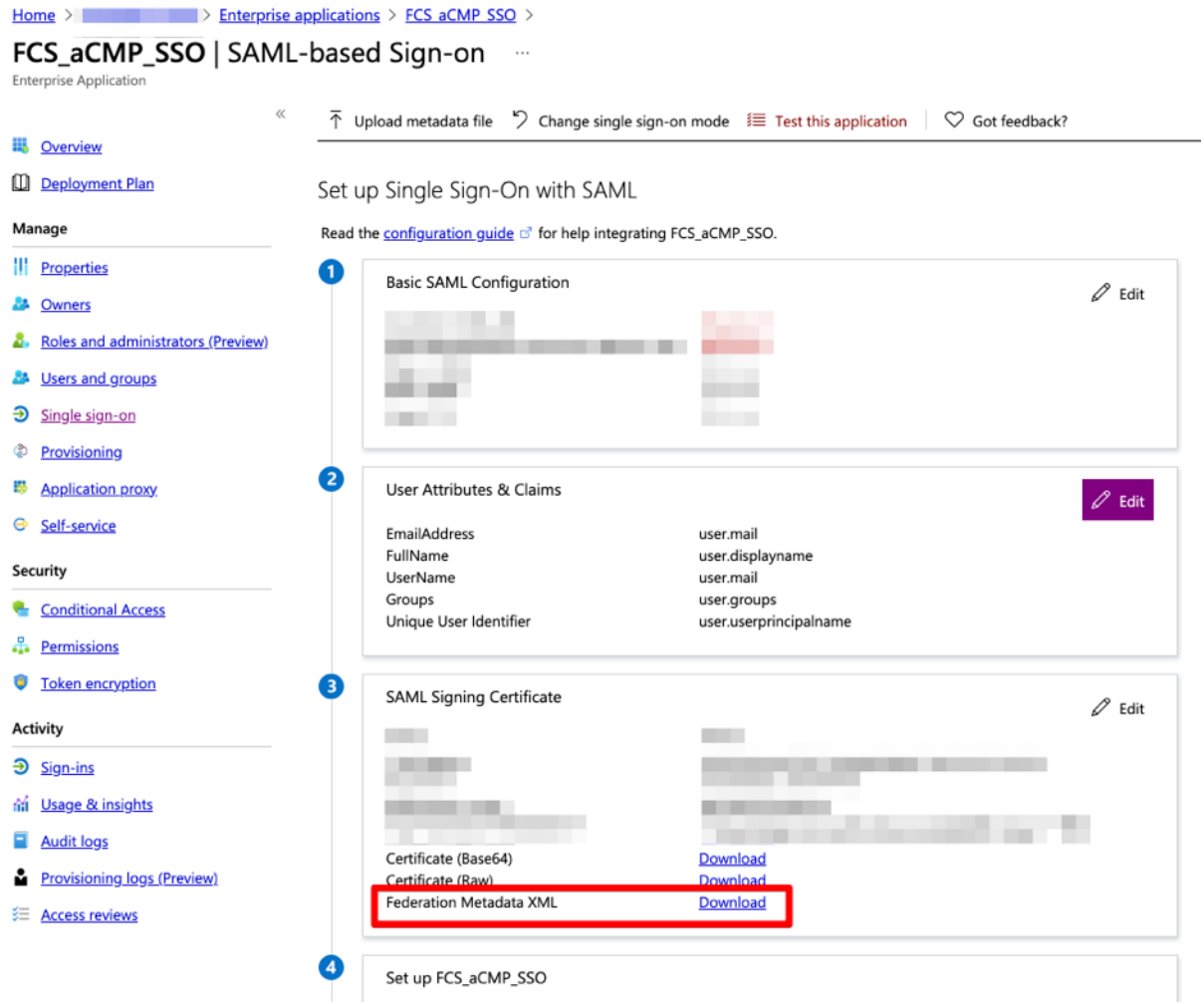
Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

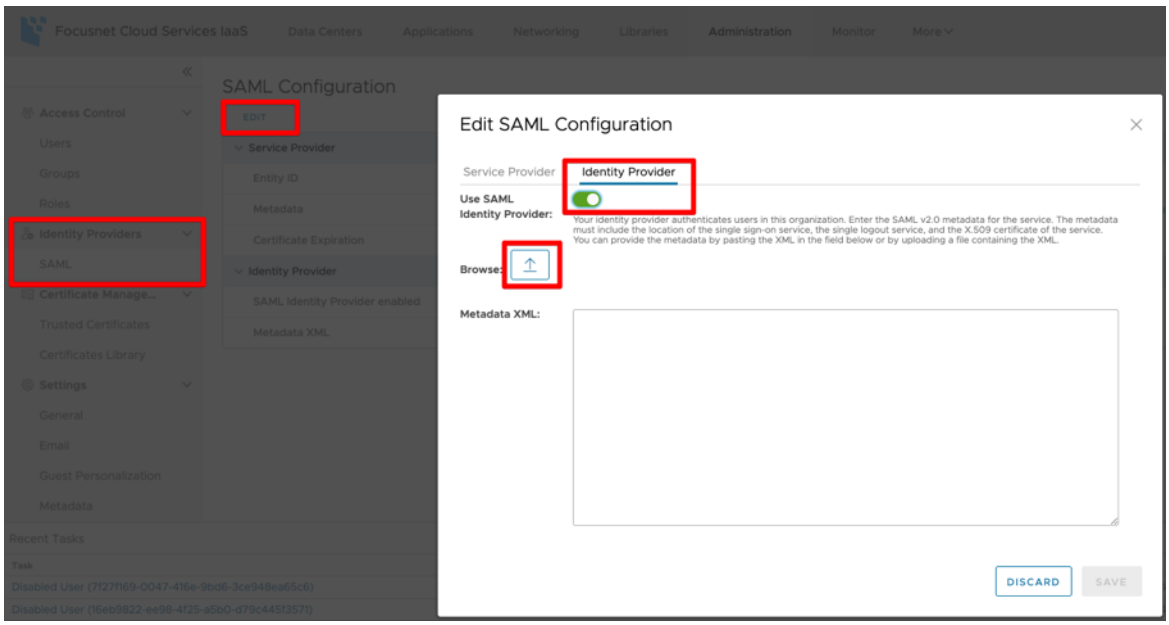
Additional claims

Claim name	Value
EmailAddress	user.mail
FullName	user.displayname
Groups	user.groups
UserName	user.mail

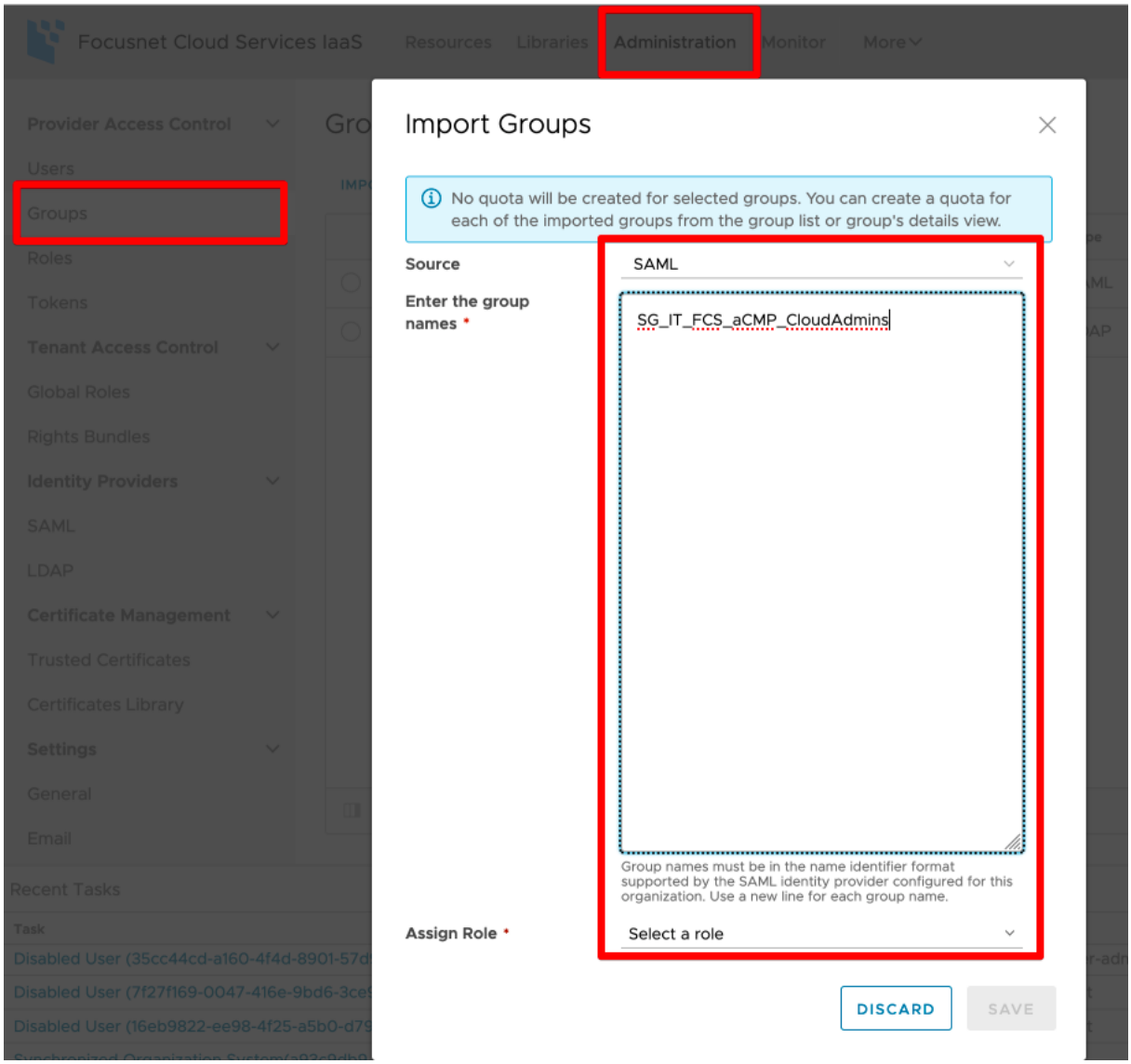
14. Nun können Sie die erzeugte FCS_aCMP_SSO XML-Datei herunterladen.



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



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:

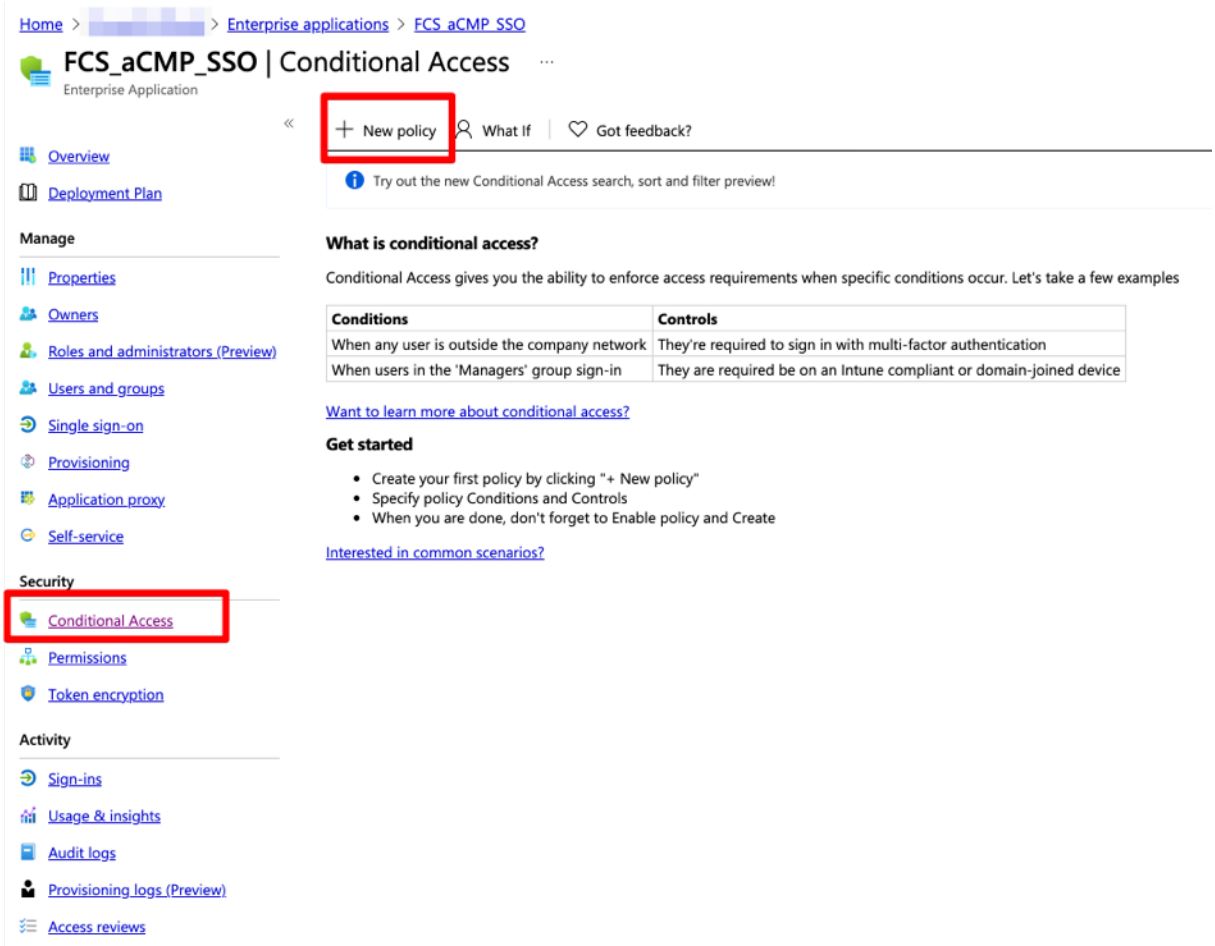


Hinweis: Wenn sie unterschiedliche Berechtigungsgruppen in Ihrem FCS IaaS Tenant nutzen, z.B. für den Zugriff auf unterschiedliche VDCs, müssen Sie diese Gruppen entsprechend im Azure-AD abbilden und die Berechtigungen an den VDCs anhand der Azure-AD-Gruppen setzen.

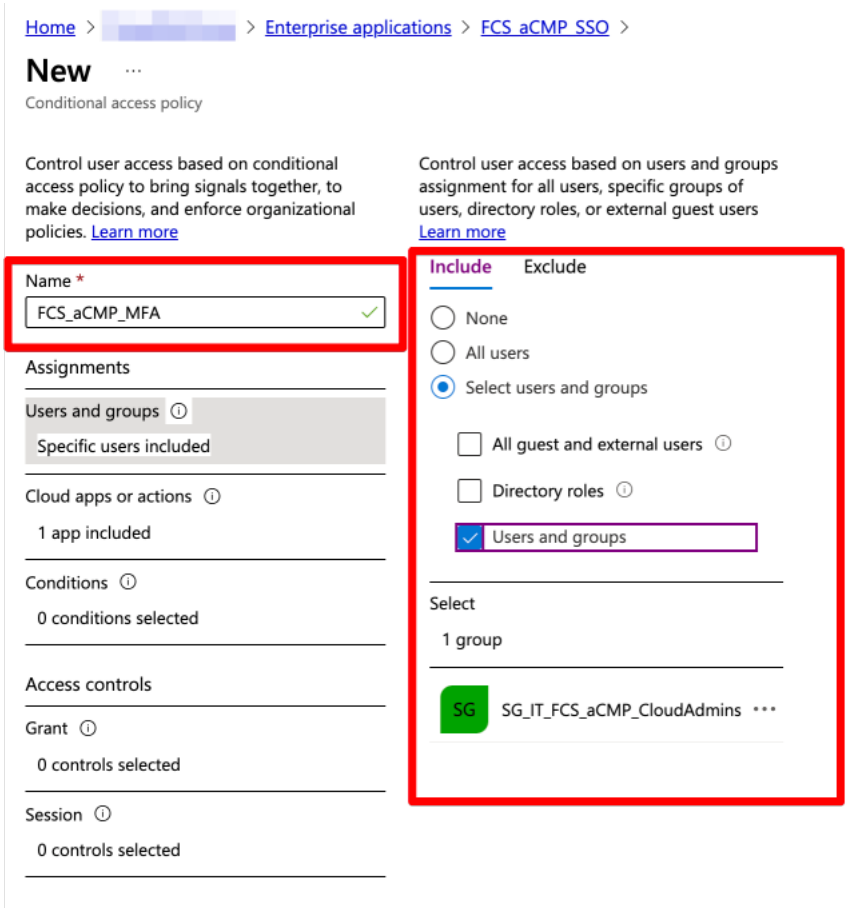
Optional: Multi-Faktor-Authentifizierung (MFA) aktivieren

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

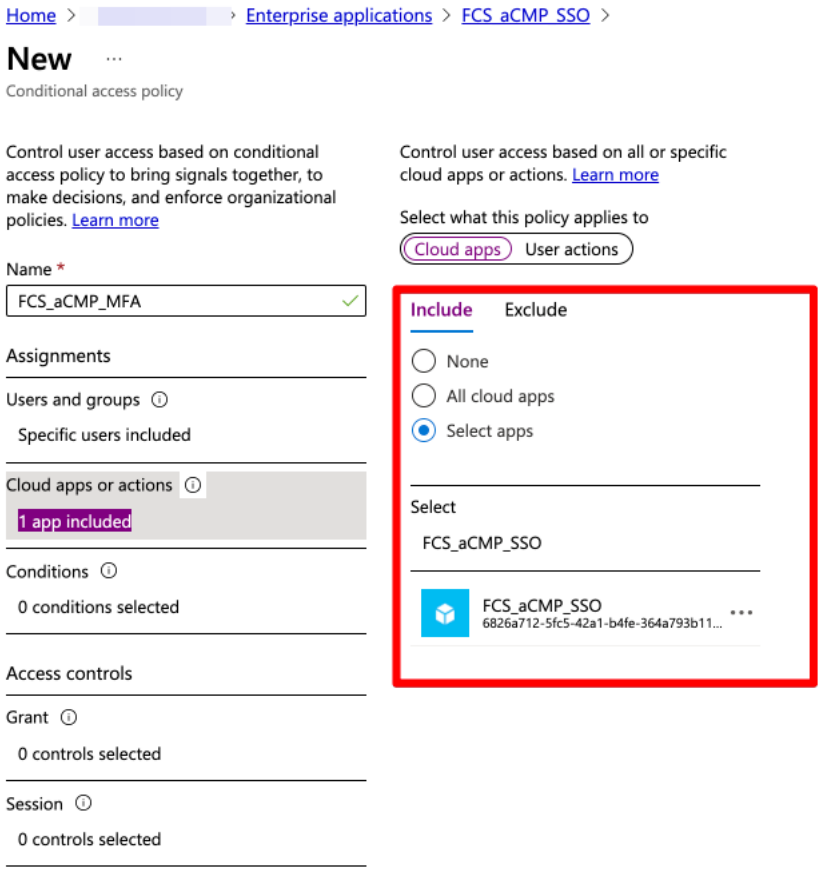
1. Klicken Sie im Azure Portal unter «Enterprise applications > FCS_aCMP_SSO > Conditional Access» auf «New policy».



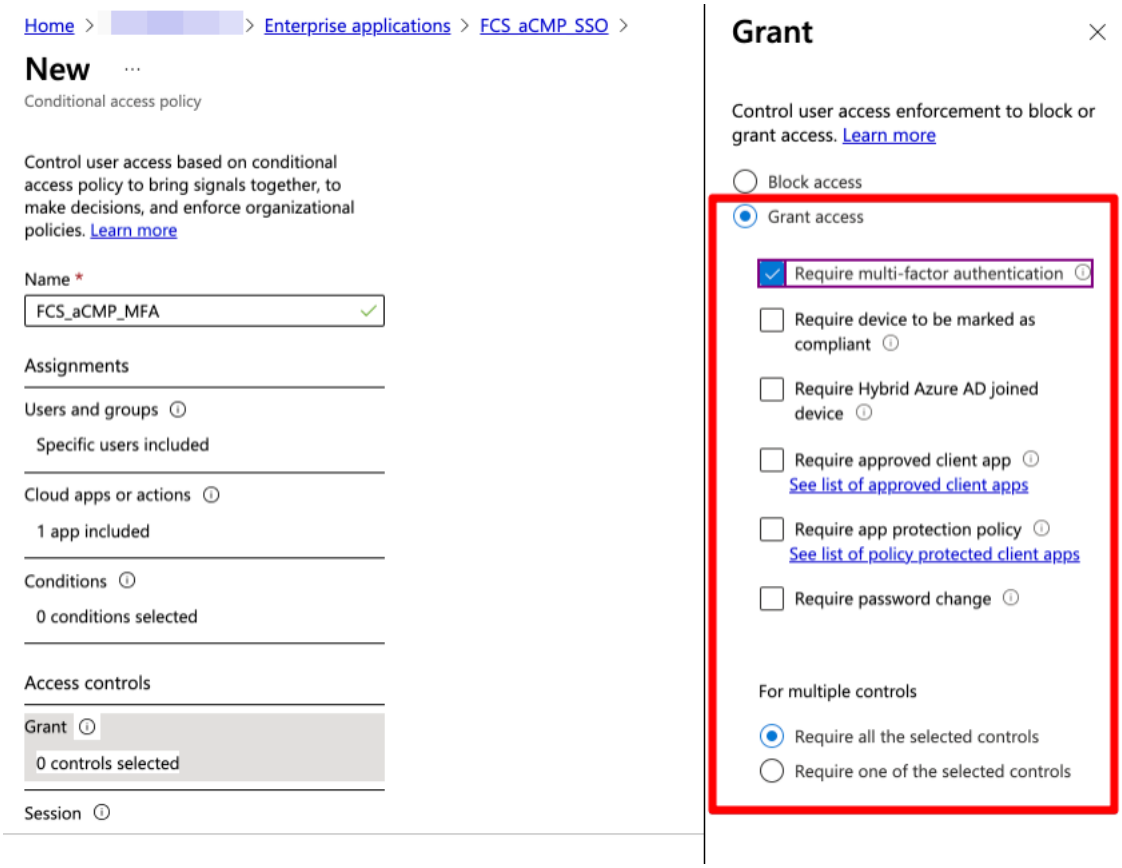
2. Benennen Sie die Policy und wählen Sie die User aus, die sich künftig mit MFA authentifizieren sollen.



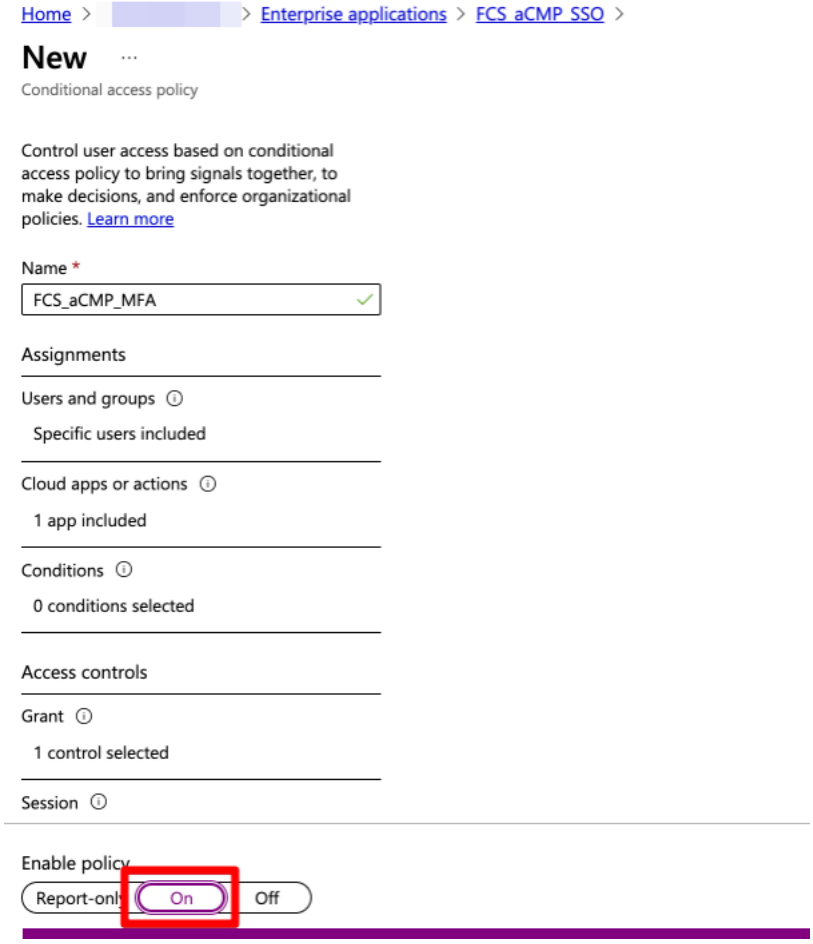
3. Wählen Sie im nächsten Schritt unter «Cloud apps» die «FCS_aCMP_SSO» Applikation.



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



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



„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