

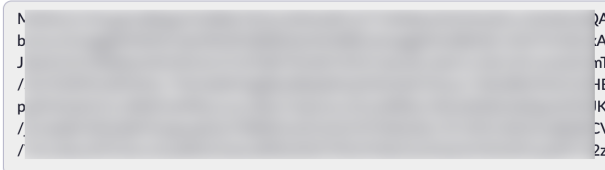
Exempel på SSO-mappning

Här följer ett exempel från Linnéuniversitetet på hur de satt upp Zoom och SAML/SSO

PERSONAL	
Profile	
Meetings	
Webinars	
Recordings	
Settings	

ADMIN	
Dashboard	
> User Management	
> Room Management	
> Account Management	
> Advanced	
App Marketplace	
H.323/SIP Room Connector	
Meeting Connector	
Skype for Business (Lync) Connector	
Branding	
Security	
Single Sign-On	
Integration	

Configure SSO Manually

Vanity URL	1	https://lnu-se.zoom.us (Approved)
Sign-in Page URL	2	https://idp.lnu.se/idp/profile/SAML2/POST/SSO
Sign-out Page URL		
Identity Provider Certificate	3	
Service Provider (SP) Entity ID	4	https://lnu-se.zoom.us
Service Provider (SP) Certificate	5	Zoom Certificate (Expires on 02/02/2022 UTC) View ✓ Automatically manage the certificate
Issuer (IDP Entity ID)	6	https://idp.lnu.se/idp/shibboleth
Binding		HTTP-POST
Signature Hash Algorithm		SHA-256
Security	7	✓ Sign SAML request ✗ Sign SAML Logout request ✓ Support encrypted assertions ✓ Enforce automatic logout after user has been logged in for 30 days ✓ Save SAML response logs on user sign-in
Provision User		At Sign-In (Default)

1. Vanity URL är adressen till er portal. Den måste vara godkänd av Zoom för att fungera (se följande artikel på wikin: [Konfigurera Zoom](#))
2. Kontakta IT-avdelningen och de som har hand om er SAML/SSO och få rätt på faktan som behövs. Inloggnings-URL för SSO
3. Certifikatet för er SAML/IDP
4. Samma adress som vanity URL för er SP
5. Det behövs också ett SP certifikat för Zoom som laddas upp här.
6. Adressen till er shibboleth
7. Säkerhetsinställningar. Vi har valt det här och det fungerar bra för oss. Provision User vid inloggning är en bra idé. "Save SAML response logs on user sign-in" är påslaget för att samla in loggar vid inloggning för felsökning. Inte nödvändigt i sig.

SAML Response Mapping

Gå till fliken SAML Response Mapping. Här mappar ni upp era användare så de hamnar i rätt grupp baserat på tillhörighet/typ av användare.

I exemplet här, baserat på vårt universitet, så har vi tre typer av användare som definieras via subdomäner i kontot. Personal, studenter och externa föreläsare/gästforskare.

Du behöver veta era urn:oid för de olika SAML attributen och ange dem tillsammans med det som ska mappas fram. Olika lärosäten har olika policies för vilken data som ska mappas.

SAML Basic Information Mapping

Default License Type	On-Prem	Edit
Email Address	<div>1</div> urn:oid:0.1.3	Edit Clear
First Name	urn:oid:2.2 ✓ Update at each SSO login	Edit Clear
Last Name	<div>2</div> urn:oid:2.4 ✓ Update at each SSO login	Edit Clear
Display Name	Map to SAML Attribute	
Phone Number (Separate multiple numbers with commas)	Map to SAML Attribute	
Employee Unique ID ?	<div>3</div> urn:oid:1.3.6	Edit Clear

1. E-postadressens, för- och efternamnets urn:oid fylls i vid respektive attribut.
2. OBS att det är en bra idé att bocka i att de ska uppdateras vid varje inloggning. Namnbyten, nya e-postadresser m.m.
3. Fortsätt fylla i de olika attribut som ni vill få in i Zooms databas. Längst ner finns Employee Unique ID. Missa inte den.

Scrolla ner till SAML Advanced Information Mapping:

SAML Advanced Information Mapping			
	SAML Attribute	SAML Value	Resulting Value
<div>License Type</div> <div>1</div>	urn:oid:1.3.1.9	employee@lnu.se	On-Prem Edit
	urn:oid:1.3.1.9	student@lnu.se	On-Prem
	urn:oid:1.3.1.9	affiliate@lnu.se	On-Prem
You can exclude users and groups to not follow the above mapping rules.			
Not set Edit			
Add-on Plan	Add		
User Role	Add		
<div>User Group</div> <div>2</div>	urn:oid:1.3.1.9	employee@lnu.se	Employee Edit
	urn:oid:1.3.1.9	student@lnu.se	Student
	urn:oid:1.3.1.9	affiliate@lnu.se	Employee
You can exclude users and groups to not follow the above mapping rules.			
<div>3</div> 1 group(s) of users are excluded. Edit			
User Group Admin	Add		
Channel	<div>?</div> <div>In order to show accurate system messages on the client, make sure users in your account update their clients to the latest version. Go to Account Settings > Meeting > Admin Options and enable Require users to update the client. Learn More.</div>		

1. License Type. Det är här ni väljer hur de olika användargrupperna ska kopplas till licensen. onPrem är det vi ska använda i dagsläget (NORDU. nets servrar). Använd urn:oid och SAML-värdet för de användargrupperna.
2. User Group är ett sätt att ge olika användare olika rättigheter i systemet. Dela upp användarna i grupper som ni önskar baserat på er SAML. Oavsett om ni tänkt låta alla användare ha samma rättigheter eller inte så är det en god idé att dela upp dem i grupper baserat på roller de har hos er för framtida bruk.
3. Man kan också skapa mindre grupper i systemet som har helt egna rättigheter utanför den större gruppen. Då måste de grupperna undantas från grundmappningen för att inte "ramla ur" den lilla extragruppen.

Ett typexempel är om du vill ge vissa anställda rättighet att använda en specifik, ny funktion för testning. Då kan du skapa en ny grupp (under Users /Groups) och ge den gruppen rättigheter samt göra gruppen till primär för användarna. Den gruppen blir då huvudgrupp vilket gör att trots att de även tillhör gruppen "personal" så har de utökade befogenheter. Den nya gruppen måste undantas mappningen, annars går användarna tillbaka till sin SAML-mappade grupp vid inloggning.

IM Groups

Slutligen finns det IM (Instant Messenger) grupper på sidan:

Zoom Rooms Admin		Add			
IM Group	urn:oid:1.3.6.1.4.1.25674.1.2.1	1.9	employee@lnu.se	Employee	Edit
	urn:oid:1.3.6.1.4.1.25674.1.2.2	1.9	student@lnu.se	Student	
	urn:oid:1.3.6.1.4.1.25674.1.2.3	1.9	affiliate@lnu.se	Employee	
You can exclude users and groups to not follow the above mapping rules.					
Not set Edit					

Det handlar om chattfunktionen och användarkataloger som kan delas upp i olika grupper. Till exempel skiljer vi på studenter och personal så studenterna inte kan leta upp sina lärare i katalogen och inte kontakta dem. Däremot kan lärare göra tvärtom. Detta är alltså om ni vill kunna skilja grupperna åt i Zoom, låta studenter skapa kanaler, chattar, videomöten med varandra, men låta personalgruppen kunna jobba ostört i egna kanaler.