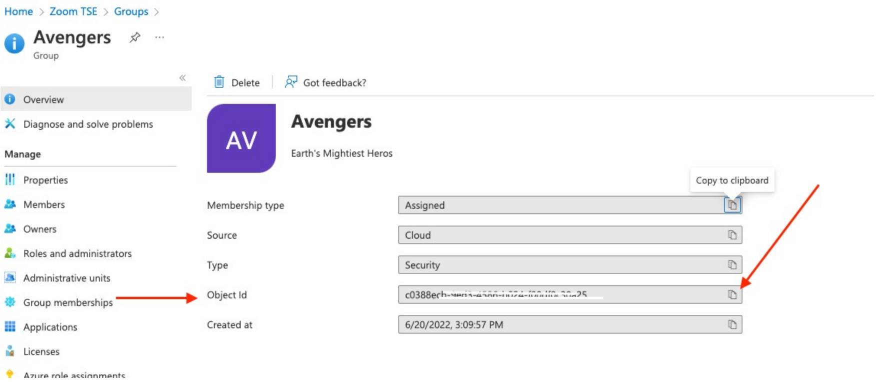
1. Create or identify an AD Group whose members are intended for a specific Zoom IM Channel. Once this group is identified or created, make note or copy the AD group’s “object ID”.

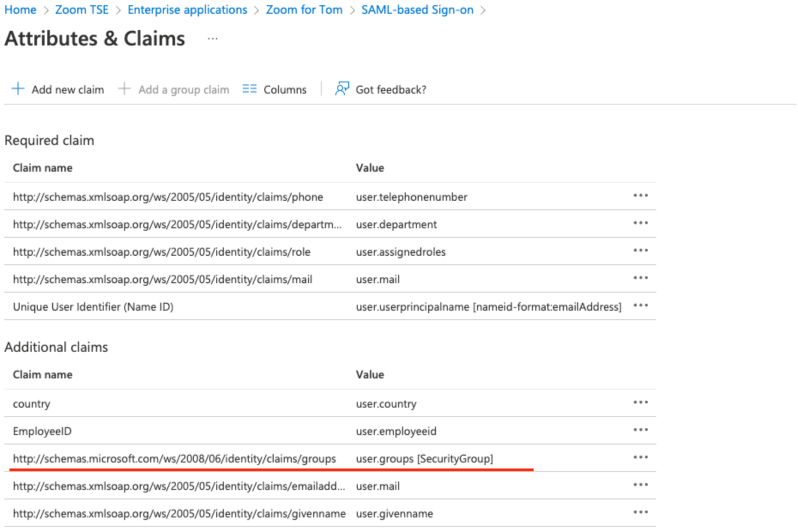


Avengers

Earth's Mightiest Heros

Membership type	Assigned
Source	Cloud
Type	Security
Object Id	c0388ech[redacted]
Created at	6/20/2022, 3:09:57 PM

2. Confirm that the Zoom SSO object in AAD is passing “group” claims:


Home > Zoom TSE > Enterprise applications > Zoom for Tom > SAML-based Sign-on >
Add new claim
Add a group claim
Columns
Got feedback?

Attributes & Claims

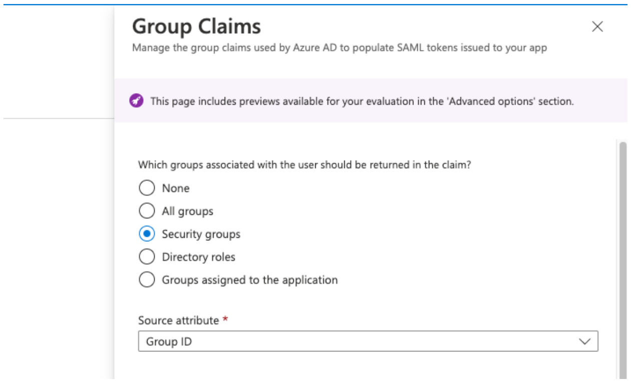
Required claim

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/phone	user.telephonenumber
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/departm...	user.department
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/role	user.assignedroles
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mail	user.mail
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress]

Additional claims

Claim name	Value
country	user.country
EmployeeID	user.employeeid
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups [SecurityGroup]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname

If “group” claim is not passed, select “Add a group claim” > select “Security Groups” > set “source attribute” to “Group ID”



Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

This page includes previews available for your evaluation in the 'Advanced options' section.

Which groups associated with the user should be returned in the claim?

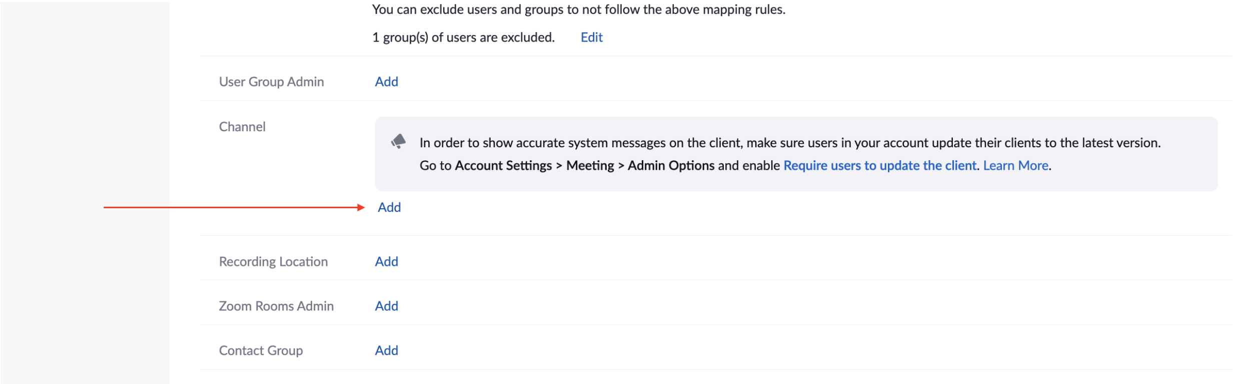
○ None
○ All groups
● Security groups
○ Directory roles
○ Groups assigned to the application

Source attribute *

Group ID

3. In the Zoom web portal, select Advanced > Single Sign-On > SAML Response Mapping > scroll down and locate “Channel” > select “Add”

NOTE: If you do not see the “advanced” tab or Single Sign-On tab, your Zoom role may not have permissions to modify.



You can exclude users and groups to not follow the above mapping rules.

1 group(s) of users are excluded. Edit

User Group Admin Add

Channel

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.

Add

Recording Location Add

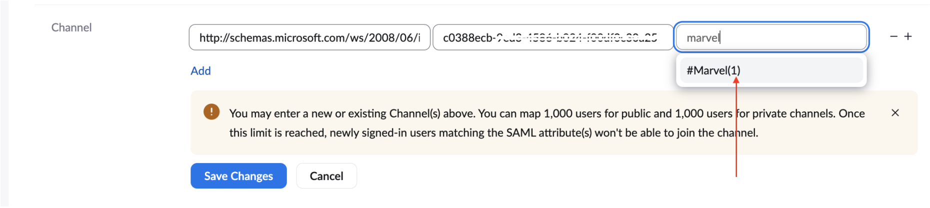
Zoom Rooms Admin Add

Contact Group Add

4. Set the following:

Attribute name: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
NOTE: this is the default claim from Azure AD. This claim could be modified in Azure AD.
Value contained: Object ID gathered from Step One
Resulting Value: Search and select your respective IM Chat Channel

NOTE: The number you see in the parenthesis is number of users in this chat channel. In my example, there is one member in the “Marvel” channel.



Channel http://schemas.microsoft.com/ws/2008/06/i c0388ecb-[redacted] marvel − +

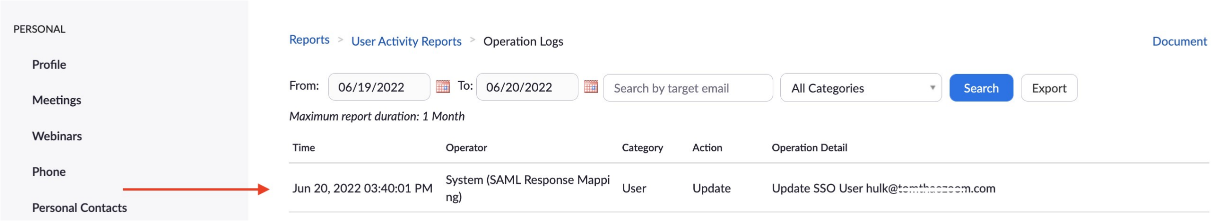
#Marvel(1)

Add

You may enter a new or existing Channel(s) above. You can map 1,000 users for public and 1,000 users for private channels. Once this limit is reached, newly signed-in users matching the SAML attribute(s) won't be able to join the channel. ×

Save Changes Cancel

5. Have your respective user log into Zoom via SSO. Upon them logging into Zoom via SSO, they will be assigned to their respective Zoom chat channel. You can confirm successful assignment by reviewing your Zoom Operation logs.



Reports > User Activity Reports > Operation Logs Document

From: 06/19/2022 To: 06/20/2022 Search by target email All Categories Search Export

Maximum report duration: 1 Month

Time	Operator	Category	Action	Operation Detail
Jun 20, 2022 03:40:01 PM	System (SAML Response Mapping)	User	Update	Update SSO User hulk@[redacted]m.com

Limitations:

Users MUST sign into Zoom via SSO for assignment to occur.

By passing security groups, the user’s SAML token to Zoom will contain the object ID of ALL AD groups they are assigned to. If your user is assigned to more than 100 AD groups, the SAML token will contain the GRAPH API endpoint of your Azure tenant. Zoom will NOT be able to read this assertion.