

Grandstream Networks, Inc.

UCM63xx SAML SSO Configuration Guide



UCM63xx SAML SSO Configuration Guide

OVERVIEW

SAML (Security Assertion Markup Language) is a standard protocol that enables applications to use an external **Identity Provider (IdP)** for user authentication and Single Sign-On (SSO). With SAML SSO, users can authenticate using their existing enterprise identity provider instead of maintaining a separate username and password on the UCM.

The UCM6300 Series supports SAML SSO by acting as the **Service Provider (SP)**. During the authentication process, the UCM redirects the user to the configured third-party IdP. After successful authentication, the IdP returns a signed SAML response containing the user's identity information. The UCM validates the response and uses the configured user-mapping information to associate the authenticated IdP user with the corresponding UCM user.

SAML SSO can be integrated with enterprise identity providers such as **Microsoft Entra ID (Azure AD), AD FS, Okta, OneLogin, and Google Workspace**. The identity provider is responsible for authenticating users, while the UCM relies on the SAML assertion provided by the IdP to complete the login process.

SAML COMPONENTS

When using SAML, there are two key elements:

- **Identity Provider (IdP):** The authority for the user's identity. It validates user credentials and provides identity attributes by knowing the user's username, password, and any groups/attributes (Example: Microsoft Entra ID, AD FS, Duo).
- **Service Provider (SP):** The application that the user wishes to use. In this case, the UCM63xx.

SAML SSO CONFIGURATION IN UCM63XX

SAML Single Sign-On (SSO) allows users to authenticate to the UCM through an external **Identity Provider (IdP)** instead of using a separate UCM username and password.

In this configuration:

- **UCM** acts as the **Service Provider (SP)**.
- The external **IdP** performs user authentication; in our example, **Microsoft Entra ID**
- The UCM uses the SAML response from the IdP to identify and authorize the corresponding UCM user.

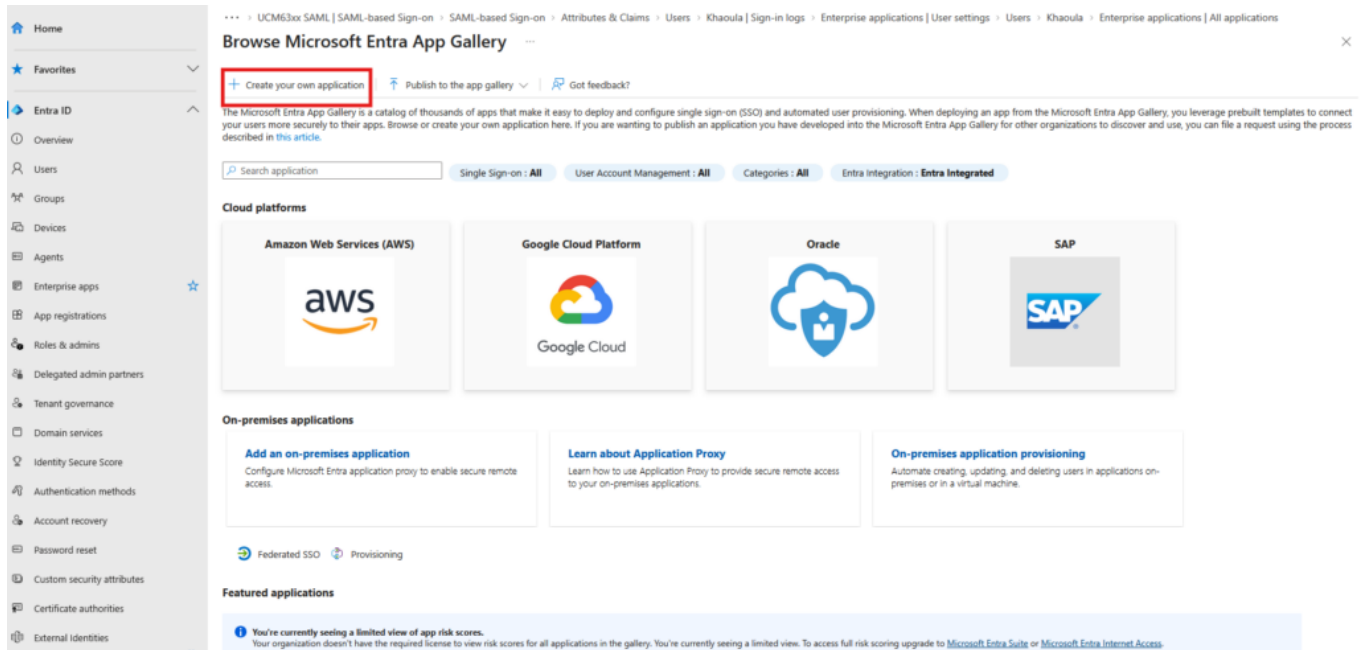
Firstly, users need to sign up for an Azure account by visiting this web page:

<https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-permissions-management>

This section mainly introduces how to configure Microsoft Entra ID (formerly known as Azure AD) as the identity provider (IdP) for UCM63xx.

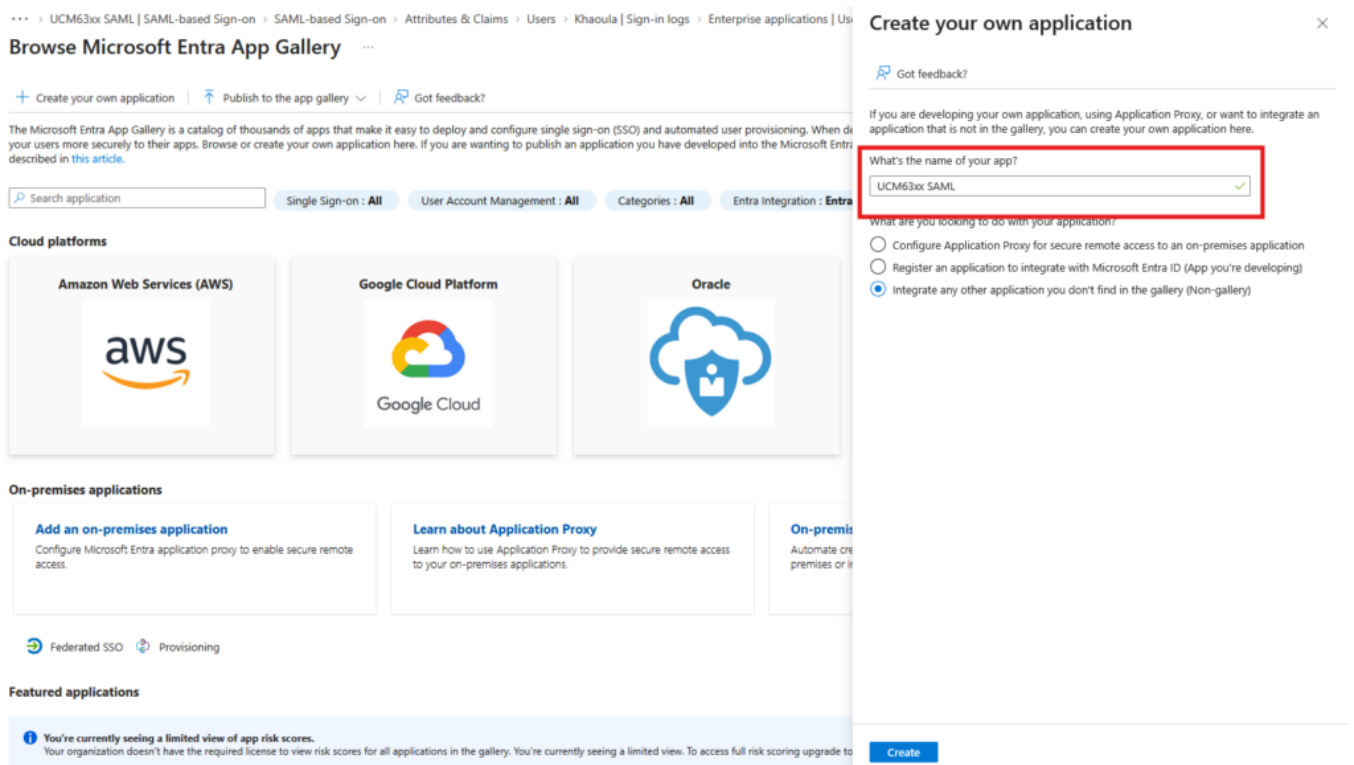
Step 1: Add a new application in Azure

1. Sign in to the Microsoft Entra admin center as a Cloud Application Administrator or higher.
2. Go to **Entra ID -> Enterprise apps -> New application**.
3. In the **Browse Microsoft Entra Gallery** section, click **Create your own application**.



Add a new application in Azure

4. Enter your application name, such as "UCM63xx SAML", and select **"Integrate any other application you don't find in the gallery (Non-gallery)"**.



5. Click **Create** to successfully create the application. You can view the application in the list.

*** > Users > Khaoula | Sign-in logs > Enterprise applications | User settings > Users > Khaoula > Enterprise applications | All applications > Browse Microsoft Entra App Gallery > UCM63xx SAML | Overview > Enterprise applications

Enterprise applications | All applications

Overview

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

4 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Activation status	Certificate Expir...	Active Certificat...	Identifier URI (E...
US UCM63xx SAML	02db60ac-c480-4e25...	2cf8...	https://account.activ...	9/11/2026	Activated	Current	9/11/2029	streamucm...
US UCM63xx SA...	bf26d338-a97f-45af...	8d09ecb1-4ffd-44dc...	https://account.activ...	9/11/2026	Activated	-	-	8d09ecb1-4ffd-44dc...
GU Grandstream ...	ddd45522-1679-42e...	d78f52ff-5977-4ae4...		1/7/2026	Activated	-	-	d78f52ff-5977-4ae4...
GU GS UCM	fec1221c-1d63-4daa...	8ed6d127-dca1-459a...		2/2/2026	Activated	-	-	8ed6d127-dca1-459a...

Step 2: Create an application role in Azure

1. Sign in to the Microsoft Entra admin center, go to Entra ID-> Applications -> APP registrations, and click on the app you have created.

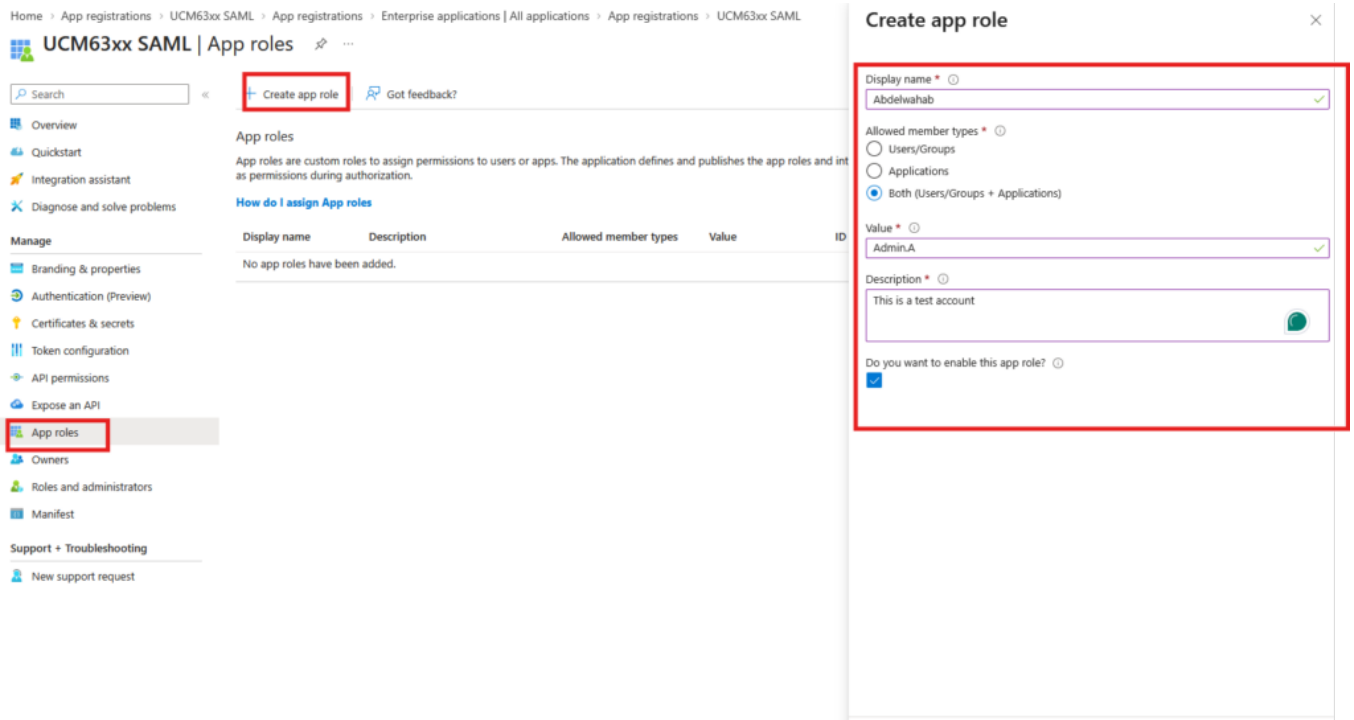
*** > SAML-based Sign-on > Enterprise applications | All applications > UCM63xx SAML | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims > Manage claim > EMEA-Lab > Users > Khaoula

App registrations

1 application found

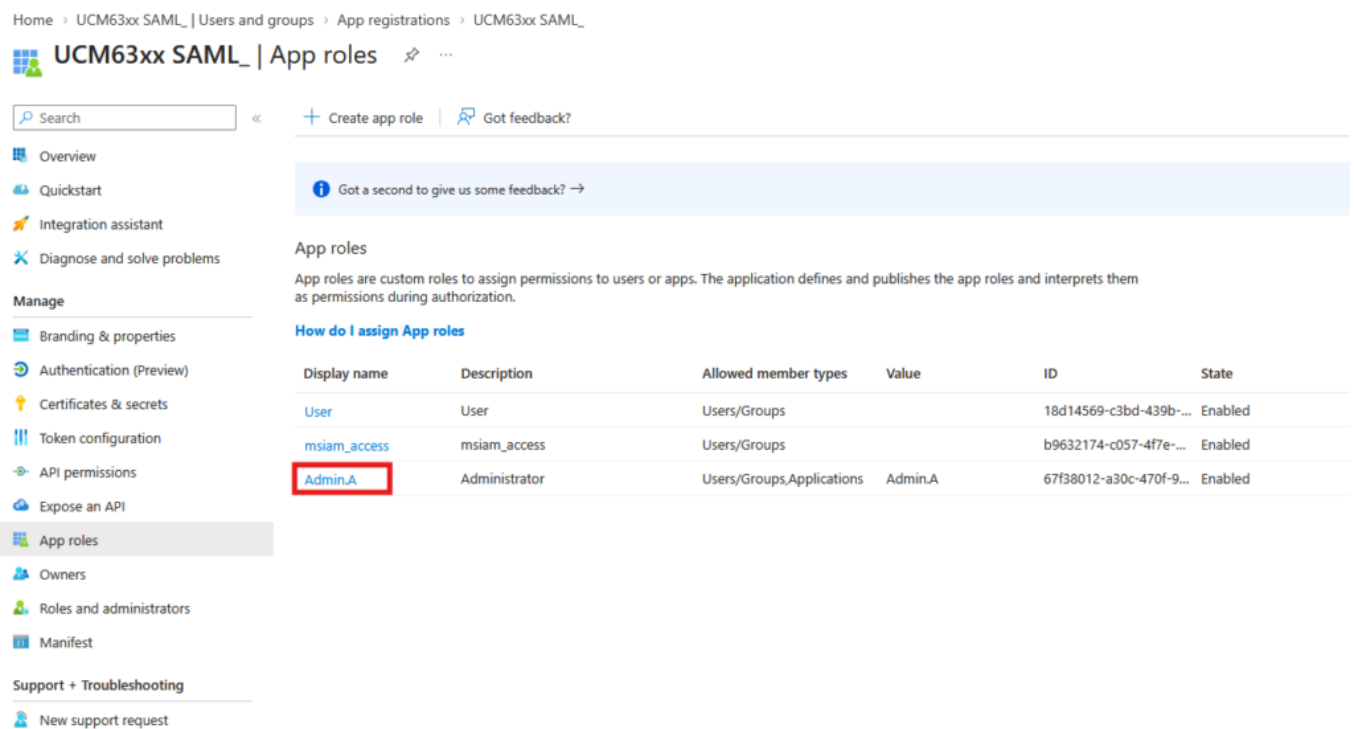
Display name	Application (client) ID	Created on	Certificates & secrets
US UCM63xx SAML	8d09ecb1-4ffd-44dc...e51455810	9/11/2026	-

2. Click **APP roles** on the left, and then click **Create app role**. Then fill in the display name, select **"Both"** for type, and the Value must be consistent with the SAML role value expected by the Service Provider, such as **"Admin.A"**.



Create an App Role

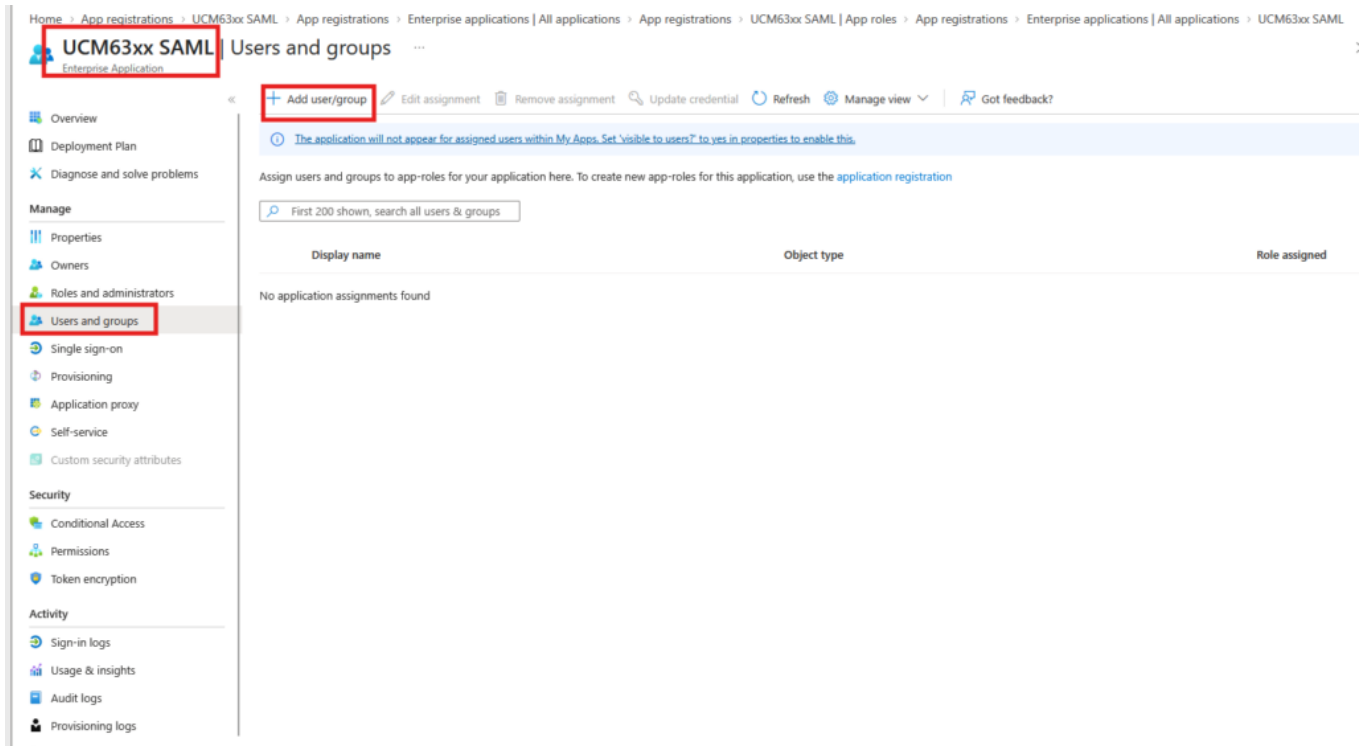
3. After successful creation, you can see this role in the list.



List of App Roles

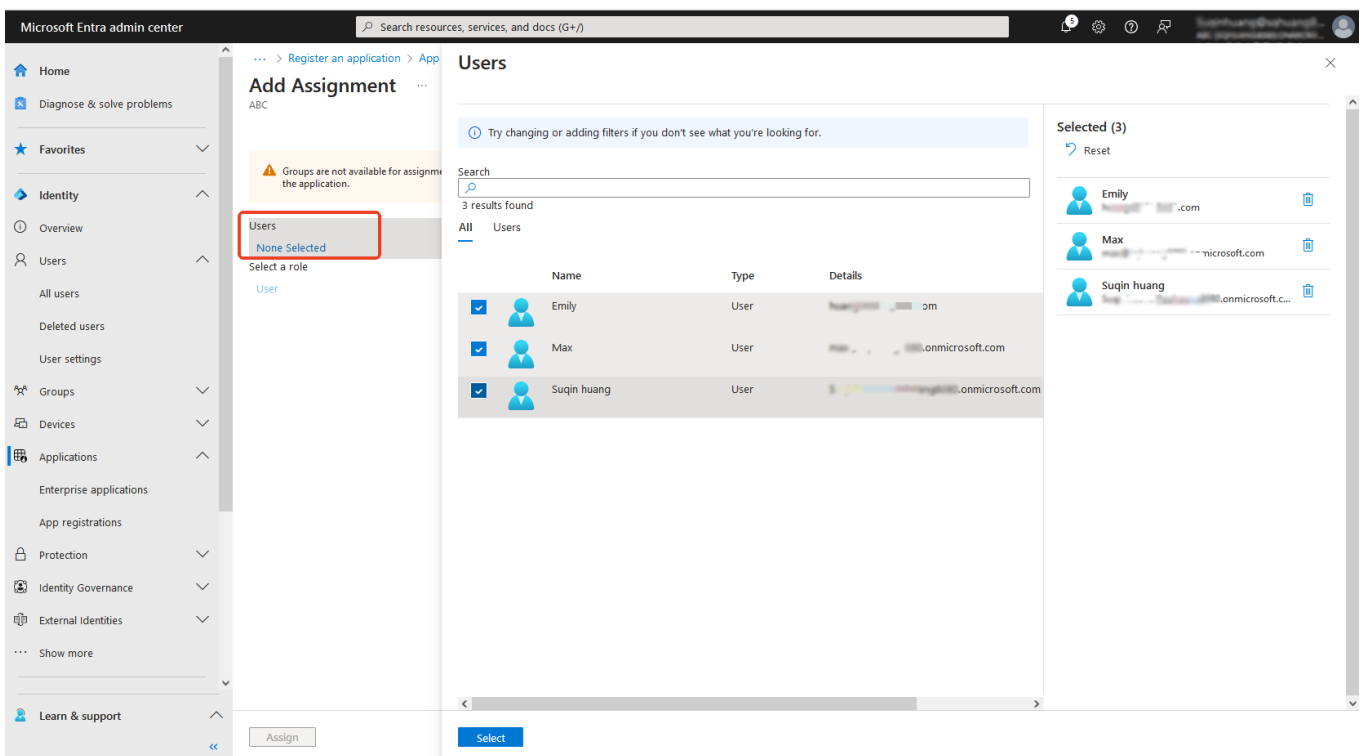
Step 3: Add users to the application in Azure

1. Sign in to the Microsoft Entra admin center, go to **Identity -> Applications -> Enterprise applications**, find and select the app you created in the application list.
2. Then, click **Users and groups** on the left bar and select **Add user/group**.



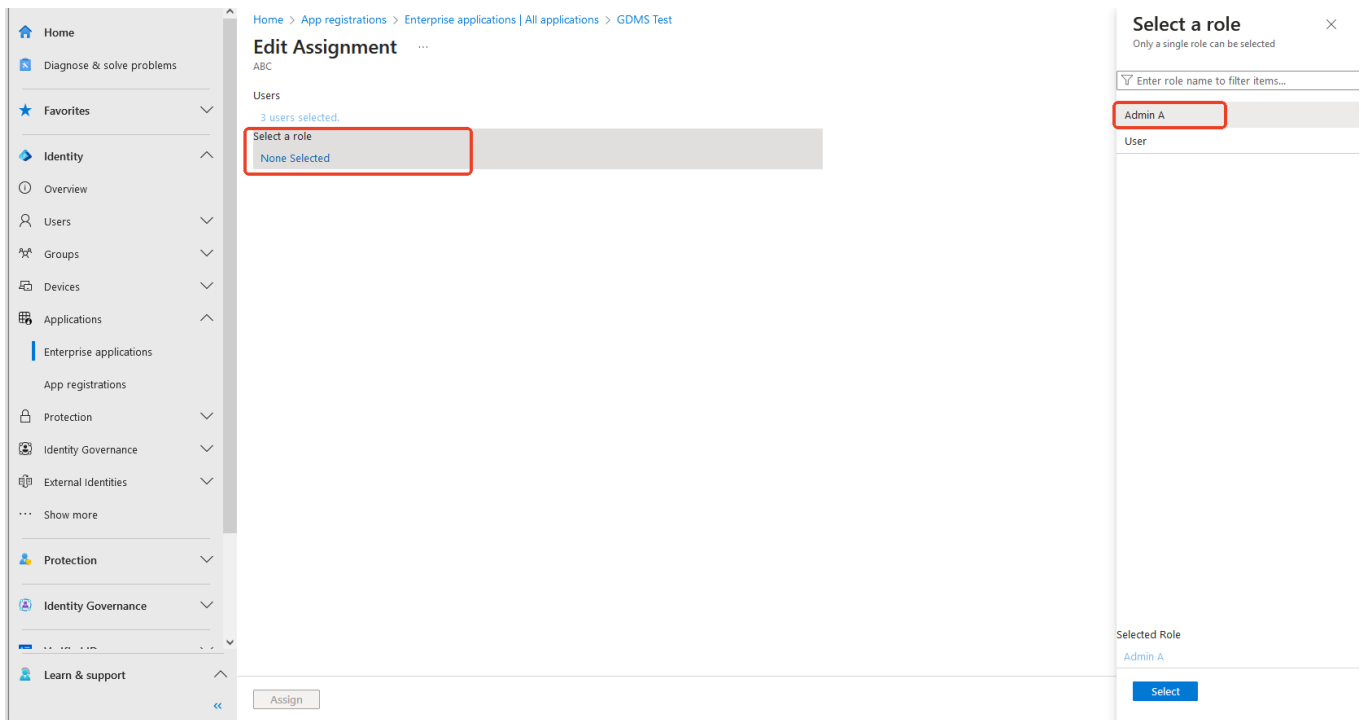
Add UserGroup to an App

3. Select the users you want to assign to use this app.



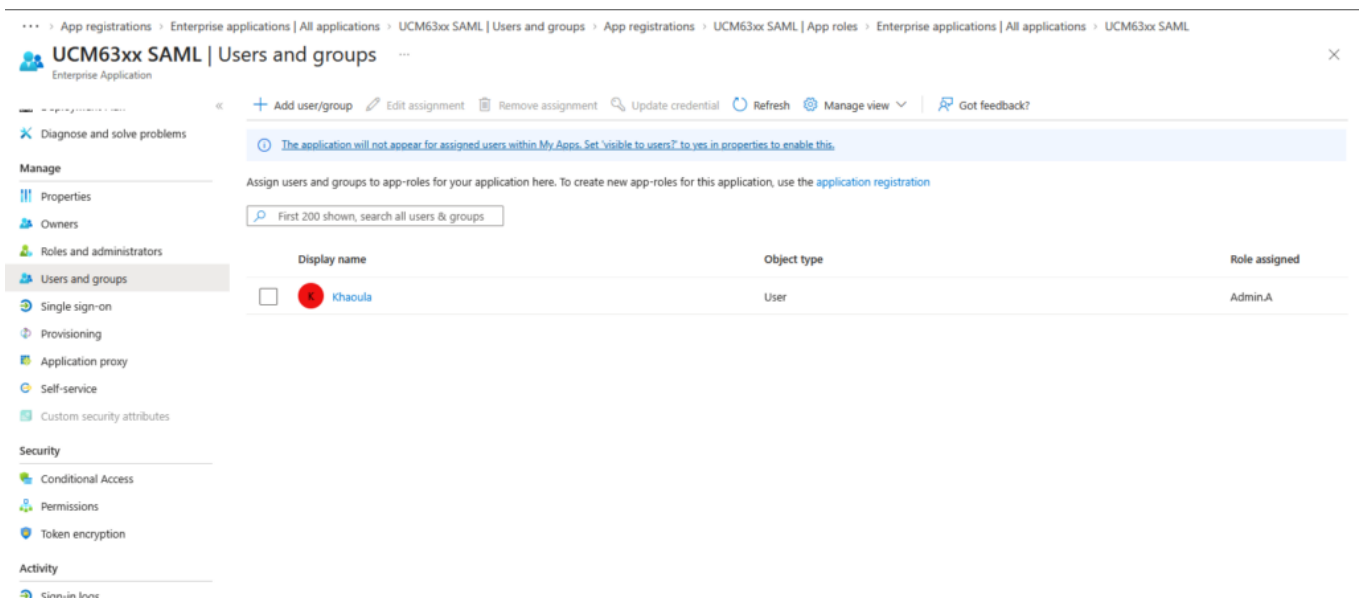
App User Selection

4. Select Assigned Roles and choose from the application roles you just created.



Assigning Roles to App Users

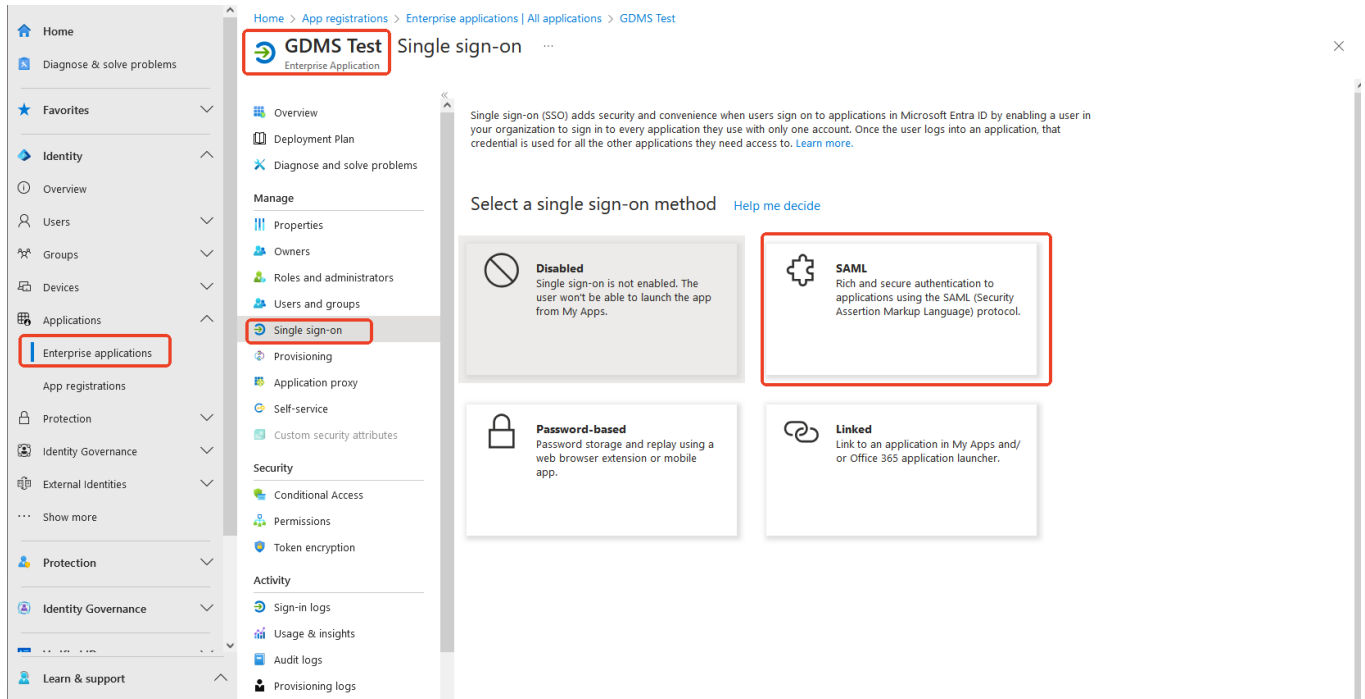
- Then click **Assign**. After the assignment is successful, you can see the selected users and the assigned roles in the list. (These users can then log in to UCM63xx with a single sign-on)



List of App Assigned Users

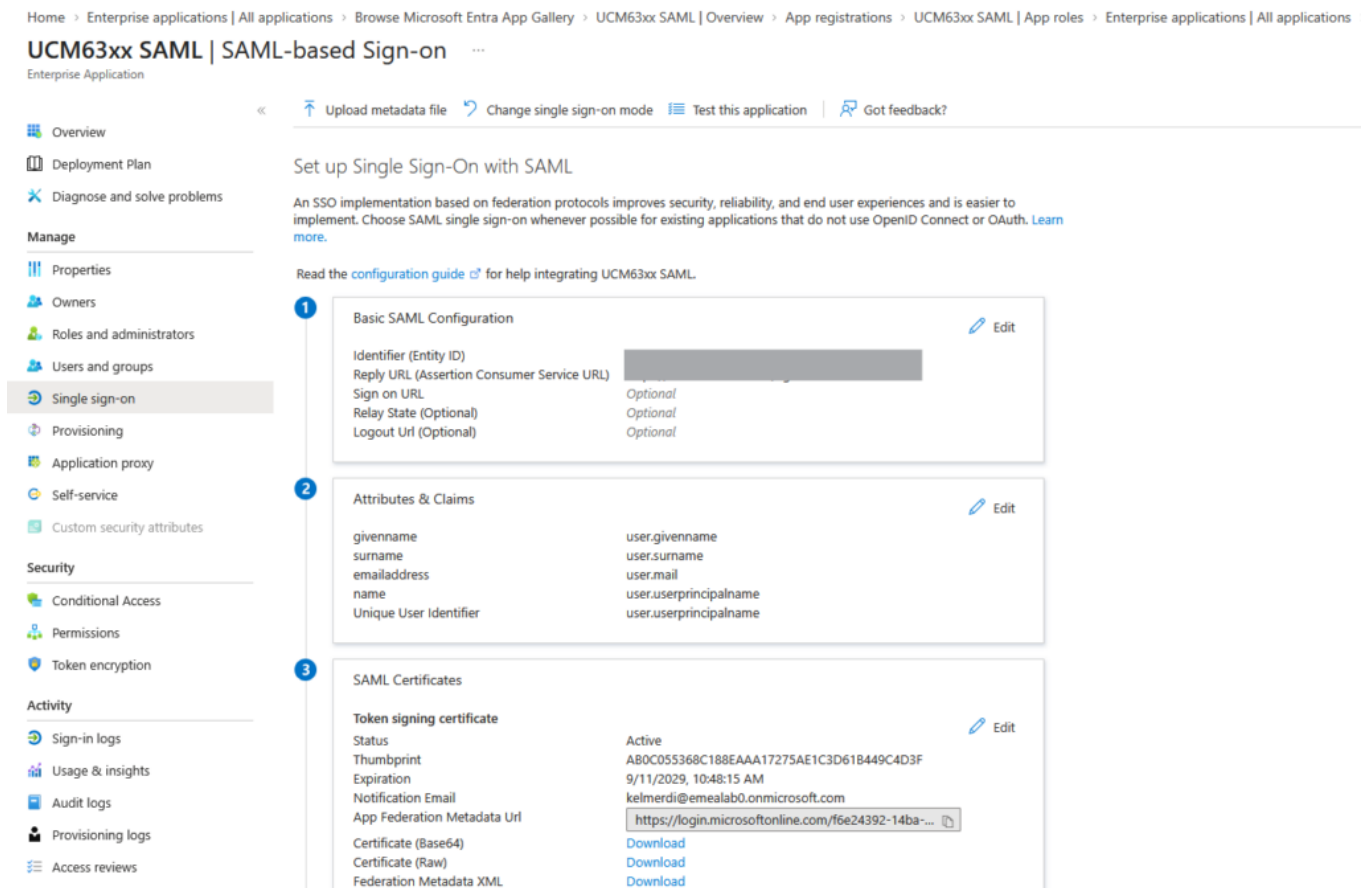
Step 4: Set up SSO in Azure

- Sign in to the Microsoft Entra admin center, go to **Identity -> Applications -> Enterprise applications**, find and click the app you have previously created.
- Click **Single Sign-on** on the left and click **SAML** on the page.



App SAML SSO Page

3. First, within the **Basic SAML Configuration** section, click **Edit**.



App Basic SAML Configuration

4. Copy the information from the UCM63xx platform and fill in the following information:

Identifier (Entity ID)	Fill in the Entity ID displayed on the SAML SSO page in Users (as shown in the picture, click one-click copy)
Reply URL	Fill in the ACS URL displayed on the SAML SSO page in Users (as shown in the figure, click one-click copy)

Relay State

Specify the Service Provider URL that users should be redirected to after successful authentication. Note: Although this field appears optional, it is required for this integration. You must configure it to prevent user errors.

Basic SAML Configuration



Save



Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
urn:grandstream: [redacted] Add identifier	✓ ⓘ [trash]

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://192.168.6 [redacted] /cgi?action=checkSAML Add reply URL		✓ ⓘ [trash]

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL ✓

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Copying the Entity ID and ACS URL to Entra ID

- Then, within the **Attributes & Claims** section, click **Edit**.

2

Attributes & Claims		Edit
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	

SAML Attributes Claims Section

- Click **Add new Claim**.

Home

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Enterprise applications

App registrations

Protection

Identity Governance

External Identities

Show more

Protection

Identity Governance

Learn & support

Home > App registrations > Enterprise applications | All applications > GDMS Test | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

+ Add new claim

+ Add a group claim

Columns

Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname [...]

Advanced settings

Add a New Claim

- Add the following SAML claims in Microsoft Entra ID. The claim names (URIs) must match the requirements of the target platform.

	Claim	Name	Source attribute
UCM63xx	Claim 1 (Role)	https://<UCM IP>[:port]/user/saml/attribute/role Example: https://192.168.6.71:8089/saml/attribute/role	user.assignedroles
	Claim 2 (Email)	https://<UCM IP>[:port]/user/saml/attribute/emailaddress Example: https://192.168.6.71:8089/saml/attribute/emailaddress	Primary: user.userprincipalname
	Claim 2 (Secondary Email)	https://<UCM IP>[:port]/user/saml/attribute/otheremail Example: https://192.168.6.71:8089/user/saml/attribute/otheremail	Fallback: user.mail

Home

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Enterprise applications

App registrations

Protection

Identity Governance

External Identities

Show more

Protection

Identity Governance

Learn & support

Home > App registrations > Enterprise applications | All applications > GDMS Test | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim

Save Discard changes Got feedback?

Name *

https://account.gdms.cloud/saml/attribute/role

Namespace

Enter a namespace URI

Choose name format

Source *

Attribute

Transformation

Directory schema extension

Source attribute *

user.assignedroles

Claim conditions

Advanced SAML claims options

SAML Claim Configuration

Home > Attributes & Claims

Manage claim

Save Discard changes Got feedback?

Name *

role

Namespace

https://192.168.6.71:8089/saml/attribute

Choose name format

Source *

Attribute

Transformation

Directory schema extension

Source attribute *

user.assignedroles

Claim conditions

Advanced SAML claims options

SAML Claim Configuration

For Entra ID integrations, it is recommended that the Email claim must be set to **user.userprincipalname**. When using **user.mail** instead, please ensure that the Contact Email field is populated to avoid any SSO failures.

Home > Users

John Doe
User

Search << Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems Custom security attributes Assigned roles Administrative units Groups Applications Licenses Devices Azure role assignments Authentication methods New support request

Overview Monitoring **Properties**

Identity

Display name John Doe

First name

Last name **user.userprincipalname**

User principal name john.doe@onmicrosoft.com

Object ID

Identities onmicrosoft.com

User type Member

Creation type

Created date time Feb 6, 2026, 9:05 AM

Assigned licenses View

Preferred language

Contact Information

Street address

City

State or province

ZIP or postal code

Country or region

Business phone

Mobile phone **user.mail**

Email john.doe@company.com

Other emails

Proxy addresses View

Fax number

Entra User Properties

- Copy the highlighted information below required to complete the UCM63xx SAML configuration and authentication.

UCM63xx SAML | SAML-based Sign-on

Enterprise Application

<< Upload metadata file Change single sign-on mode Test this application Got feedback?

Overview Deployment Plan Diagnose and solve problems

Manage

Properties Owners Roles and administrators Users and groups **Single sign-on** Provisioning Application proxy Self-service Custom security attributes

Security

Conditional Access Permissions Token encryption

Activity

Sign-in logs

Unique User Identifier user.userprincipalname

3 SAML Certificates

Token signing certificate

Status Active

Thumbprint AAA17275AETC3D61B449C4D3F

Expiration 9/11/2029, 10:48:15 AM

Notification Email kelmerdi@

App Federation Metadata Url https://login.microsoftonline.com/f6e24392-14ba-...

Certificate (Base64) Download

Certificate (Raw) Download

Federation Metadata XML Download

Verification certificates (optional)

Required No

Active 0

Expired 0

4 Set up UCM63xx SAML

You'll need to configure the application to link with Microsoft Entra ID.

Login URL https://login.microsoftonline.com/14ba-...

Microsoft Entra Identifier https://sts.windows.net/f6e24392-943-...

Logout URL https://login.microsoftonline.com/f6e24392-14ba-...

Step 5: SAML SSO in Configuration on UCM63xx

- Paste the copied information into the **SAML SSO** configuration page on the UCM63xx. Navigate to: **Integrations -> Collaborative Office Integration -> SAML SSO**.

Collaborative Office Integration

Enterprise Platform **SAML SSO**

SAML SSO 

*** IdP Entity ID** 1 - 128 characters

X.509 Cert SHA1 Fingerprint 0 - 512 characters

*** SSO Login URL** 1 - 256 characters

*** User Mapping Attribute Name**  1 - 256 characters

Reply URL [Click to copy](#)

 Before using SSO, please fill this URL into the SAML Service Provider configuration.

Identifier ID [Click to copy](#)

Learn more about SAML SSO with the [SAML SSO Configuration Guide](#)

Providing Authentication information

2. In the **User Mapping Attribute Name** field, enter the **Source Attribute** defined in the **Manage claim** section of the Microsoft Entra admin center. This attribute is used to retrieve the corresponding user value from Entra ID and map it to the UCM6300 user.

Collaborative Office Integration

Enterprise Platform **SAML SSO**

SAML SSO 

*** IdP Entity ID** 1 - 128 characters

X.509 Cert SHA1 Fingerprint 0 - 512 characters

*** SSO Login URL** 1 - 256 characters

*** User Mapping Attribute Name**  1 - 256 characters

Reply URL [Click to copy](#)

 Before using SSO, please fill this URL into the SAML Service Provider configuration.

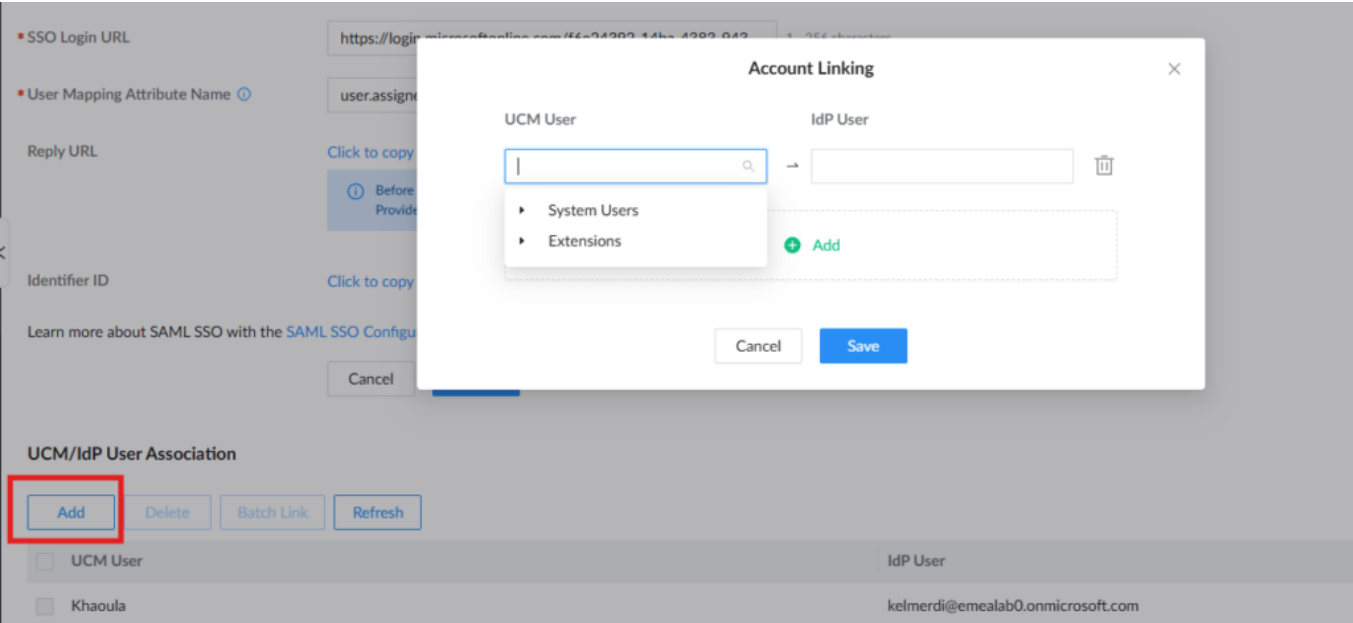
Identifier ID [Click to copy](#)

Learn more about SAML SSO with the [SAML SSO Configuration Guide](#)

Only the super administrator account has the permission to configure SAML SSO.

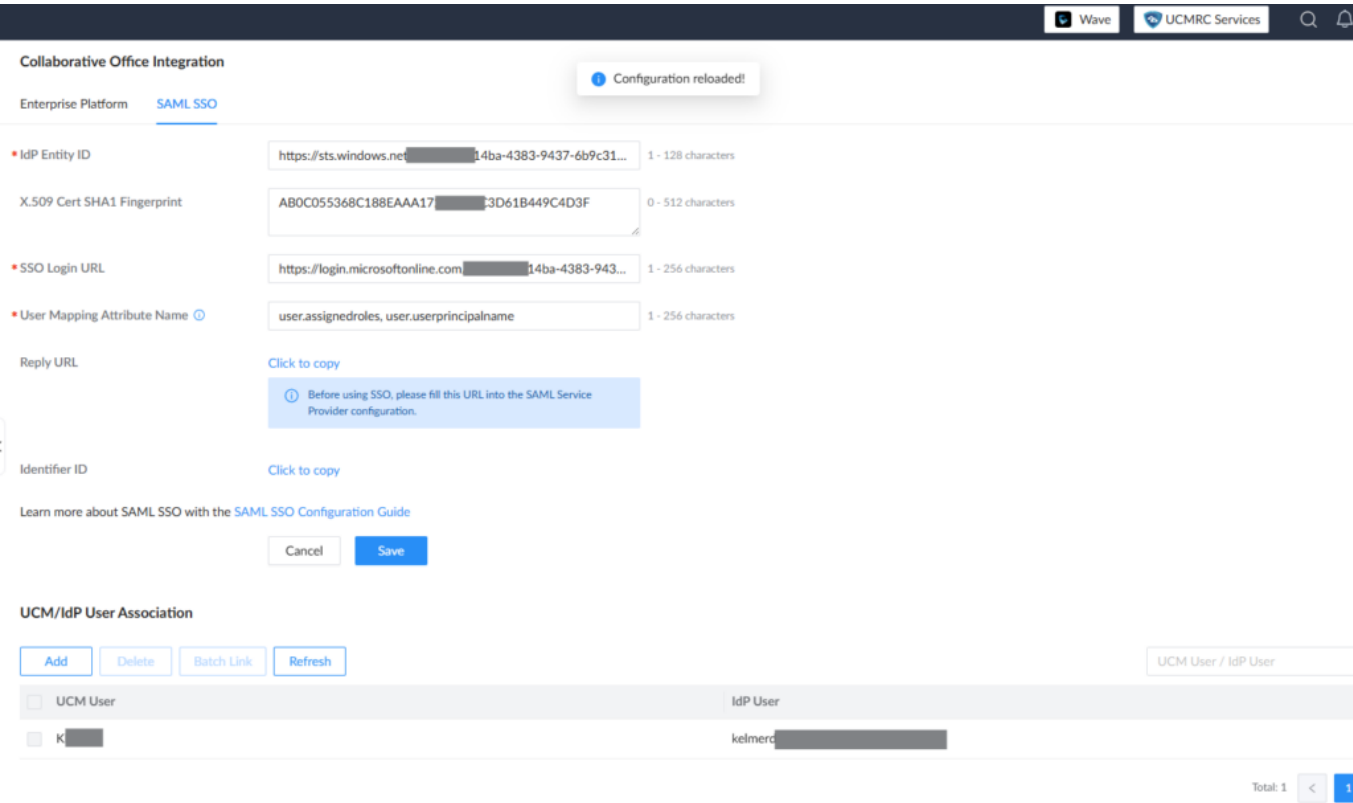
3. After establishing the SAML connection, create a **UCM User/IdP User mapping** to associate the users configured on the UCM6300 with their corresponding users in **Microsoft Entra ID**. UCM users can be

selected either from the **Extension List** or from the **registered users under User Management**.

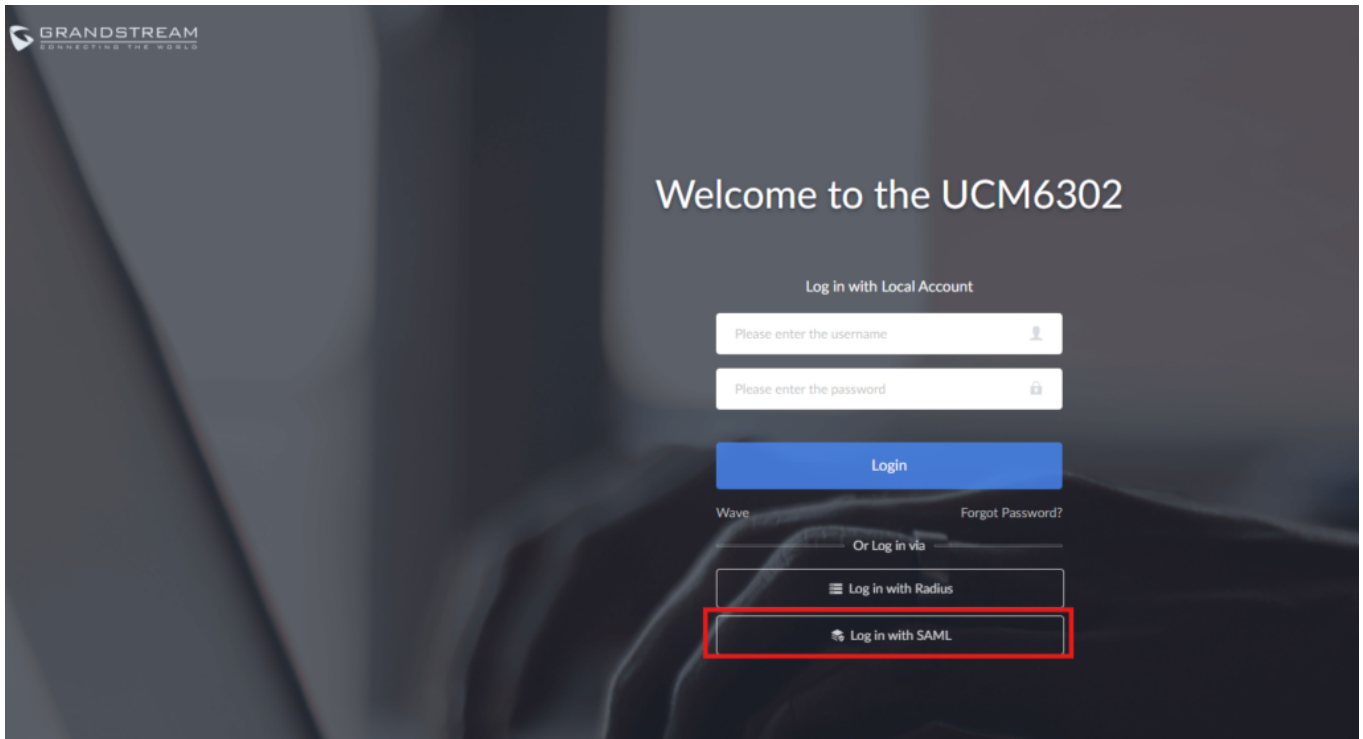


Adding SAML IdP in GDMS

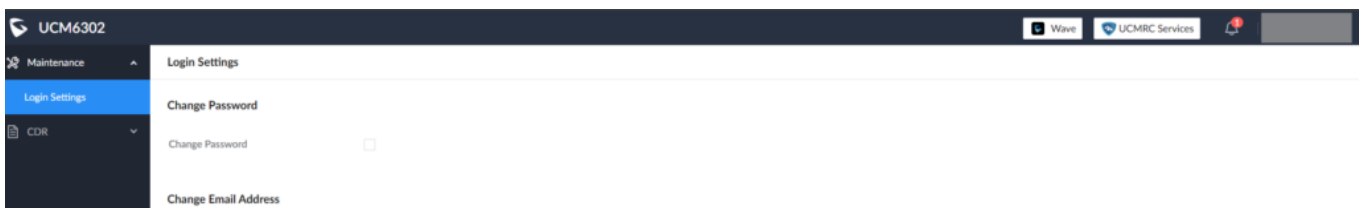
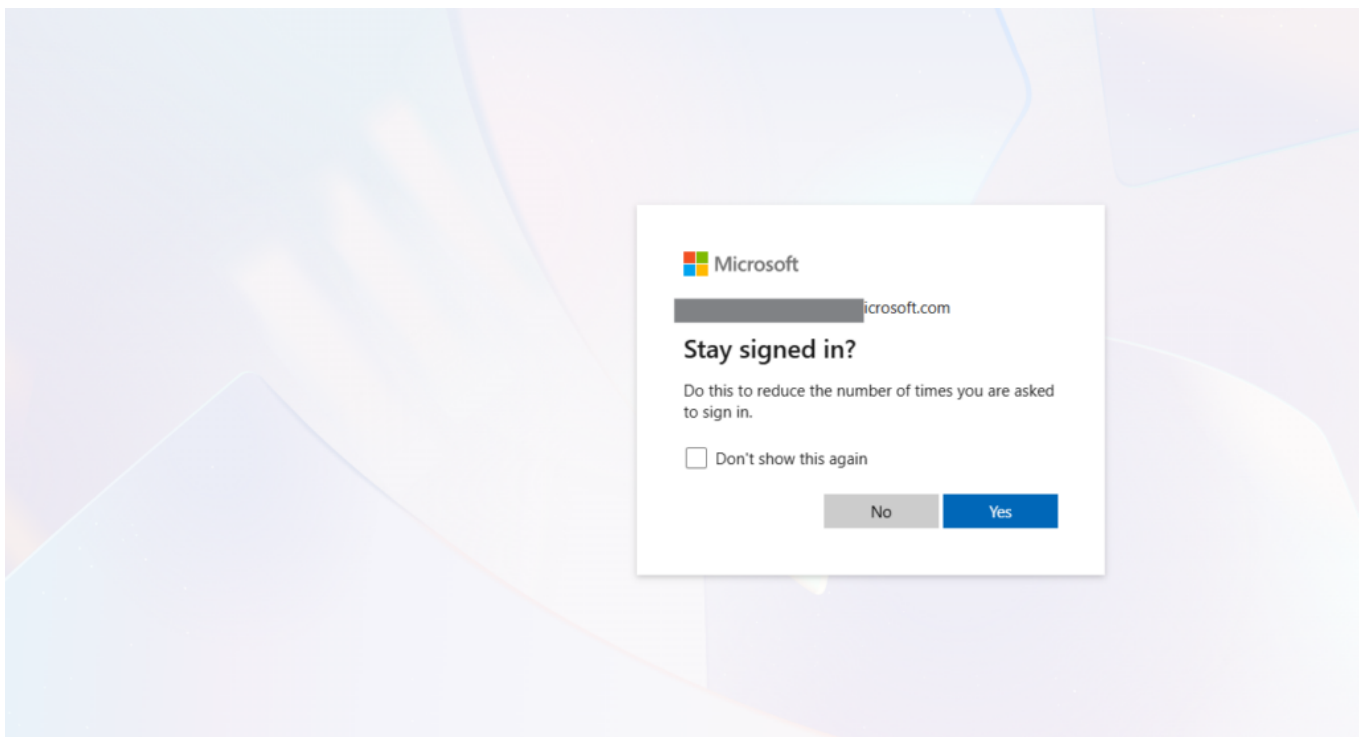
4. After adding the **UCM User/IdP User mapping**, save the configured users and click **Apply Changes** to save the SAML SSO configuration. The configuration is now complete.



5. To test the setup, return to the UCM login page and click the highlighted **Log in with SAML** icon to initiate SSO authentication.



6. You will then be redirected to the Microsoft login page. Enter the email address and password of the Microsoft Entra ID user associated with the UCM/IdP mapping. After successful authentication, you will be automatically logged in to the UCM6300.



SAML SSO LOGS

Administrators can review SAML SSO authentication activity from both the **UCM6300 local WebUI** and **Microsoft Entra ID** logs.

- **UCM6300:** Review the system logs from the local WebUI to troubleshoot SAML SSO authentication activity.
- **Microsoft Entra ID:** Review the sign-in logs for authentication attempts and related SAML activity.

Reviewing logs on both the **Service Provider (UCM6300)** and **Identity Provider (Microsoft Entra ID)** sides can help identify configuration or authentication issues.

UCM6300 records SAML SSO login and logout events in the **System Log**.

1. Log in to the **UCM6300 WebUI** as a **Super Administrator**.
2. Access the logs using the following path:
 - Navigate to **Maintenance -> Operation Log**.
3. SAML-based login attempts are recorded in the operation log and can be reviewed for authentication activity and troubleshooting.

GDMS Unified Communications

Plans & Services

World

yxxu123

Dashboard

Organization

Default

VoIP Device

Call Quality

Device Template

Site

Task

Diagnostics

System

Resources

Alerts

Reseller Channel

RPS Management

Users

System Log

API Developer

System Log

Account Center

All Levels

All Operations

Q Operator / IP

Filter

Time	Operator	IP Address	Level	Details
2024/10/31 20:30	yxxu123	192.168.126.122	Notice	Sign In
2024/10/31 20:30	h[REDACTED]m	192.168.126.122	Notice	Sign Out
2024/10/31 20:17	h[REDACTED]om	192.168.126.122	Notice	Sign In
2024/10/31 20:16	yxxu123	192.168.126.122	Notice	Sign Out
2024/10/31 20:11	yxxu123	192.168.126.122	Notice	Sign In
2024/10/31 15:17	yxxu123	192.168.126.122	Notice	Sign Out
2024/10/31 15:17	yxxu123	192.168.126.122	Notice	Sign Out
2024/10/31 14:25	yxxu123	172.16.141.36	Notice	Sign In
2024/10/31 12:10	yxxu123	192.168.126.122	Notice	Sign In
2024/10/31 12:06	yxxu123	192.168.126.122	Notice	Sign Out

Total 101

10/page

<

1

2

3

4

5

6

...

11

>

© 2024 Grandstream Networks, Inc.

Cookies

GDMS SAML SSO Logs

You can also review SAML SSO login attempts in the **Microsoft Entra ID sign-in logs**, including successful and failed authentication events.

Enterprise applications | Sign-in logs

DownloadExport data SettingsTroubleshootRefreshManage viewGot feedback?

Want to switch back to the legacy signin logs experience? Click here to leave the preview.

Add filterShow dates as: U...Date range: Last 24 hoursReset filters

User sign-ins (Interactive)User sign-ins (non-interactive)Service principal sign-insManaged identity sign-ins

Date ↓	Request ID	User principal name	Application	Status	IP address	Resource	Res
2026-09-11T12:05:59Z		kelme	UCM63xx SAML	Success	197.230.72.219	Windows Azure Active ...	00C
2026-09-11T12:05:24Z		kelme	UCM63xx SAML	Interrupted	197.230.72.219	Windows Azure Active ...	00C
2026-09-11T12:05:15Z		kelme	UCM63xx SAML	Failure	197.230.72.219	Windows Azure Active ...	00C
2026-09-11T12:05:03Z		kelme	UCM63xx SAML	Failure	197.230.72.219	Windows Azure Active ...	00C
2026-09-11T10:38:47Z		kelme	UCM63xx SAML	Success	197.230.72.218	Windows Azure Active ...	00C
2026-09-11T10:38:34Z		kelme	UCM63xx SAML	Success	197.230.72.218	Windows Azure Active ...	00C
2026-09-11T10:37:25Z		kelme	UCM63xx SAML	Success	197.230.72.218	Windows Azure Active ...	00C
2026-09-11T10:37:23Z		kelme	UCM63xx SAML	Interrupted	197.230.72.218	Windows Azure Active ...	00C
2026-09-11T10:37:13Z		kelme	UCM63xx SAML	Failure	197.230.72.218	Windows Azure Active ...	00C

Overview

Diagnose and solve problems

Manage

Security

Activity

SUPPORTED DEVICES

Models	Firmware Required
UCM630x Series	1.0.35.4+
UCM630xA Series	1.0.35.4+