

Grandstream Networks, Inc.

SAML Single Sign-On (SSO) Configuration Guide



OVERVIEW

GDMS and GWN Manager support SAML (Security Assertion Markup Language) to provide external authentication and Single Sign-On (SSO) using third-party identity providers such as Microsoft Entra ID (Azure AD), AD FS, and Duo.

This guide outlines how to configure SAML information on supported third-party identity providers as well as how to use SAML SSO on GDMS (Cloud) and GWN Manager (On-Prem).

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 GDMS platform and GWN Manager.

SAML SSO LOGIN METHODS

SAML SSO login supports two methods:

- ↳ **Method 1:** Users authenticate directly from a third-party identity provider portal (such as Entra MyApps or Duo Dashboard) and are redirected to the platform.
- ↳ **Method 2:** Users access the GDMS or GWN Manager login page directly and are redirected to the configured SAML identity provider for authentication.

SAML SSO WITH MICROSOFT ENTRA ID

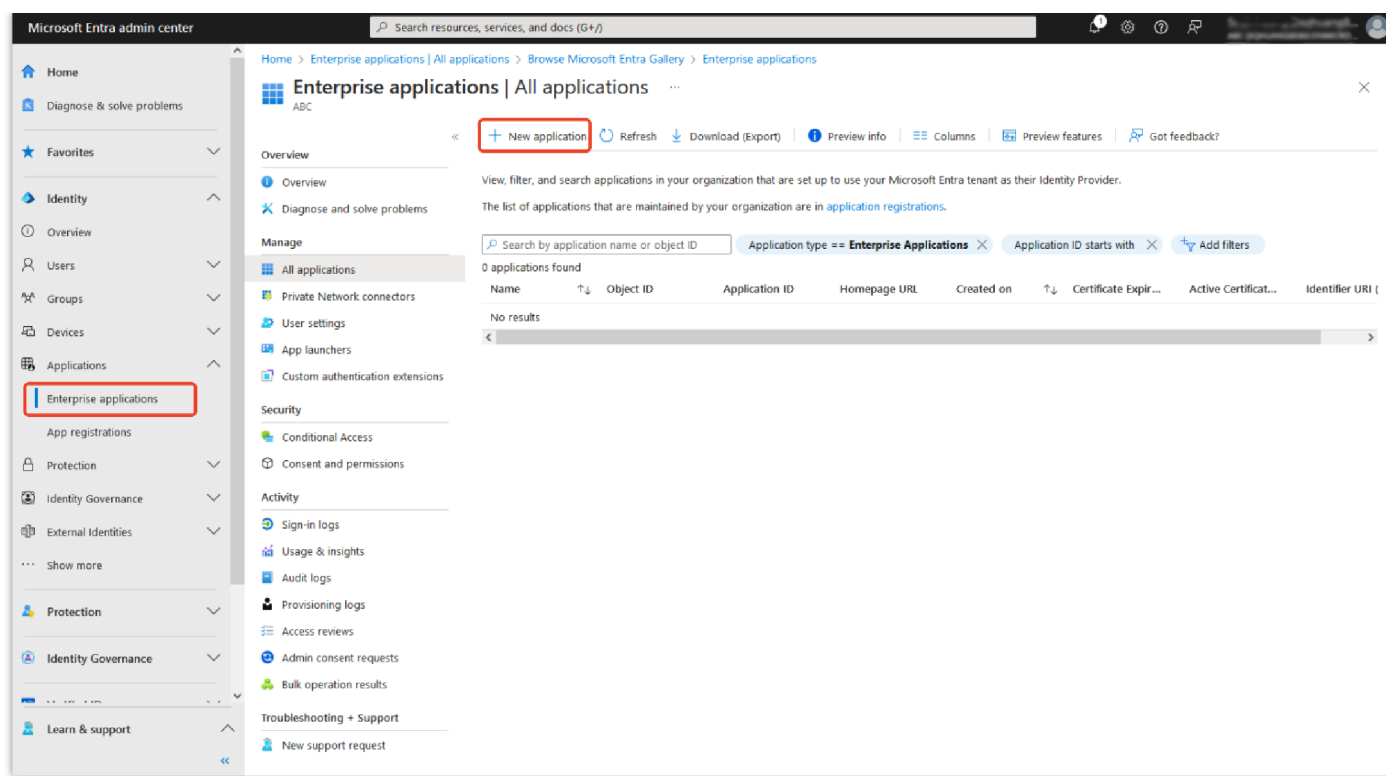
Firstly, users need to sign up for an Azure account by visiting this web page:

<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 GDMS.

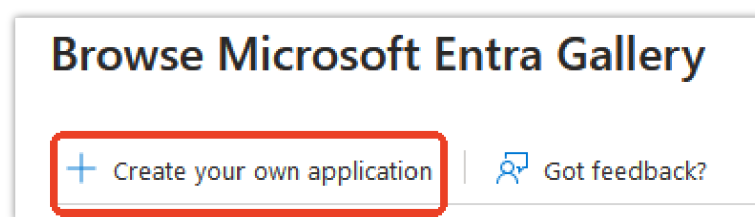
Step 1: Add a new application in Azure

1. Sign in to the [Microsoft Entra admin center](#) as a [Cloud Application Administrator](#) or higher.
2. Go to **Identity** → **Applications** → **Enterprise applications** → **New application**.

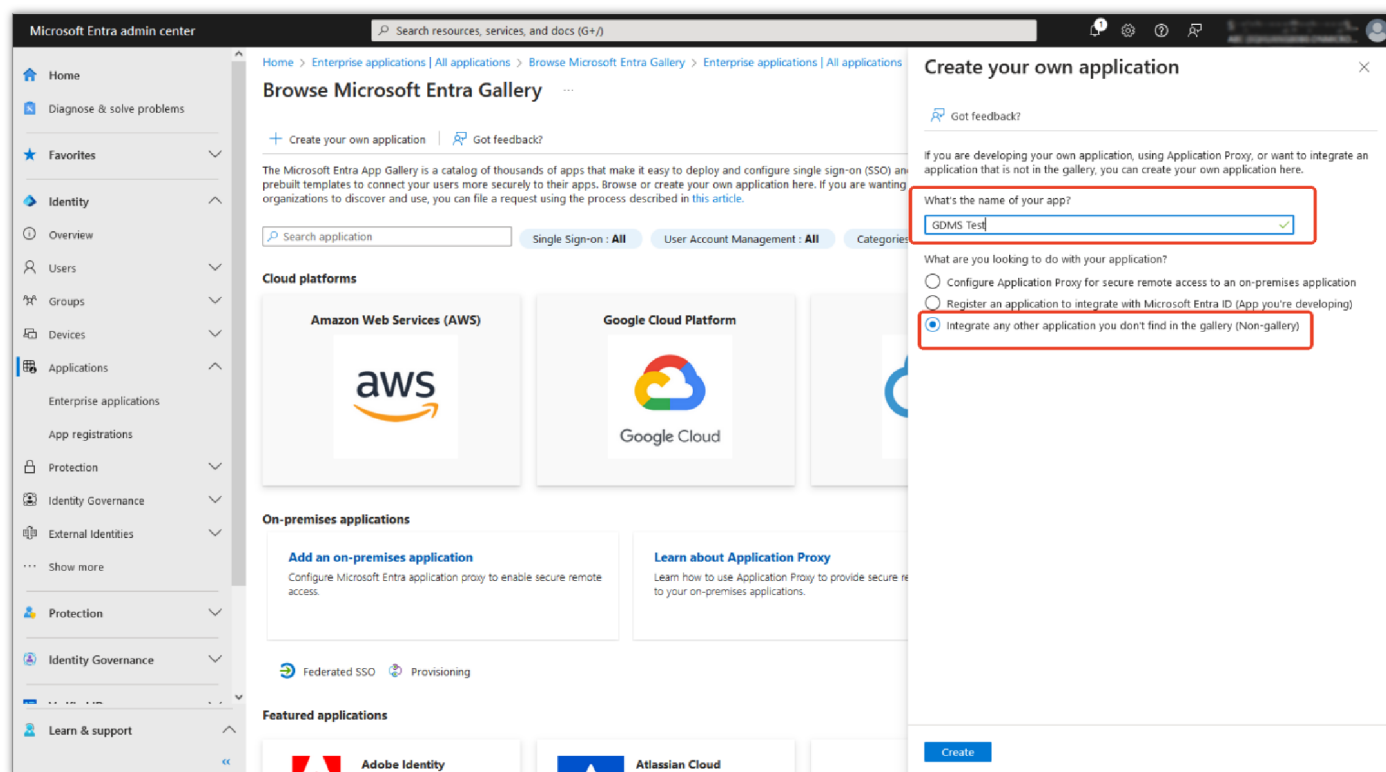


Add a New Application

3. In the **Browse Microsoft Entra Gallery** section, click **Create your own application**.



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



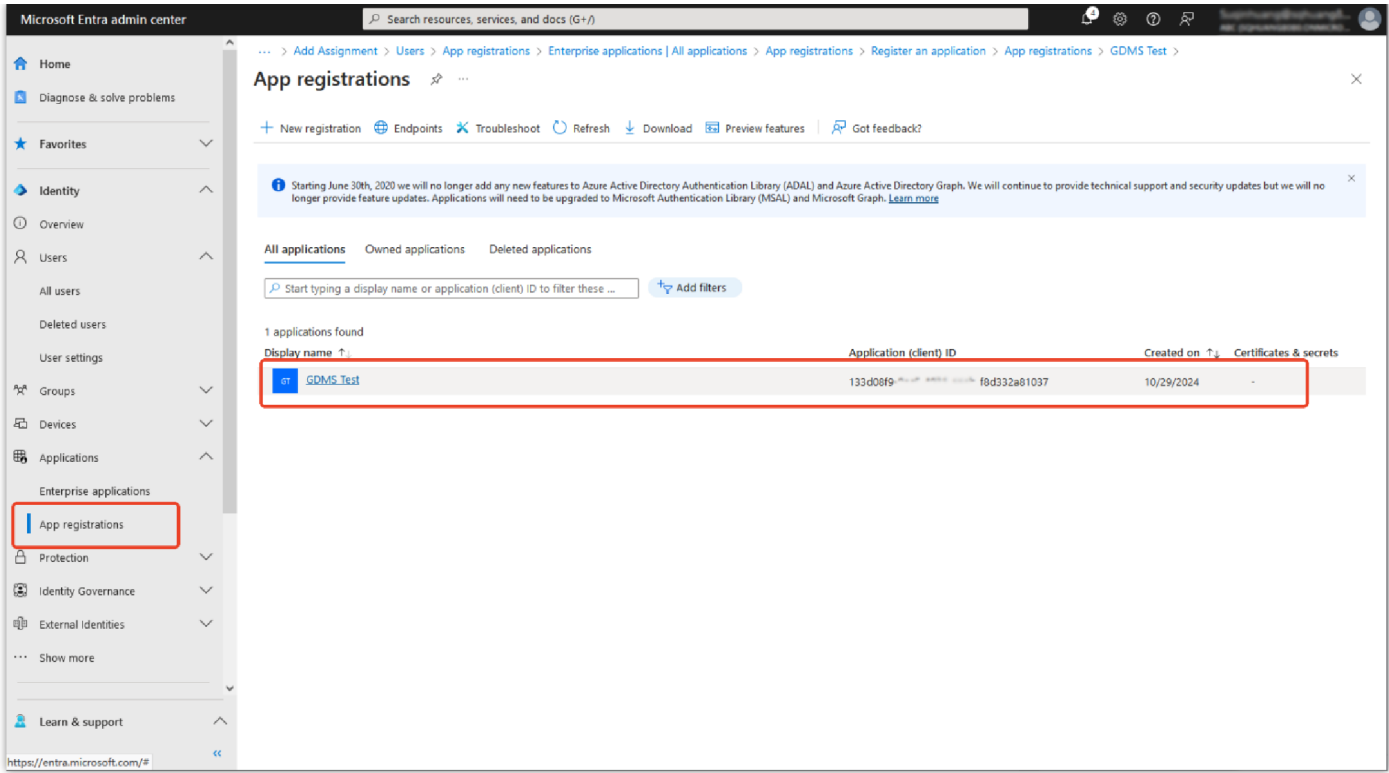
Creating an Application in Azure

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

1 application found							
Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry St...	Active Certificate Ex...	Identifier URI (Entity...
GDMS Test	0ac73d01-4a64-ba...	133d01-4021-aae...	https://account.activedire...	10/29/2024	-	-	133d01-4021-aae...

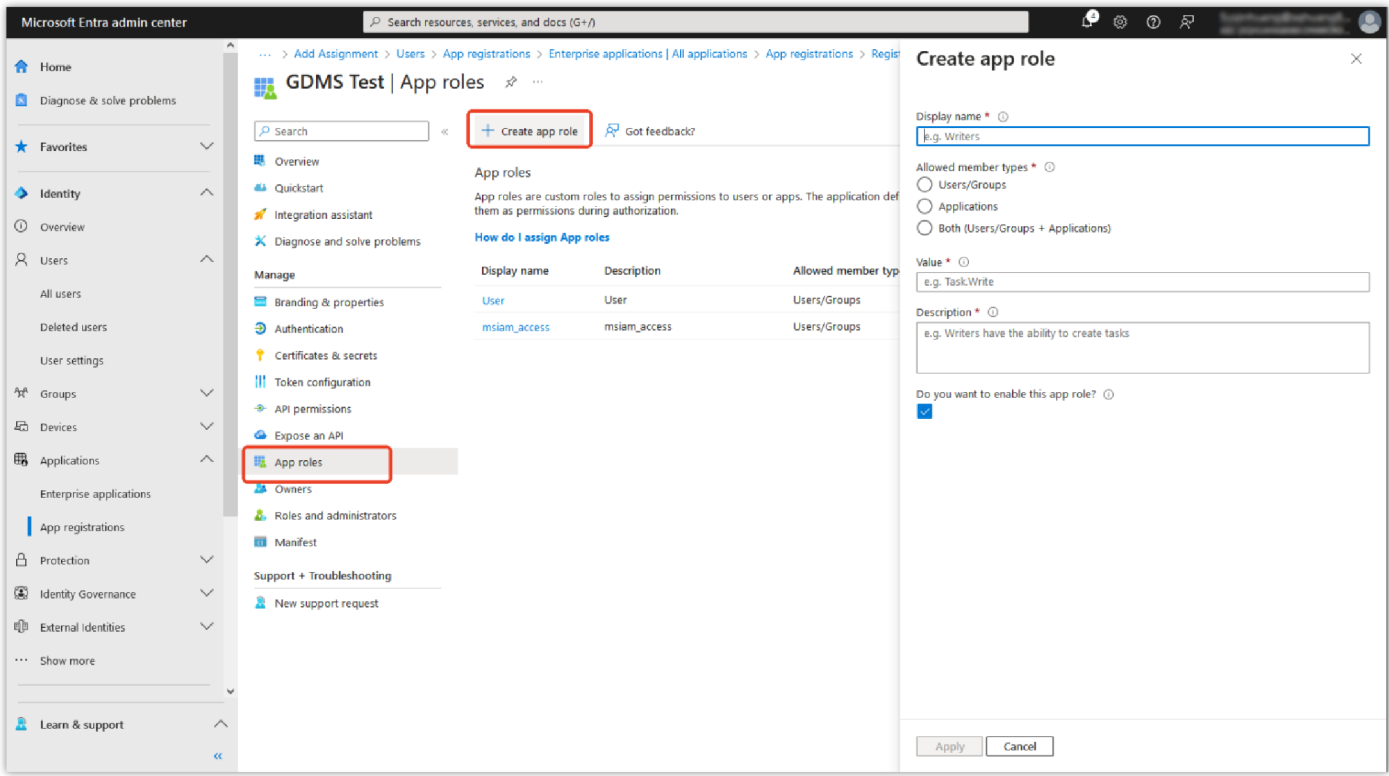
Step 2: Create an application role in Azure

1. Sign in to the [Microsoft Entra admin center](#), go to Identity → Applications → APP registrations, and click on the app you have created.



Azure App Registrations Page

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

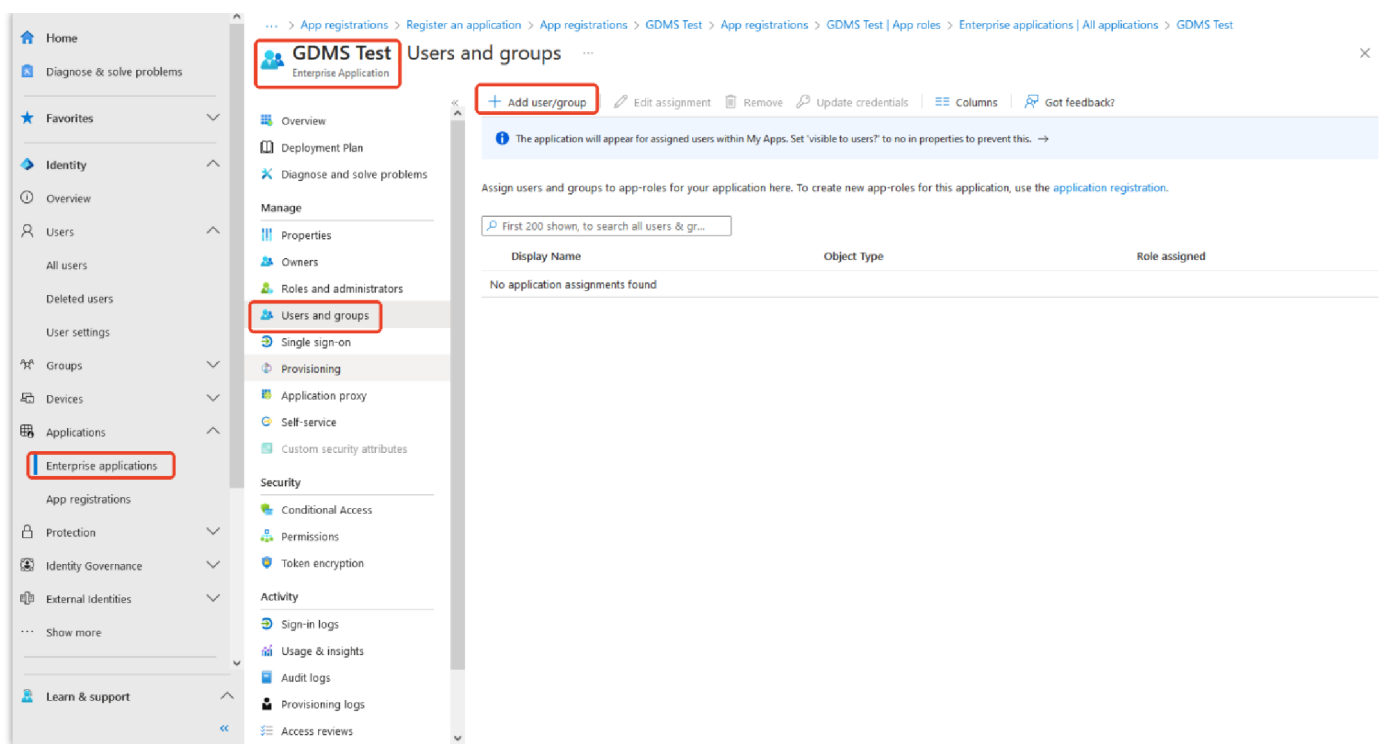
3. After successful creation, you can see this role in the list.

App roles					
App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.					
How do I assign App roles					
Display name	Description	Allowed member types	Value	ID	State
User	User	Users/Groups		18d14569-c3bd-439b-...	Enabled
msiam_access	msiam_access	Users/Groups		b9632174-c057-4f7e-9...	Enabled
Admin A	Admin A is an admin	Users/Groups	Admin.A	7528cbcc-cc39-425c-9...	Enabled

List of App Roles

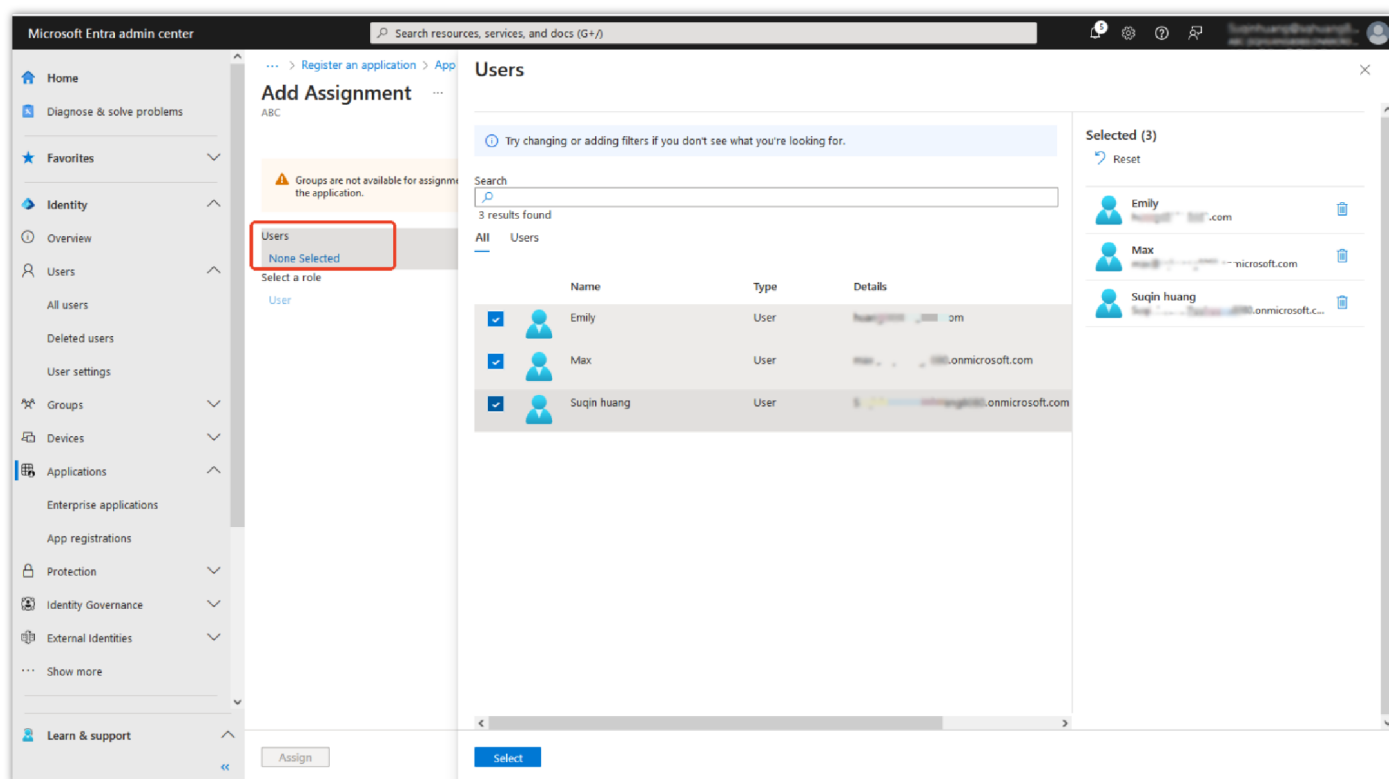
Step 3: Add users to the application in Azure

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**.



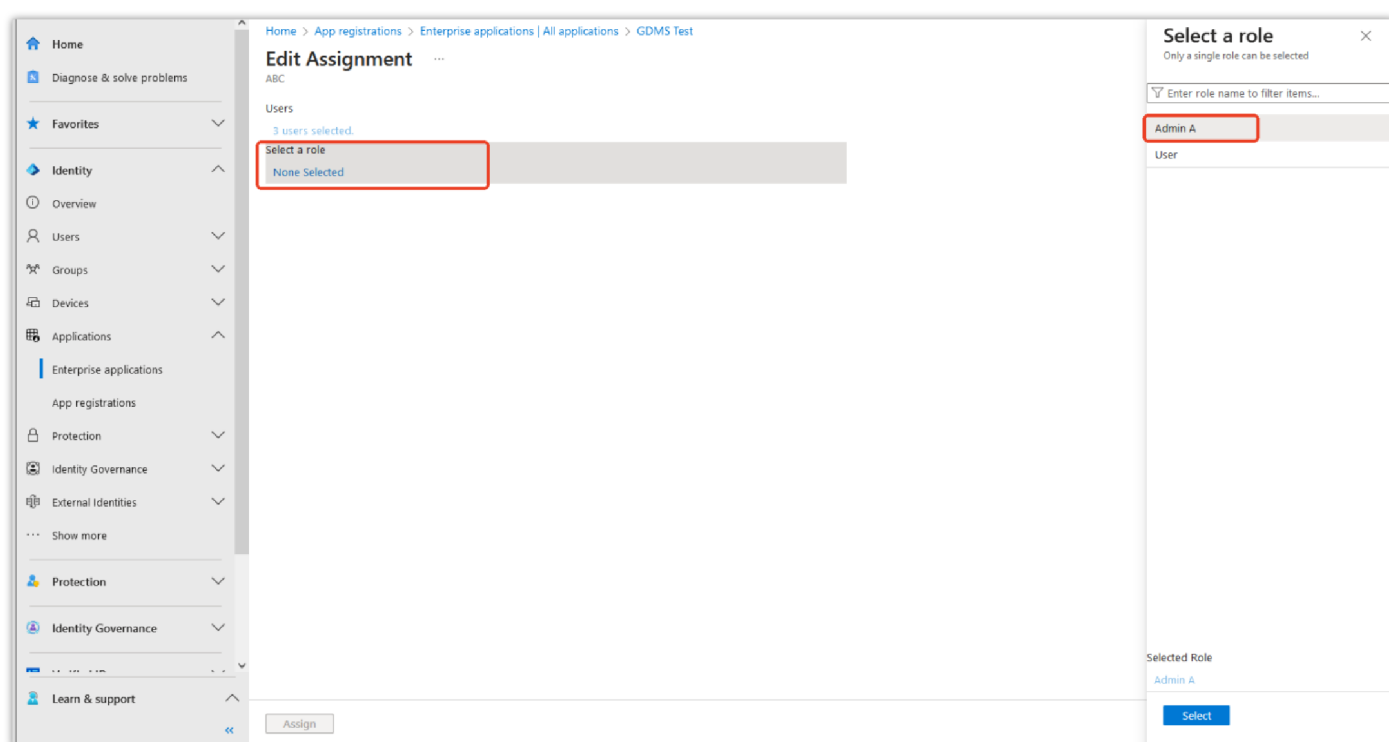
Add UserGroup to an App

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



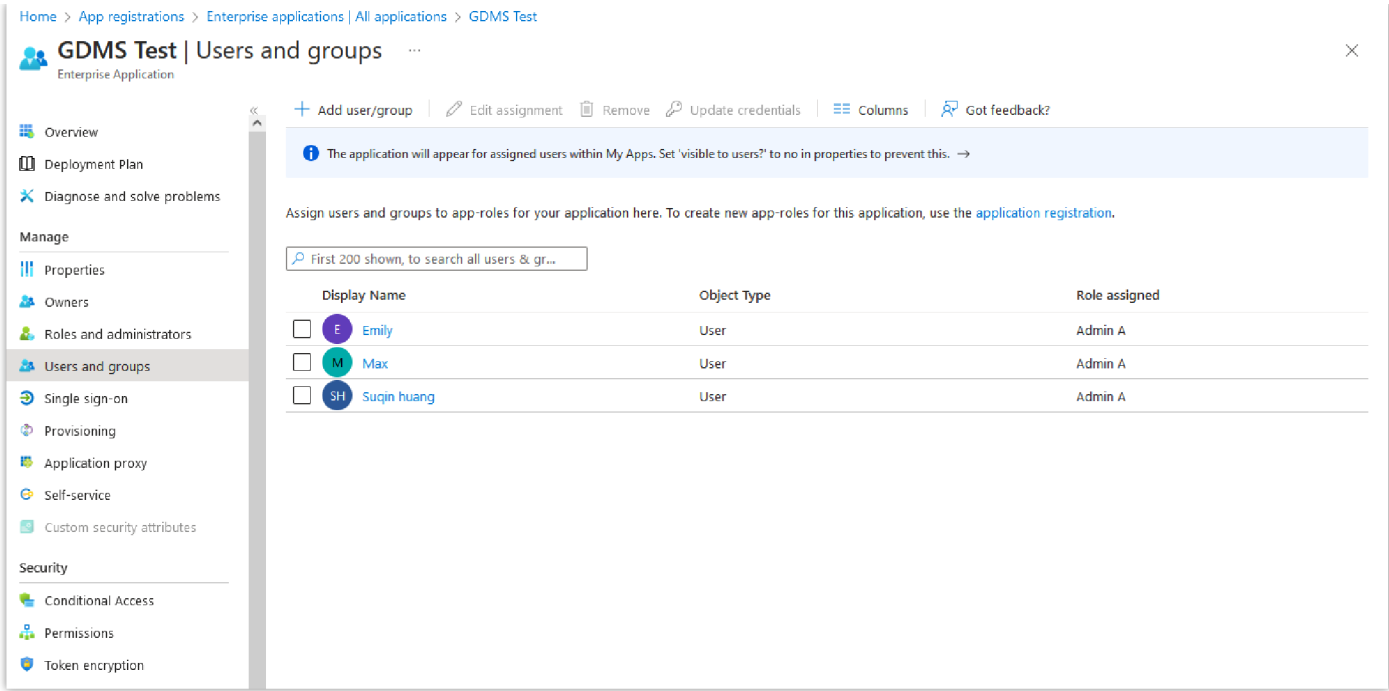
App User Selection

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



Assigning Roles to App Users

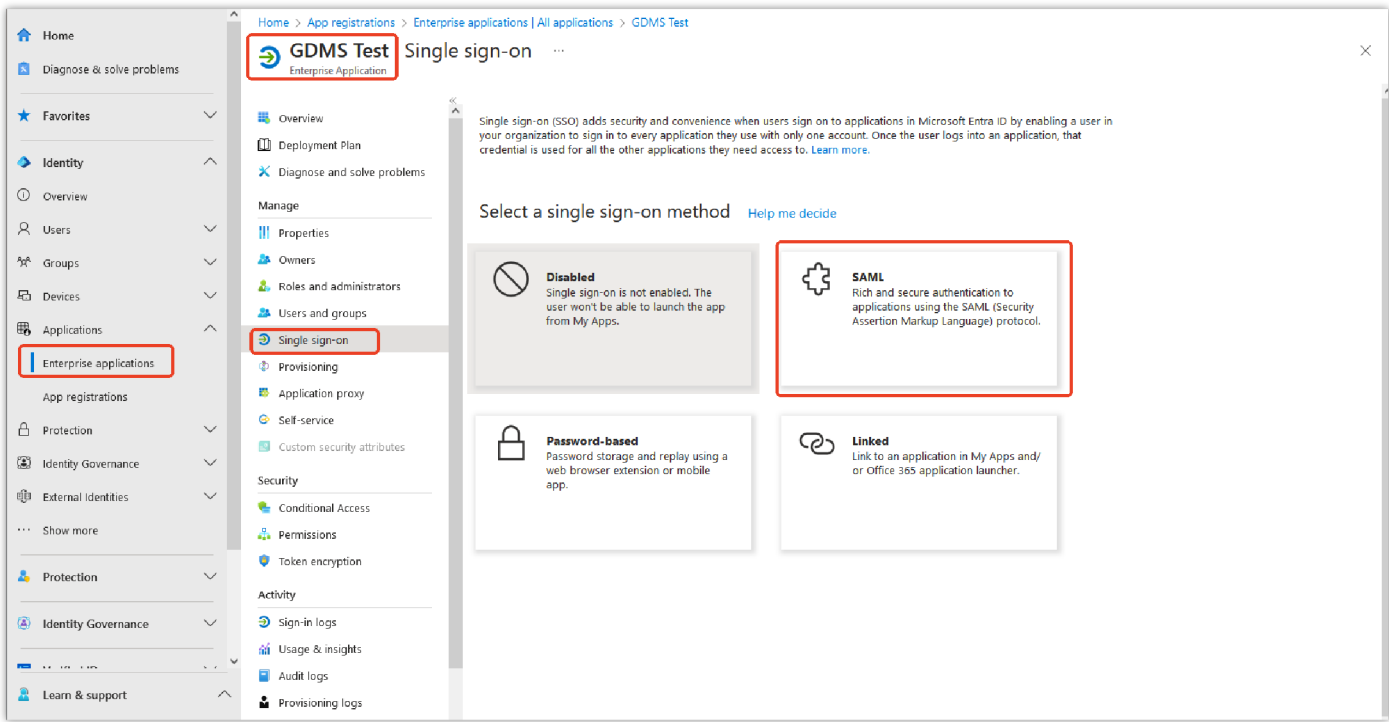
5. Then click **Assign**. After the assignment is successful, you can see the selected users and the assigned roles in the list. (These users can then log in to GDMS/GWN Manager with a single sign-on)



List of App Assigned Users

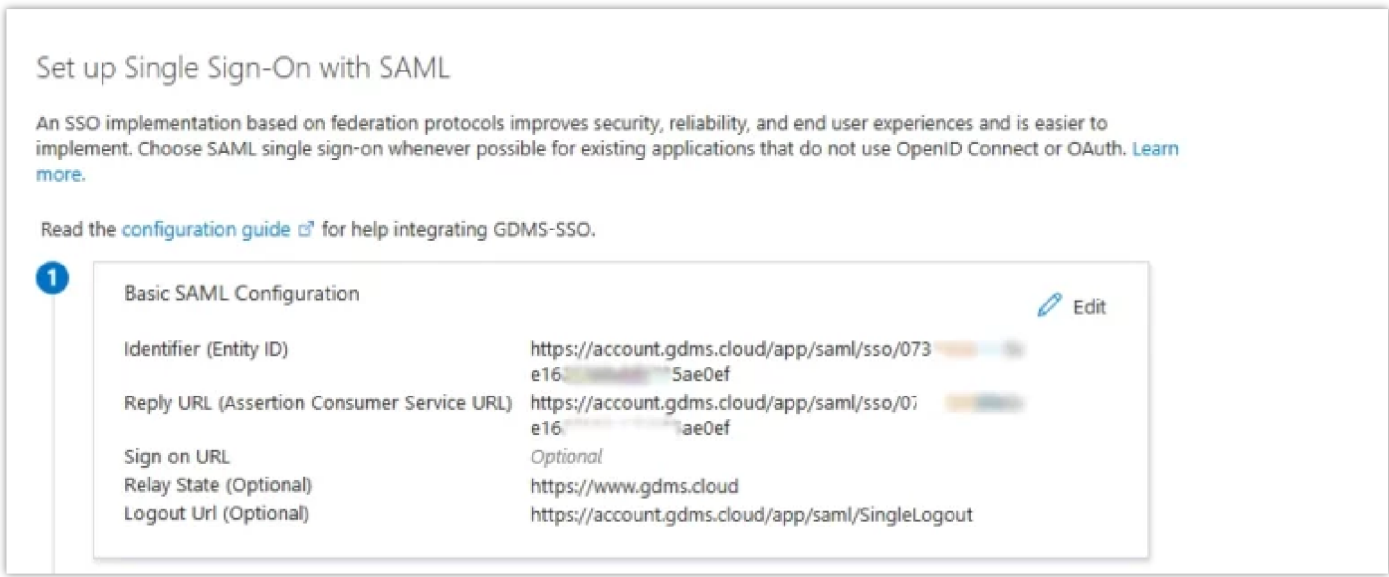
Step 4: Set up SSO in Azure

- 1. Sign in to the [Microsoft Entra admin center](#), go to **Identity** → **Applications** → **Enterprise applications**, find and click the app you have previously created.
- 2. 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**.

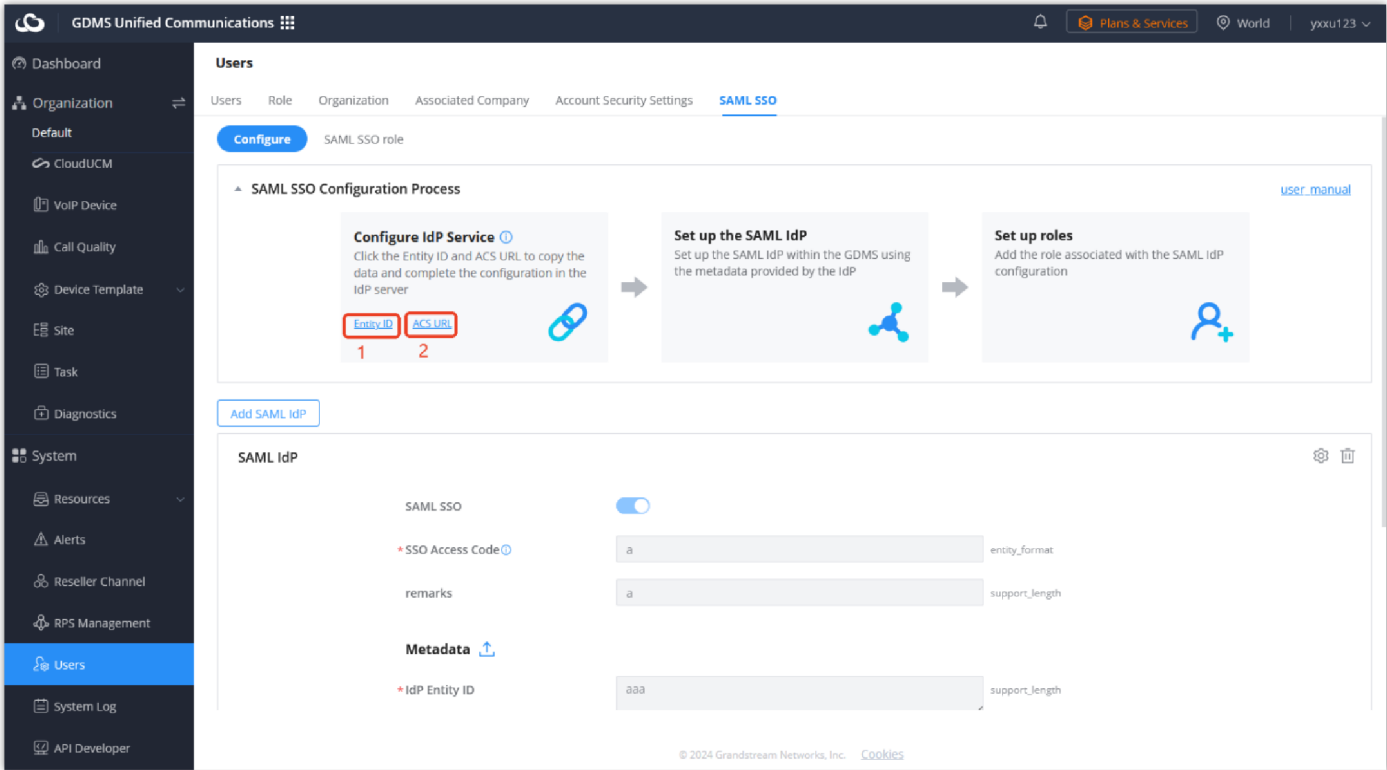


App Basic SAML Configuration

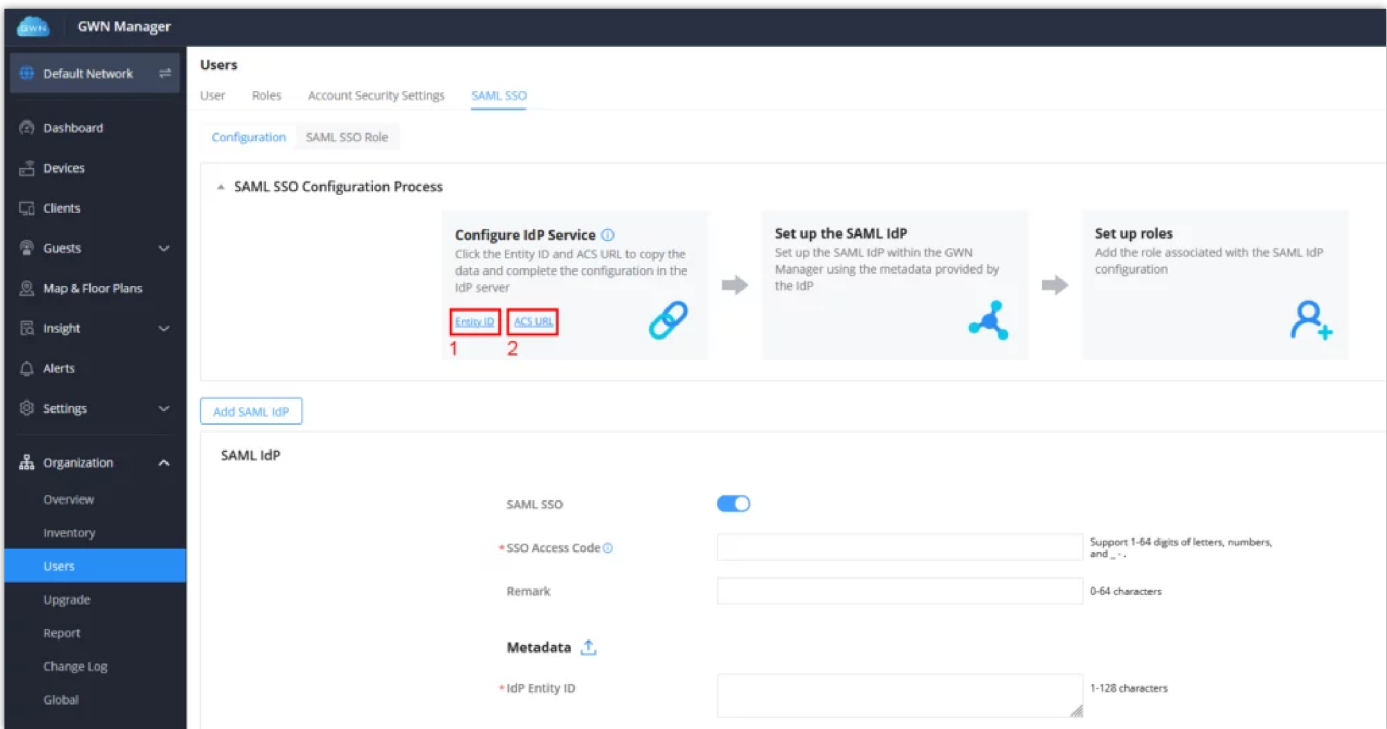
- 4. Copy the information from the GDMS/GWN platform and fill in the following information:

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)

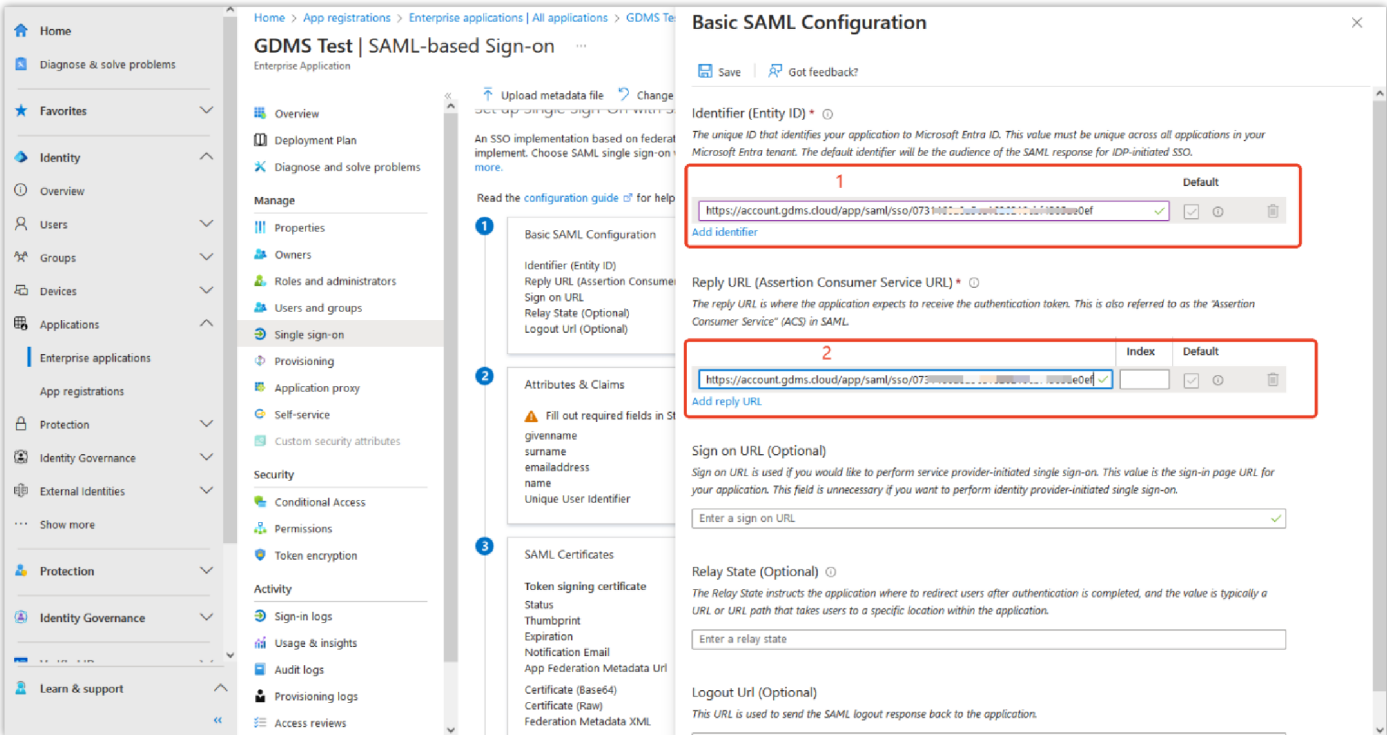
Relay State	Specify the Service Provider URL that users should be redirected to after successful authentication. • For GDMS, enter: <i>https://www.gdms.cloud</i> • For GWN Manager, enter the access URL, which may be either: <i>https://<gwn-manager-domain>:<port></i> or <i>https://<gwn-manager-ip>:<port></i> Note: Although this field appears optional, it is required for this integration. You must configure it to prevent user errors.
-------------	--



GDMS SAML SSO Configuration Page



GWN Manager SAML SSO Configuration Page



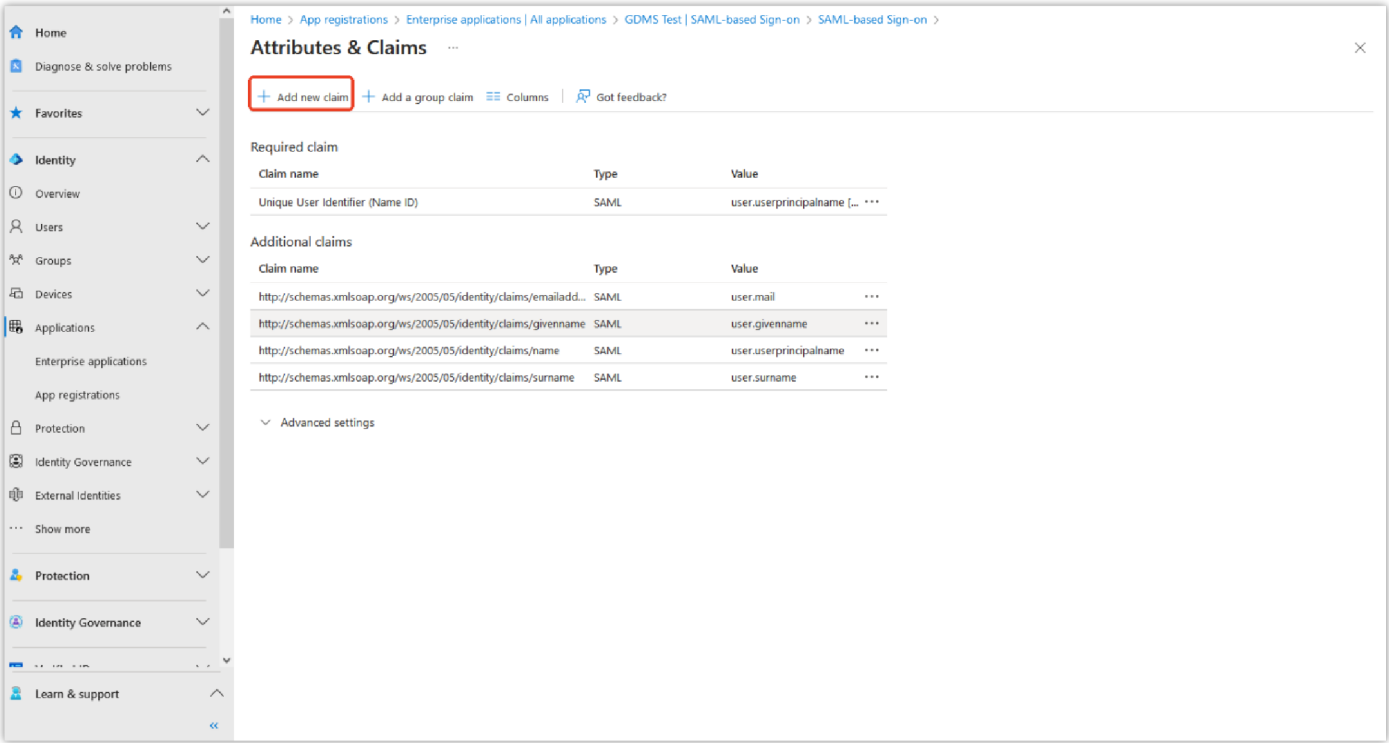
Copying the Entity ID and ACS URL to Entra ID

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

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

SAML Attributes Claims Section

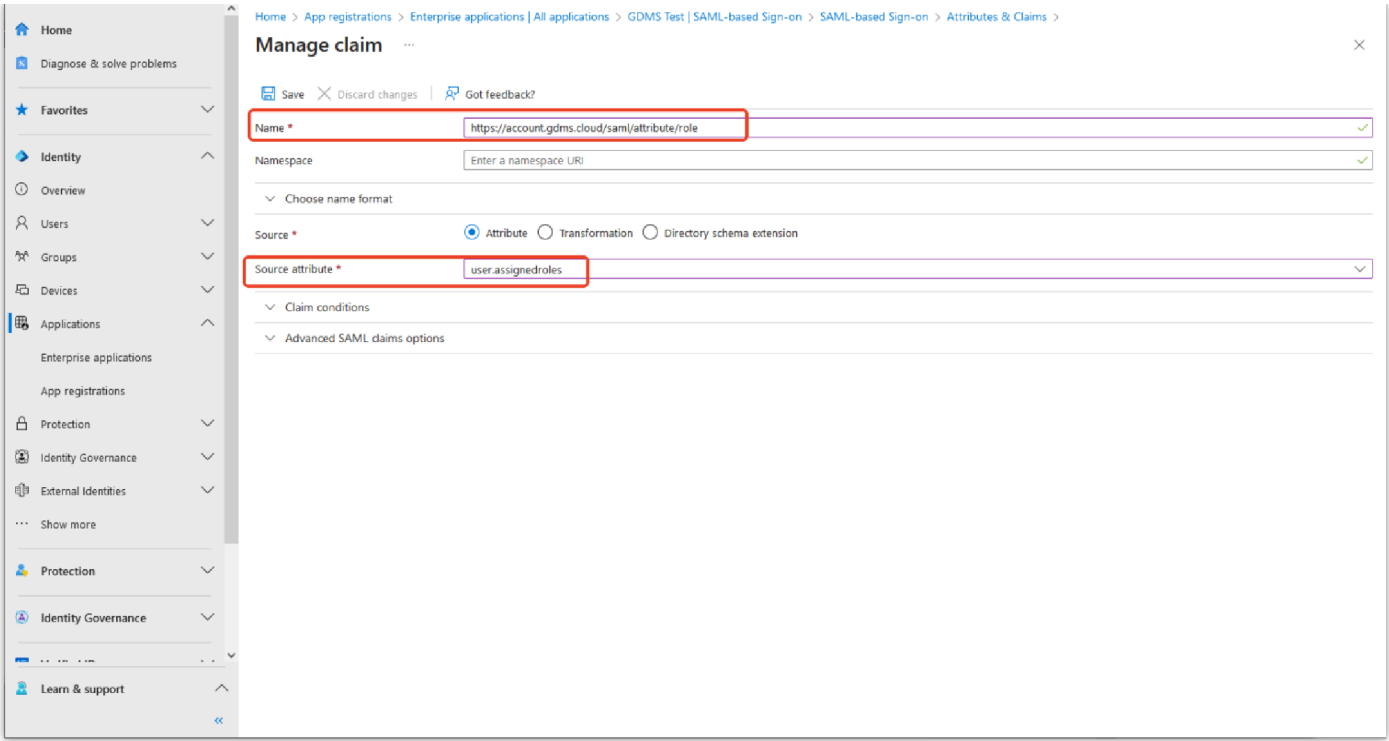
6. Click **Add new Claim**.



Add a New Claim

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

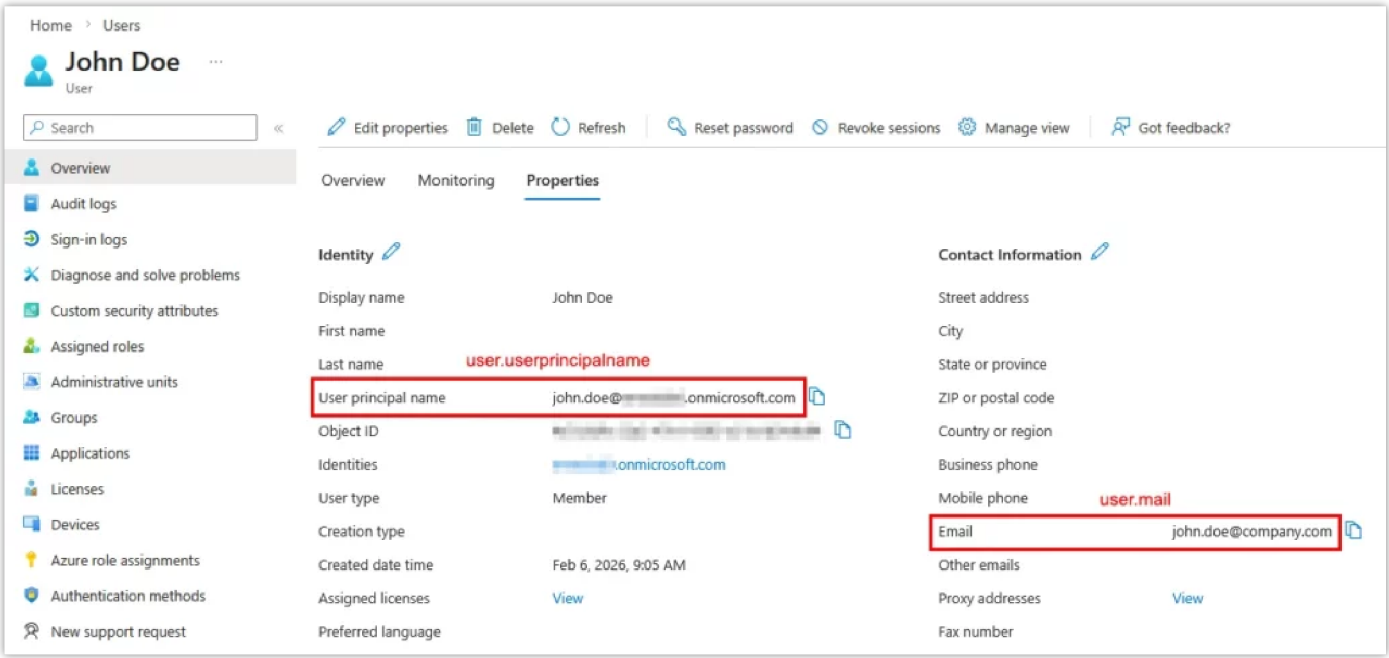
	Claim	Name	Source attribute
GDMS	Claim 1 (Role)	https://account.gdms.cloud/saml/attribute/role	user.assignedroles
	Claim 2 (Email)	https://account.gdms.cloud/saml/attribute/emailaddress	○ Primary: user.userprincip alname ○ Fallback: user.mail
	Claim 3 (Other Email)	https://account.gdms.cloud/saml/attribute/otheremail	user.mail
GWN Manager	Claim 1 (Role)	<a href="https://<gwn-manager-host>[:port]/user/saml/attribute/role">https://<gwn-manager-host>[:port]/user/saml/attribute/role	user.assignedroles
	Claim 2 (Email)	<a href="https://<gwn-manager-host>[:port]/user/saml/attribute/emailaddress">https://<gwn-manager-host>[:port]/user/saml/attribute/emailaddress	○ Primary: user.userprincip alname ○ Fallback: user.mail
	Claim 3 (Other Email)	<a href="https://<gwn-manager-host>[:port]/user/saml/attribute/otheremail">https://<gwn-manager-host>[:port]/user/saml/attribute/otheremail	user.mail



SAML Claim Configuration

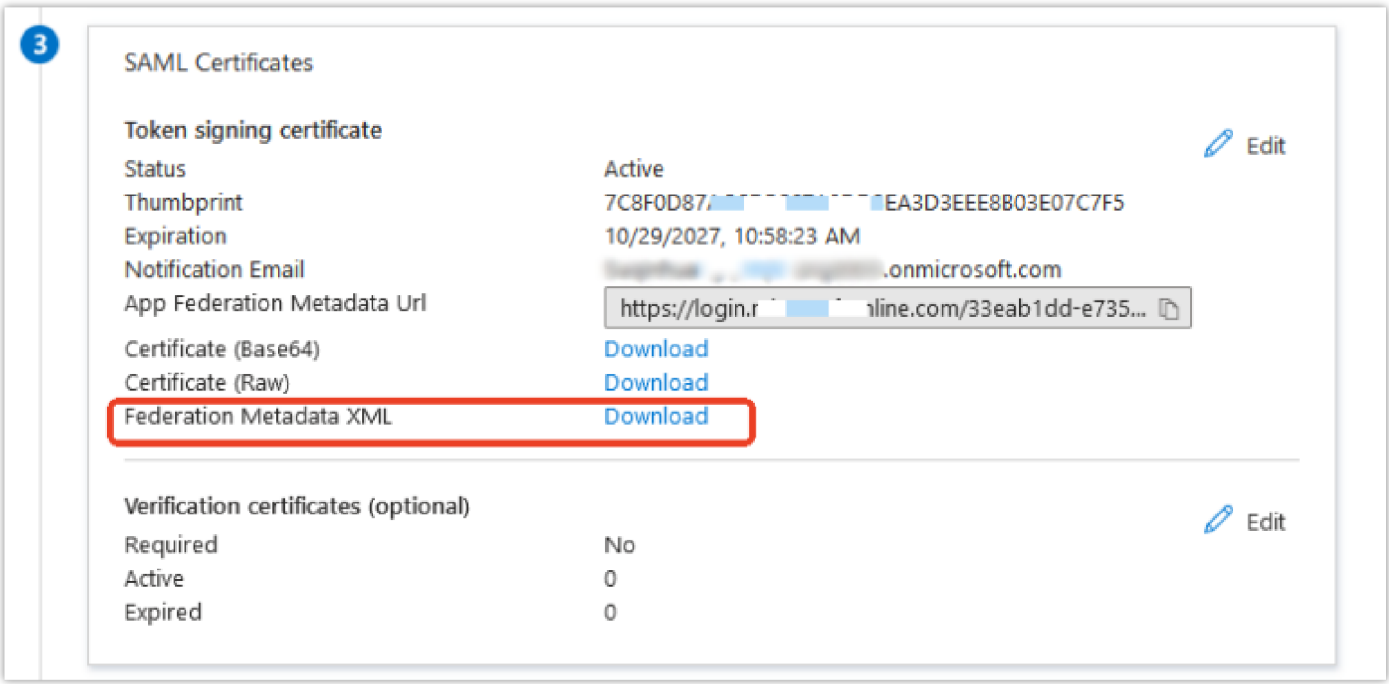
Note:

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.



Entra User Properties

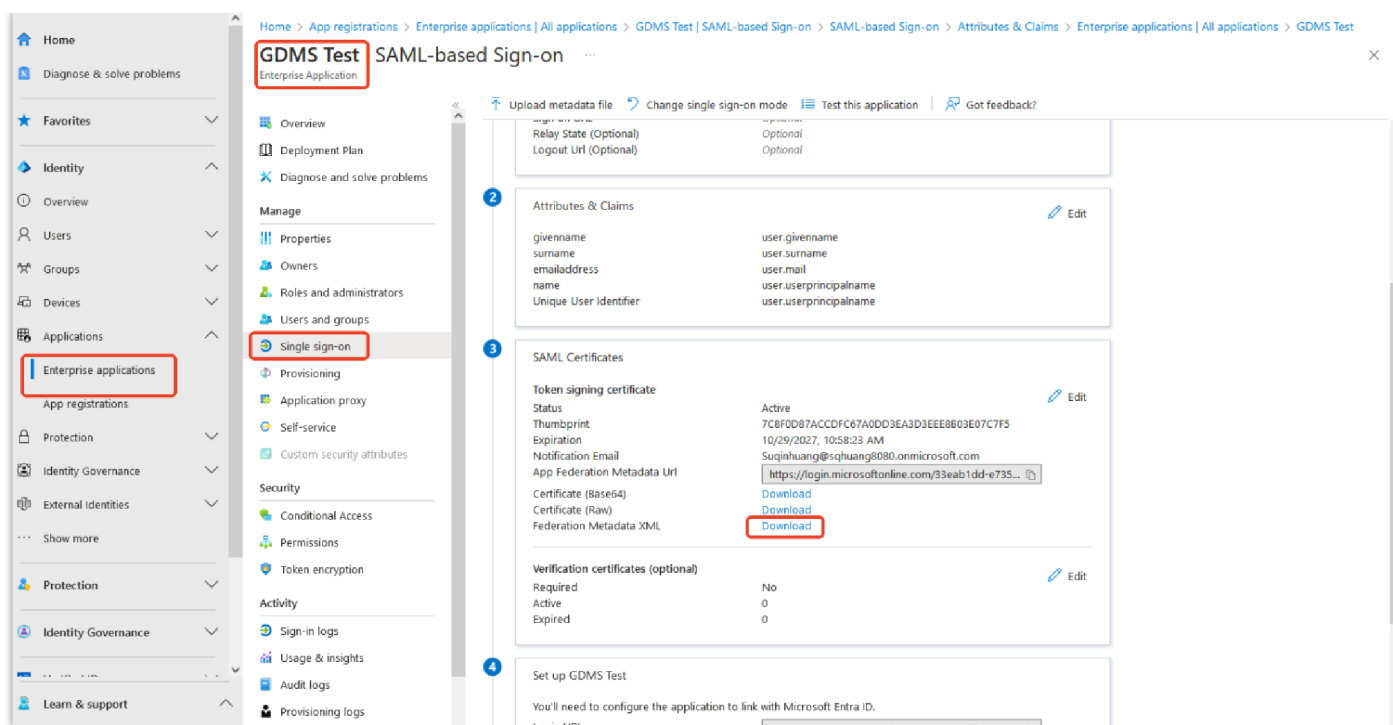
8. Download the metadata file for configuration on GDMS.



SAML XML Metadata

Step 5: SAML SSO in GDMS/GWN Manager

1. Download the metadata of the GDMS application you created from Azure.



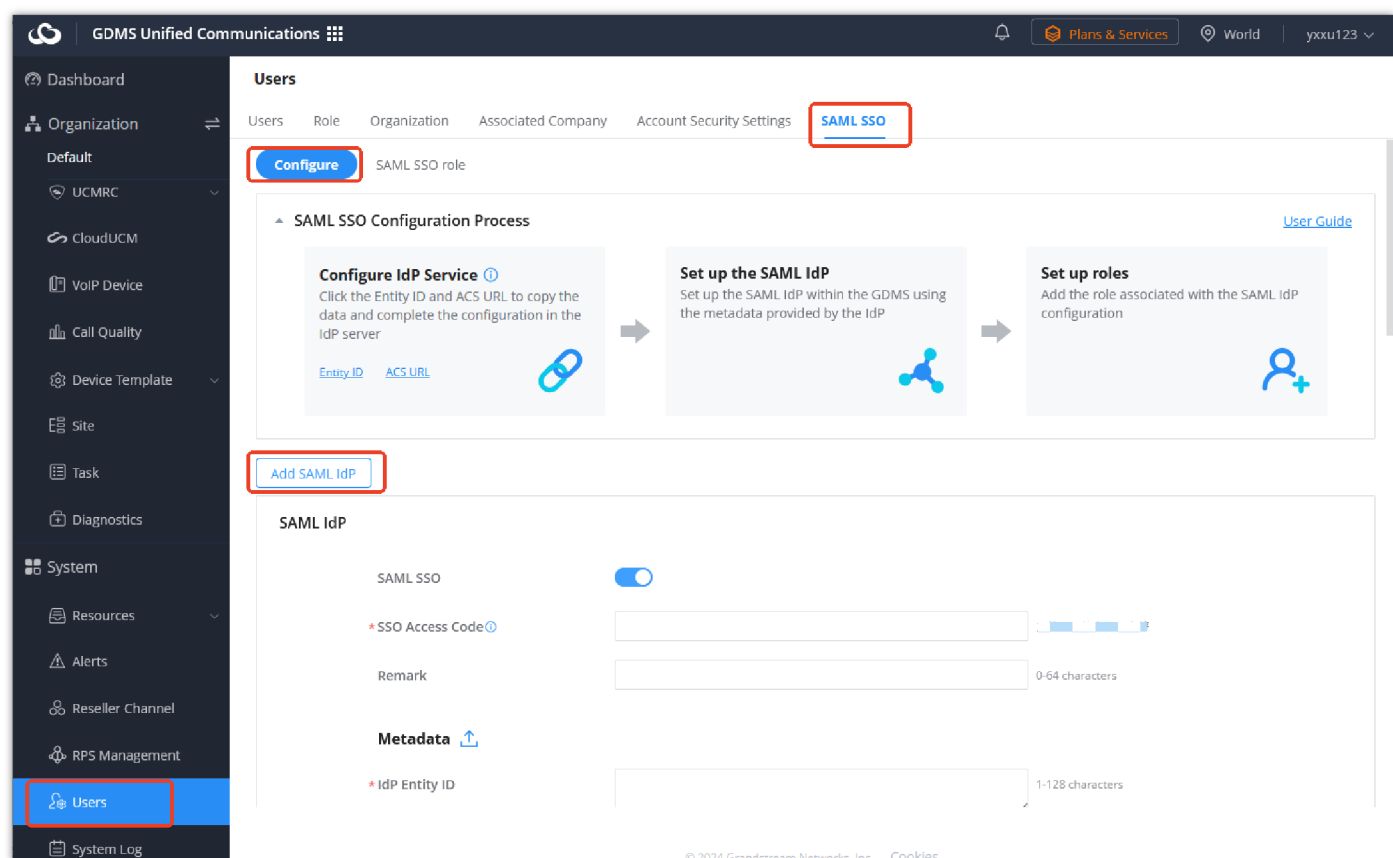
Downloading the SAML Metadata File

2. Log in to the GDMS or GWN Manager platform as a super administrator and navigate to **Users**→**SAML SSO**.

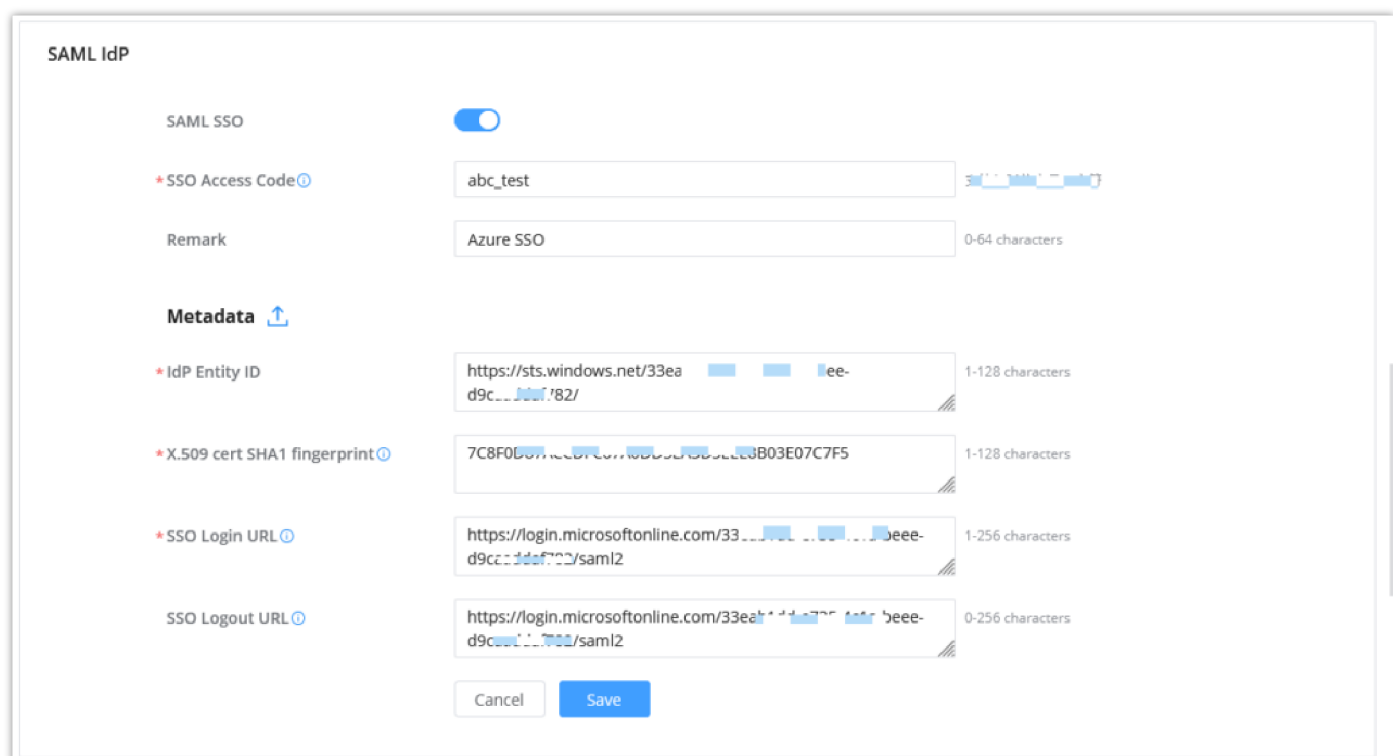
Note:

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

3. To configure the identity provider, click “Add SAML IdP” and fill in the information:



Adding SAML IdP in GDMS



SAML SSO	Enable or disable. If disabled, users will no longer be able to use the configured SSO authentication to log in.
SSO Access Code	Used to enter this SSO Access Code on the GDMS/GWN Manager login page, and can log in through this IdP service authentication.
Remarks	Enter your remarks.
Metadata	Upload the “Federation Metadata XML” file downloaded from Azure.

4. After adding the IdP, configure the SAML SSO role as described in section [[SAML SSO ROLES IN GDMS/GWN MANAGER](#)]. The Role Name must exactly match the role value sent by the IdP.

SAML SSO WITH ADFS

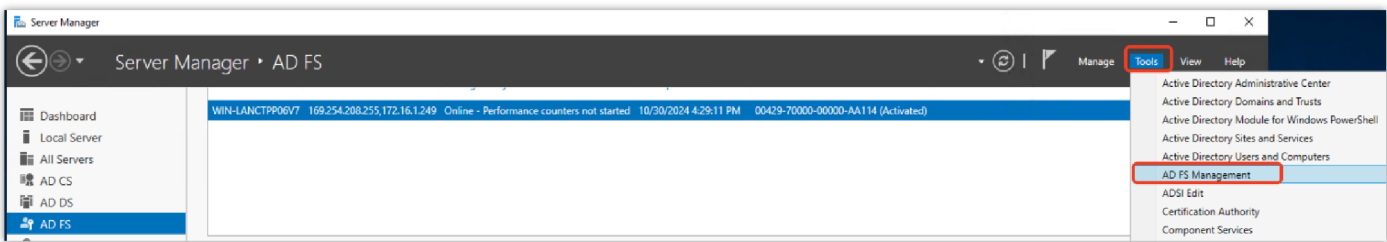
This section describes how to configure AD FS as the Identity Provider for GDMS Cloud and GWN Manager. For more configuration instructions on ADFS, refer to [Microsoft’s deployment guide](#).

Note:

The steps in this article only cover examples of necessary configurations. The exact implementation may vary depending on the environment, Active Directory implementation, and Windows Server updates. However, the **NameID**, **Email Address**, and **Role** attributes described below must be provided in the SAML assertion/token.

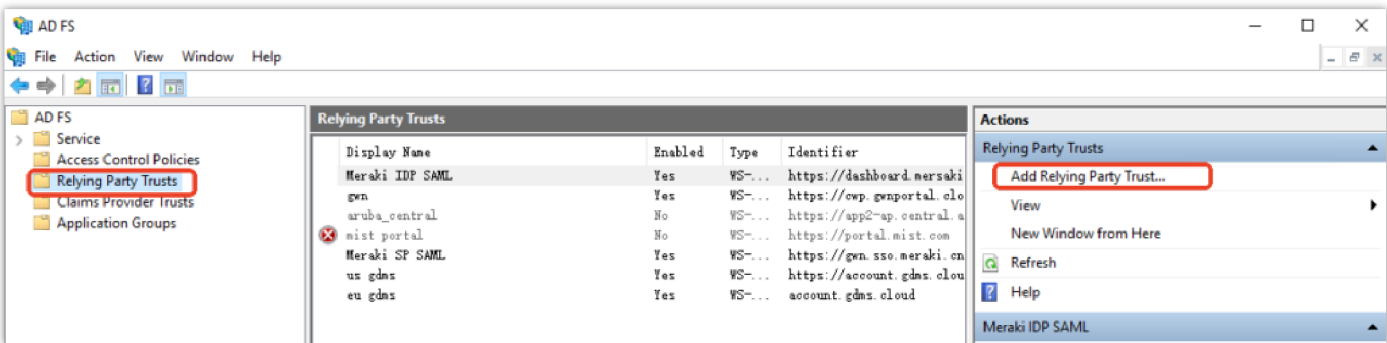
Step 1: Add Relying Party Trust in ADFS

1. Open the AD FS management console via **Server Manager**→**Tools**→**AD FS Management**.



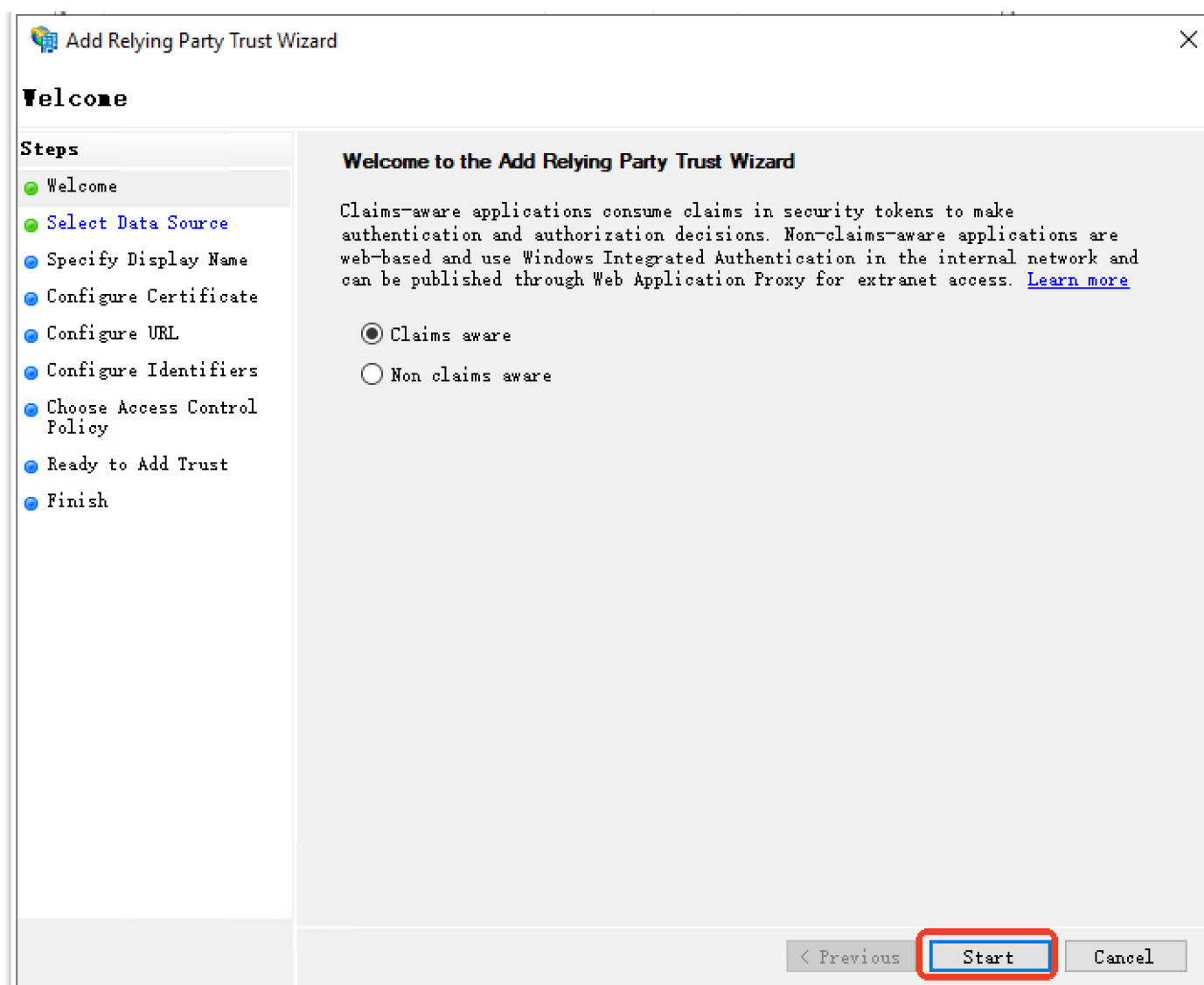
Active Directory FS Management

2. Click on the top-level folder (**AD FS**) and click **Add Relying Party Trust** from the **Actions** menu.



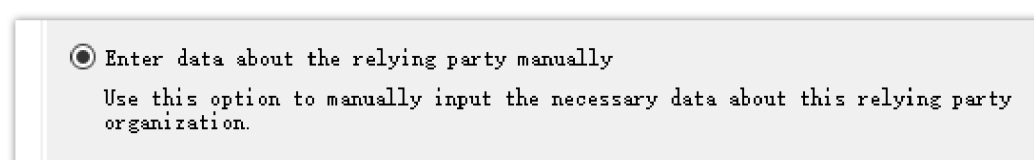
Add Relying Party Trust

3. Click **Start** to launch the wizard.



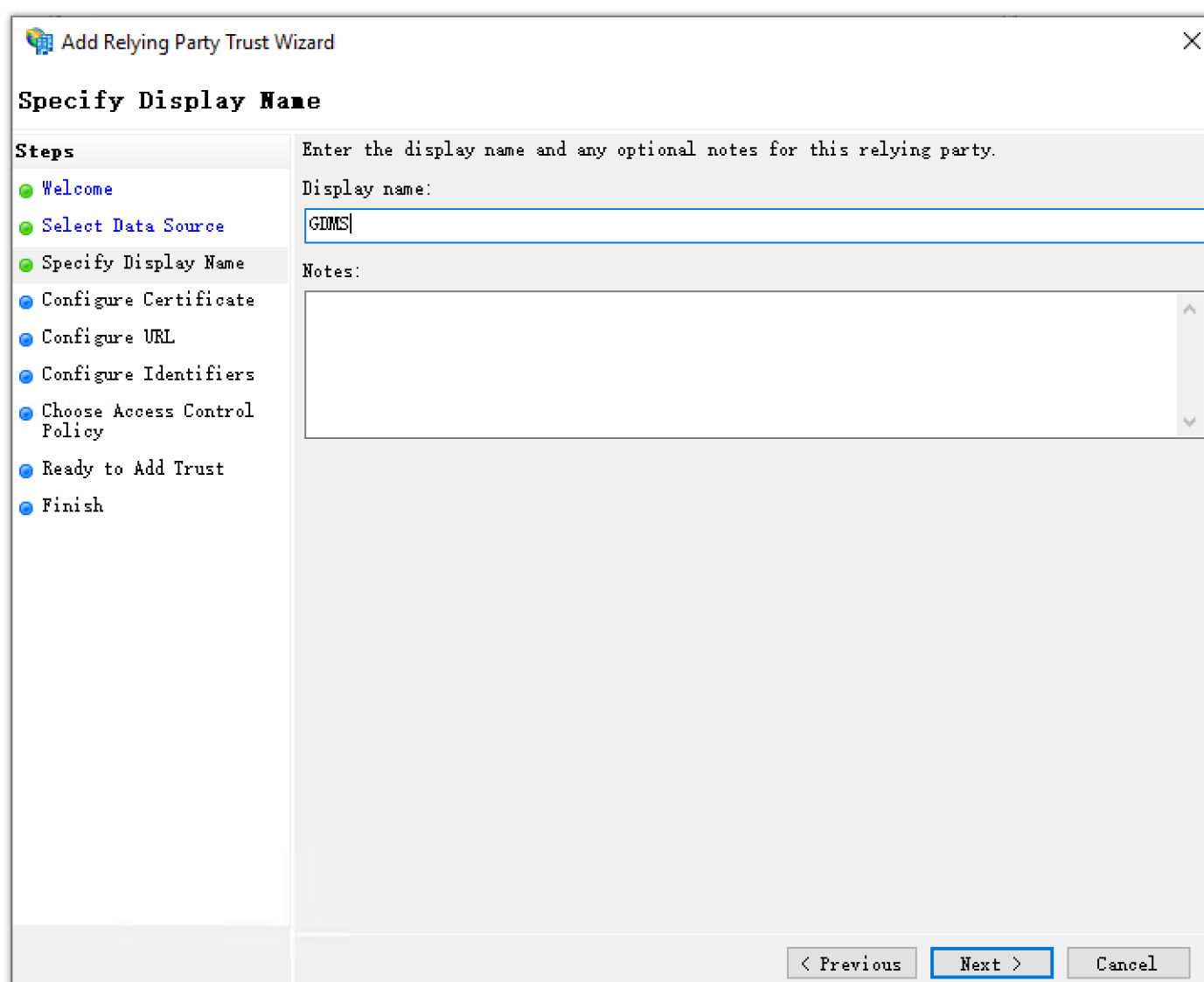
Add Relying Party Trust Wizard

4. Choose to **Enter data about the relying party manually**. Then click **Next**.



Selecting Data Source

5. Enter a **Display name**, such as "GDMS" or "GWN Manager", which will be displayed in the management console and to users connecting to GDMS. Then click **Next**.



Choosing a Display Name

6. Click **Next** to skip the step of **Configure Certificate**.

7. Enable **Support for the SAML 2.0 WebSSO protocol**.

☒ Enable support for the SAML 2.0 WebSSO protocol

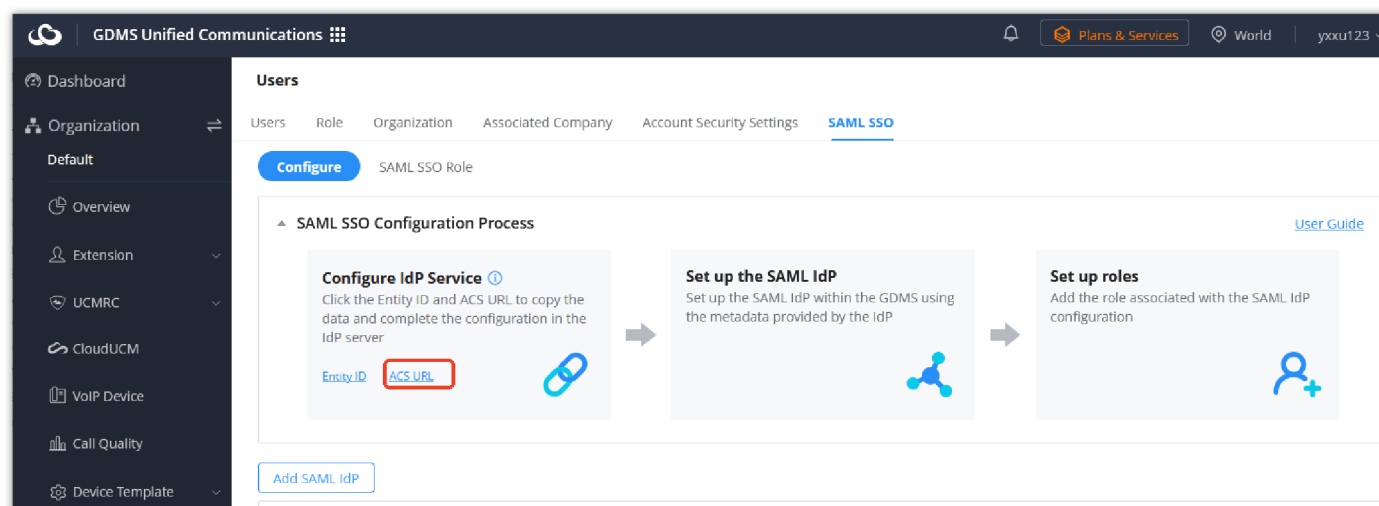
The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: https://www.contoso.com/adfs/lz/

Replying party SAML 20 SSO

8. Enter the **Relying Party SAML 2.0 SSO service URL** (ACS URL), which can be copied from:
 - o **GDMS: Users→SAML SSO**
 - o **GWN Manager: Organization→Users→SAML SSO**

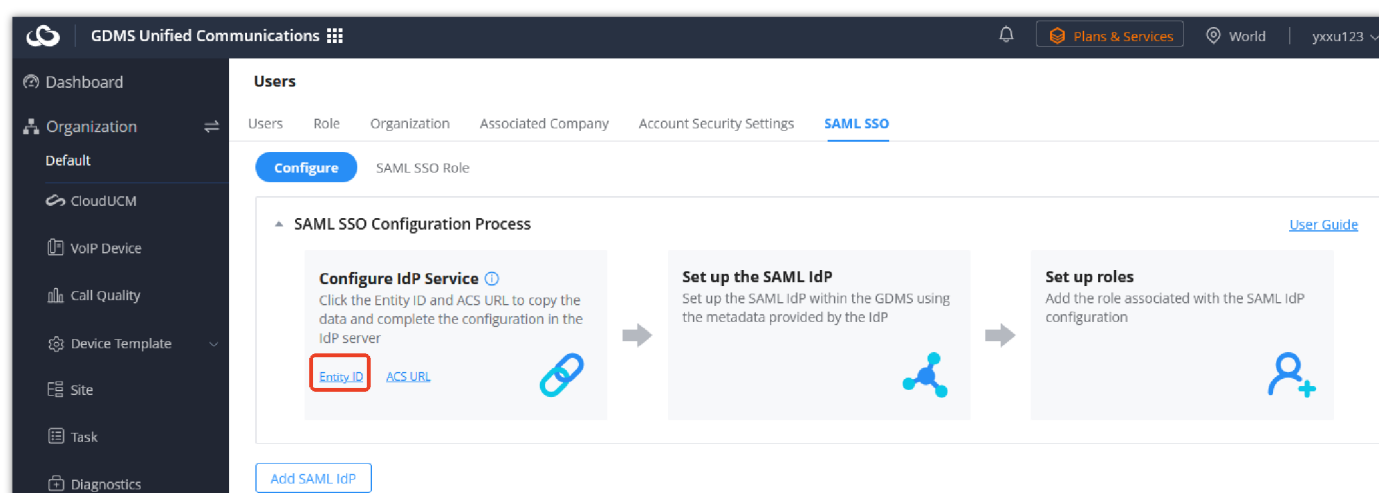


ACS URL GDMS SAML SSO

9. For the **Relying party trust identifier**, fill in the **Entity ID** displayed on the corresponding **SAML SSO** (as shown in the figure, click one-click copy). Then click **Add** and **Next**.

Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust



Relying Party Trust Identifier

10. Select the default issuance authorization rule based on your preferred security behavior. For this example, select **Permit everyone**. Then click **Next**.

Add Relying Party Trust Wizard

Choose Access Control Policy

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy**
- Ready to Add Trust
- Finish

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users of the relying party.
Permit everyone and require MFA from unauthenticated access	Grant access to everyone and require MFA from unauthenticated access.
Permit everyone and require MFA, allow automatic logon	Grant access to everyone and require MFA, allow automatic logon.
Permit everyone for intranet access	Grant access to the intranet users of the relying party.
Permit specific group	Grant access to users of one or more groups.

Policy

Permit everyone

☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

< Previous Next > Cancel

Choosing Access Control Policy

11. Review your settings and complete the wizard.

Add Relying Party Trust Wizard

Ready to Add Trust

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust**
- Finish

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring Identifiers Encryption Signature Accepted Claims Organization

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

☐ Monitor relying party

☐ Automatically update relying party

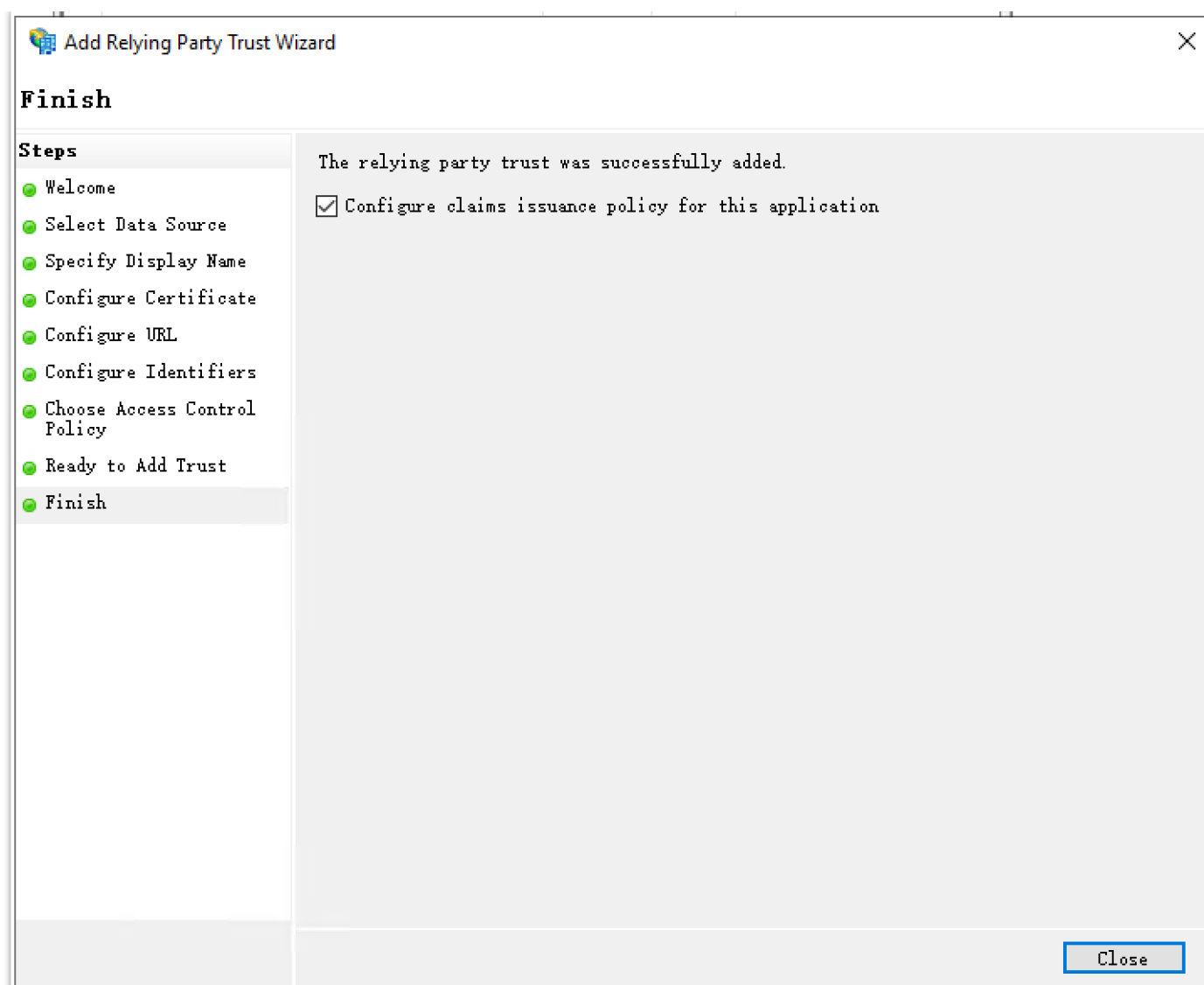
This relying party's federation metadata data was last checked on:
< never >

This relying party was last updated from federation metadata on:
< never >

< Previous **Next >** Cancel

Reviewing Settings

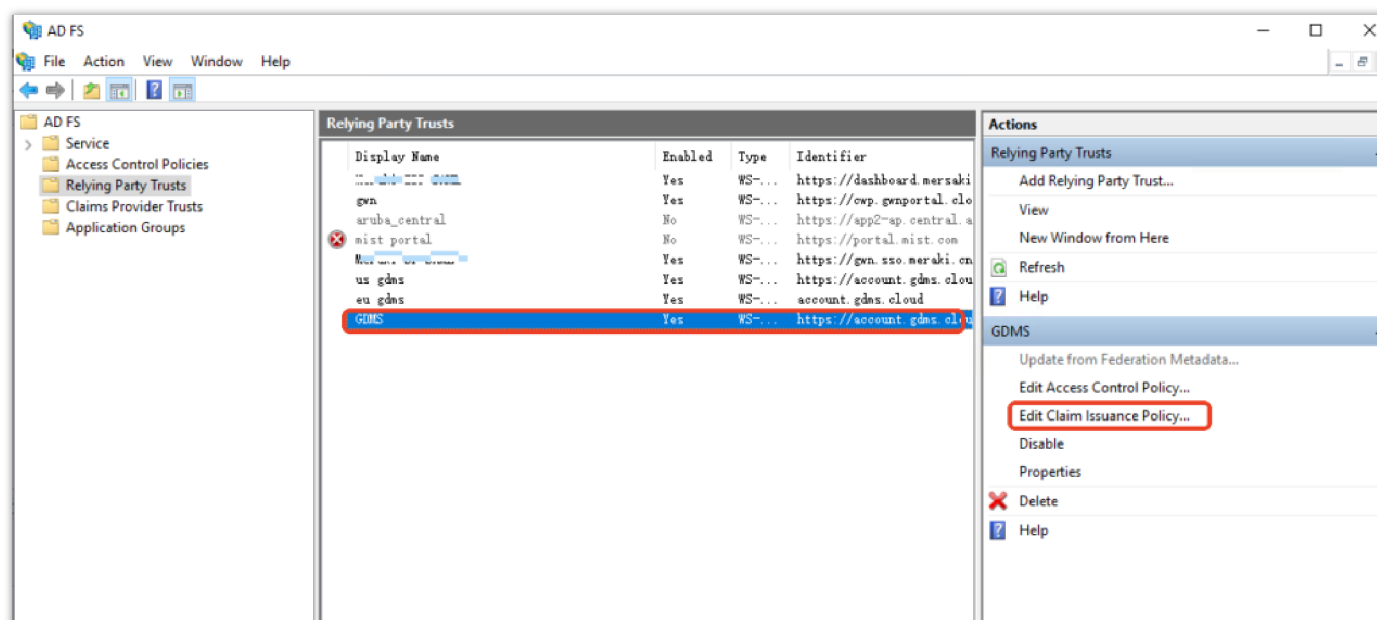
12. Ensure **Configure claim issuance policy for this application** is checked.



Relying Party Trust Added

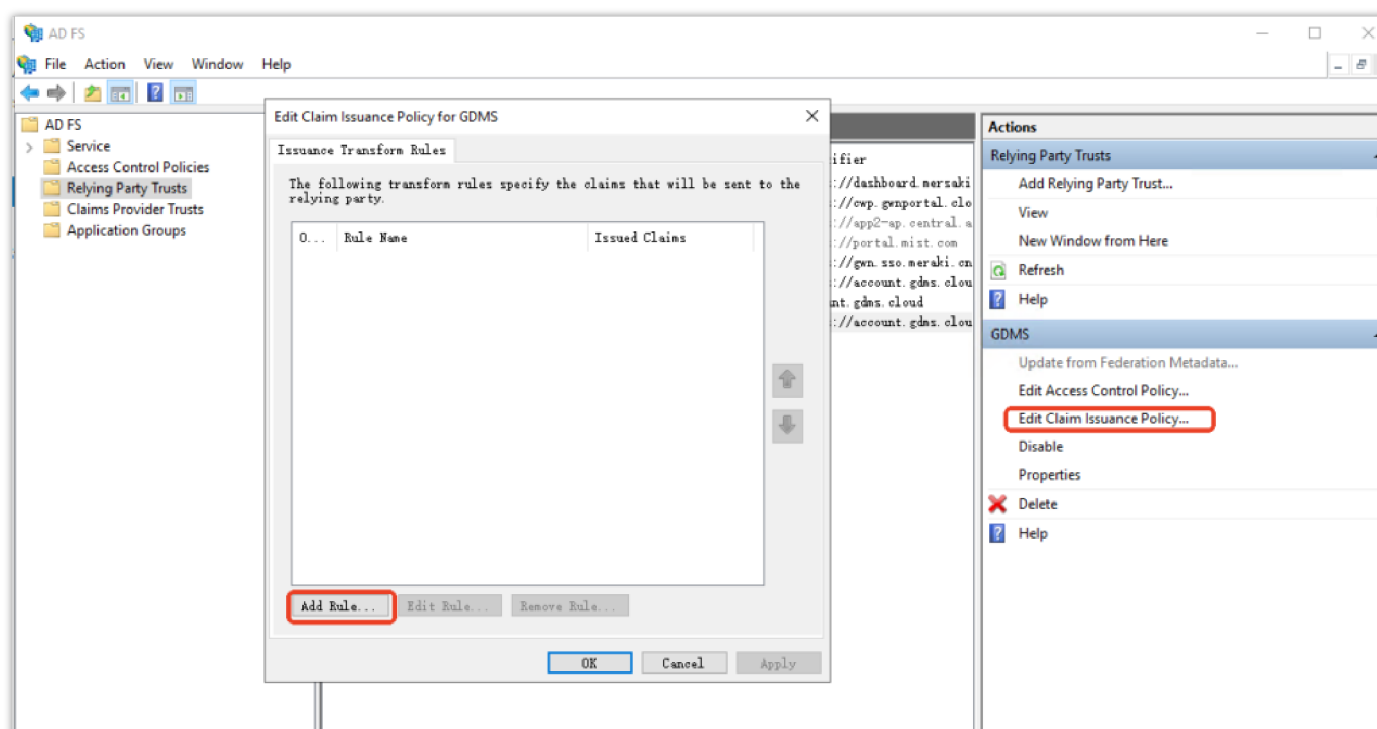
Step 2: Set NameID Attribute in ADFS

1. Select the **Relying Party Trusts** you created and click **"Edit Claim Issuance Policy"** on the right.



Edit Claim Issuance Policy

2. In the **Edit Claim Rules** dialog, click **Add Rule**.



3. For the **Claim rule template**, choose to **Transform an Incoming Claim**. Then click Next.

Claim rule template:

Transform an Incoming Claim

4. Fill in the Claim rule name, Incoming claim type, Outgoing name ID Format, and select **Pass Through all claim values** as shown in the following screenshot. Then click **Finish**.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: NameID

Rule template: Transform an Incoming Claim

Incoming claim type: Windows account name

Incoming name ID format: Persistent Identifier

Outgoing claim type: Name ID

Outgoing name ID format: Persistent Identifier

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

< Previous Finish Cancel

Configuring Claim Rule

Step 3: Set Email Address Attribute in ADFS

1. Select the **Relying Party Trusts** you created and click **"Edit Claim Issuance Policy"** on the right.

AD FS

File Action View Window Help

AD FS

- Service
- Access Control Policies
- Relying Party Trusts
- Claims Provider Trusts
- Application Groups

Relying Party Trusts

Display Name	Enabled	Type	Identifier
...	Yes	WS-...	https://dashboard.meraki...
gwn	Yes	WS-...	https://owp.gwnportal.clo...
aruba_central	No	WS-...	https://app2-ap.central.a...
mist portal	No	WS-...	https://portal.mist.com
Mu...	Yes	WS-...	https://gwn.sso.meraki.cn...
us gds	Yes	WS-...	https://account.gds.clou...
eu gds	Yes	WS-...	account.gds.cloud
GDMS	Yes	WS-...	https://account.gds.cl...

Actions

Relying Party Trusts

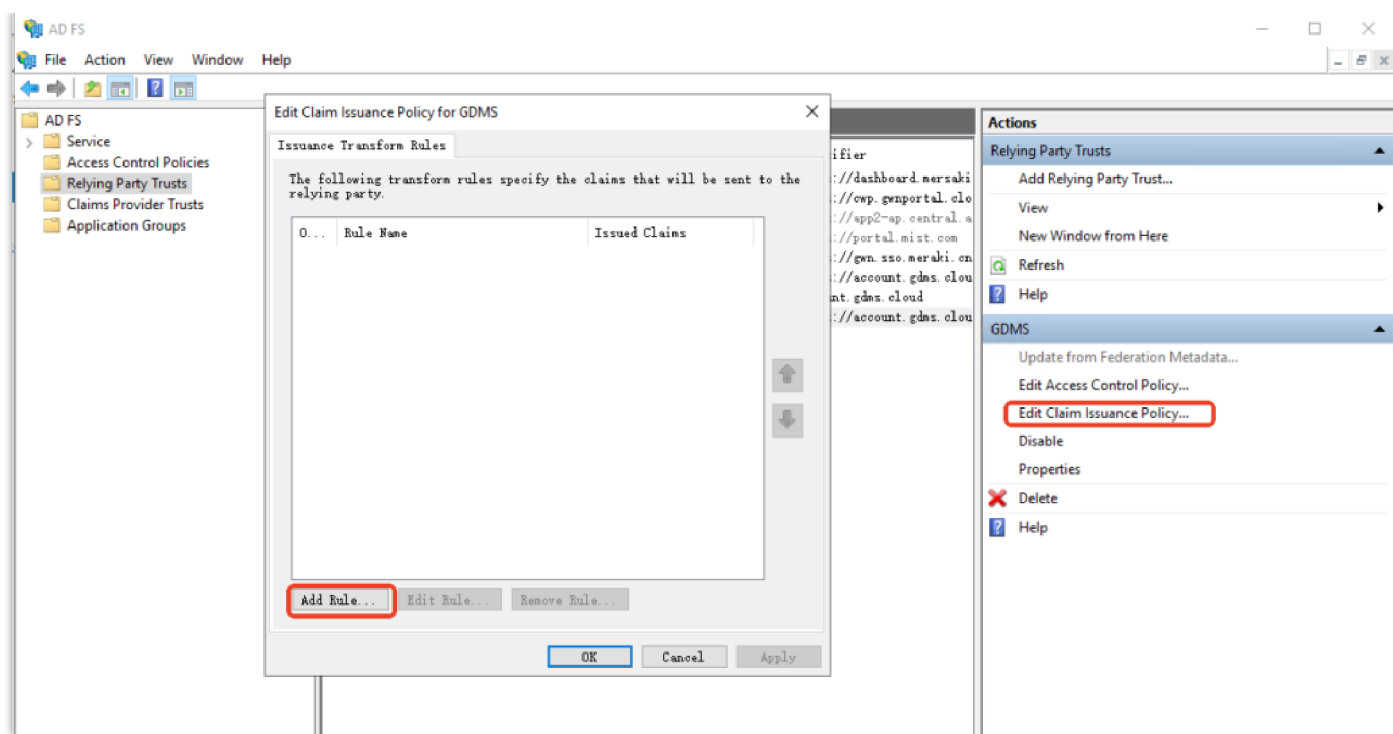
- Add Relying Party Trust...
- View
- New Window from Here
- Refresh
- Help

GDMS

- Update from Federation Metadata...
- Edit Access Control Policy...
- Edit Claim Issuance Policy...
- Disable
- Properties
- Delete
- Help

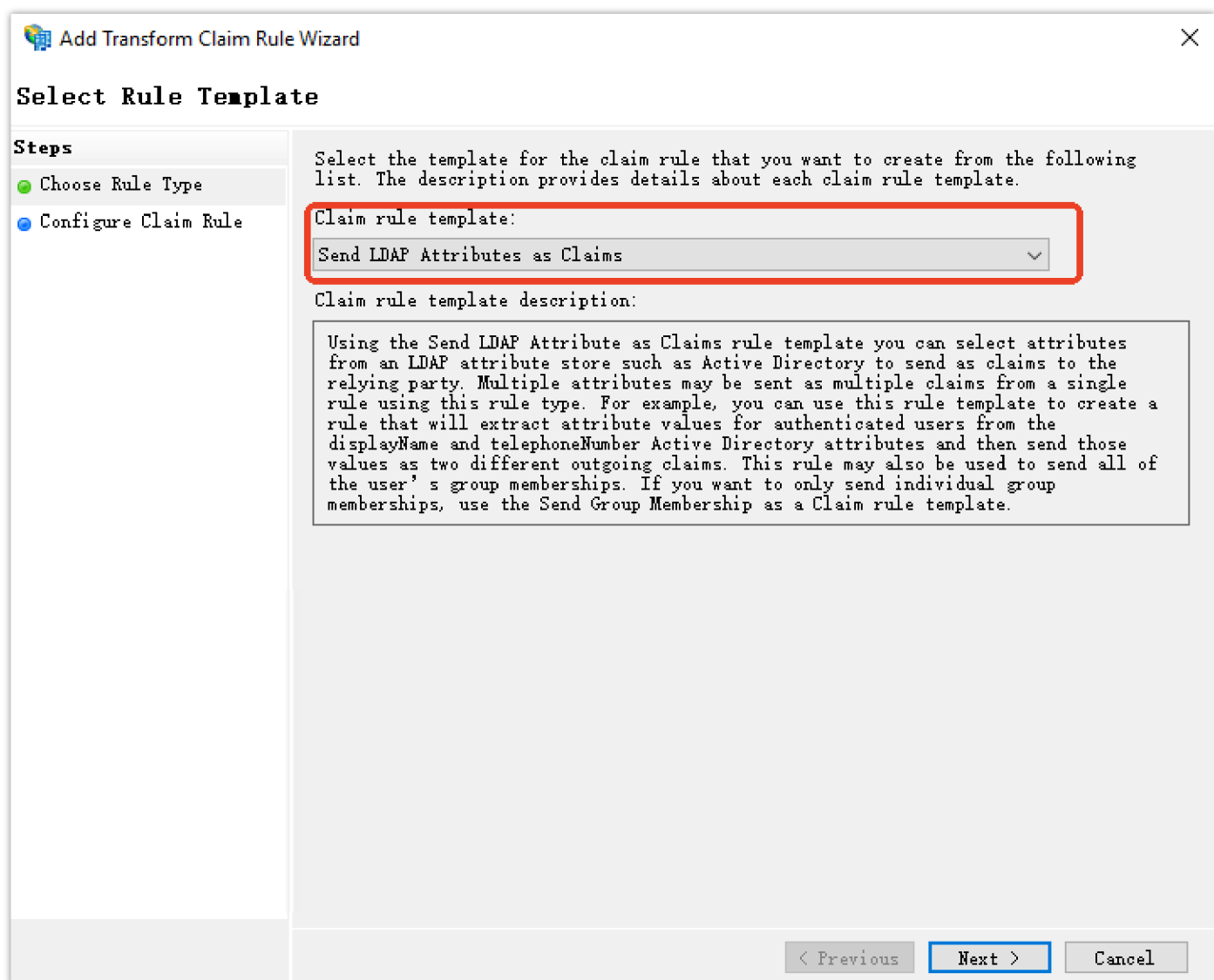
Edit Claim Issuance Policy

2. In the **Edit Claim Rules** dialog, click **Add Rule**.



Add Rule

3. For the **Claim rule template**, choose to **Send LDAP Attributes as Claims**. Then click **Next**.



Claim Rule Template Send LDAP Attributes as Claims

4. Fill in the following information and click **Finish**.

Claim Rule Name	Enter a name, such as “emailaddress”.
Attribute Store	Select Active Directory
LDAP Attribute	Select User-Principal-Name
Outgoing Claim Type	Enter the following based on the service provider: ○ GDMS: https://account.gdms.cloud/saml/attribute/emailaddress ○ GWN Manager: <a href="https://<gwn-manager-host>[:port]/user/saml/attribute/emailaddress">https://<gwn-manager-host>[:port]/user/saml/attribute/emailaddress Note: If GWN Manager is not bound to port 443, the port number must be included in the URI.

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
emailaddress

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

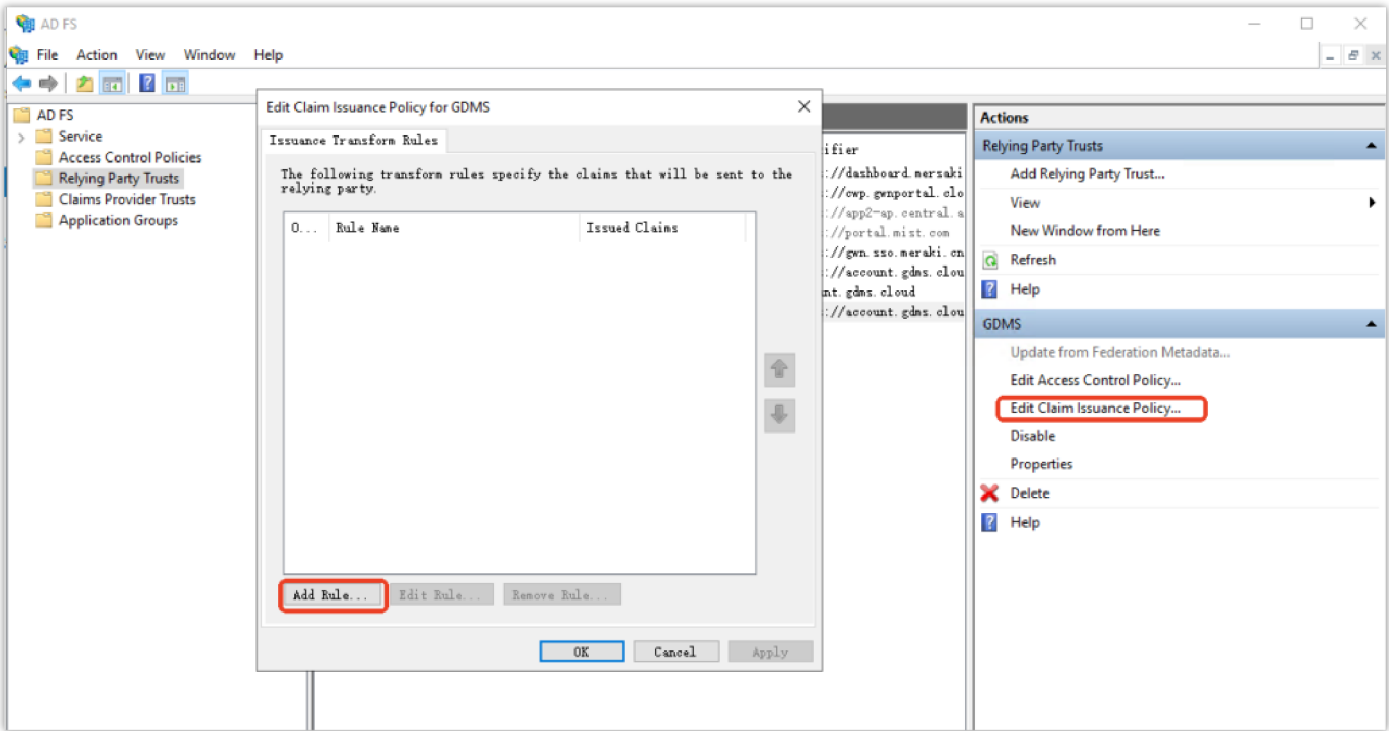
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	tps://account.gdms.cloud/saml/attribute/emailaddress
*		

Mapping of LDAP Attributes

Step 4: Set Role Attribute in ADFS

1. In the **Edit Claim Rules** dialog, click **Add Rule**.



Add Rule

2. For the **Claim rule template**, choose to **Send Group Membership as a Claim**.

Claim rule template:
Send Group Membership as a Claim

3. Fill in the following information and click **Finish**.

Claim Rule Name	Enter a name, such as “role”.
User’s Group	Select the AD user group that will use this Relying Party Trust.
Outgoing Claim Type	Enter the following based on the service provider: - GDMS: https://account.gdms.cloud/saml/attribute/role - GWN Manager: <a href="https://<gwn-manager-host>[:port]/user/saml/attribute/role">https://<gwn-manager-host>[:port]/user/saml/attribute/role Note: If GWN Manager is not bound to port 443, the port number must be included in the URI.
Outgoing Claim Value	The value of the role must be the same as the SAML SSO role name configured on GDMS or GWN Manager, such as “Admin.A”.

You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue.

Claim rule name:

Rule template: Send Group Membership as a Claim

User's group:

Outgoing claim type:

Outgoing name ID format:

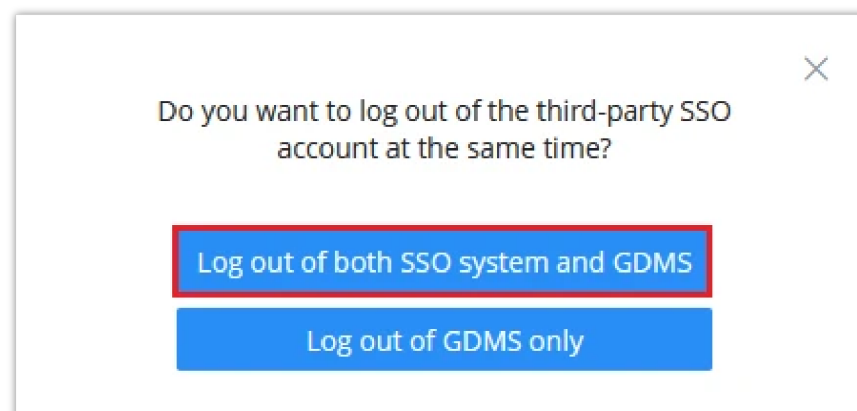
Outgoing claim value:

Claim Rule Template Send Group Membership a Claim

Step 5: Configure Single Logout (Optional)

This step describes how to configure SAML Single Logout for GDMS Cloud and GWN Manager when using AD FS as the Identity Provider.

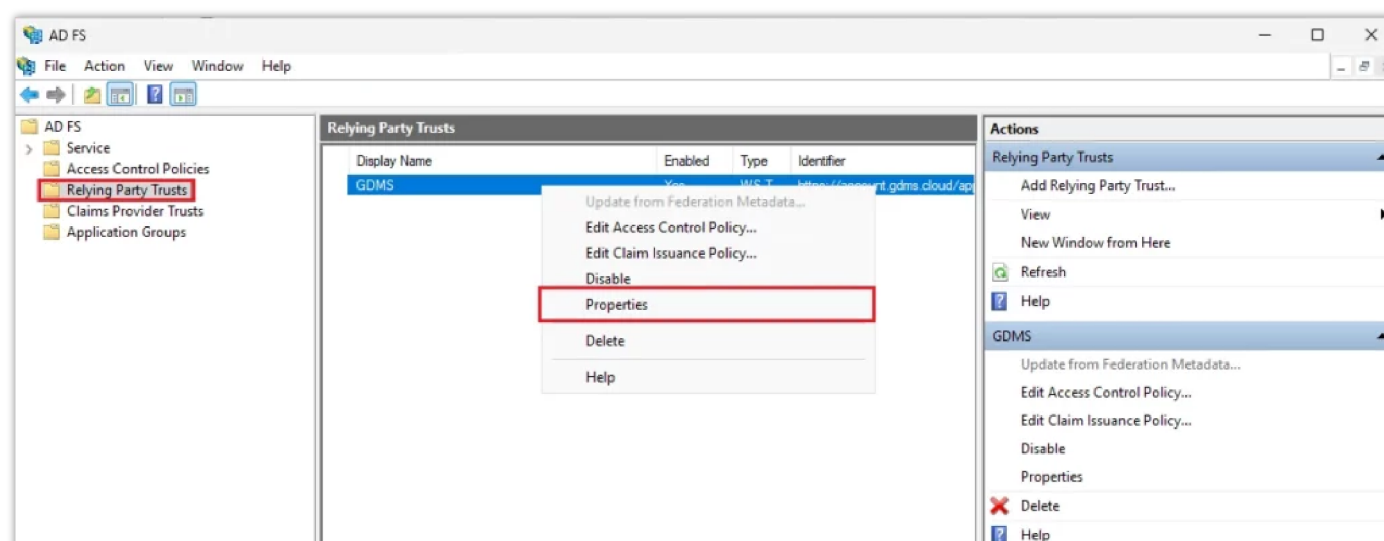
If SAML Single Logout is not configured correctly, users will encounter errors when selecting “Logout from both application and SSO system”.



GDMS Logout Prompt

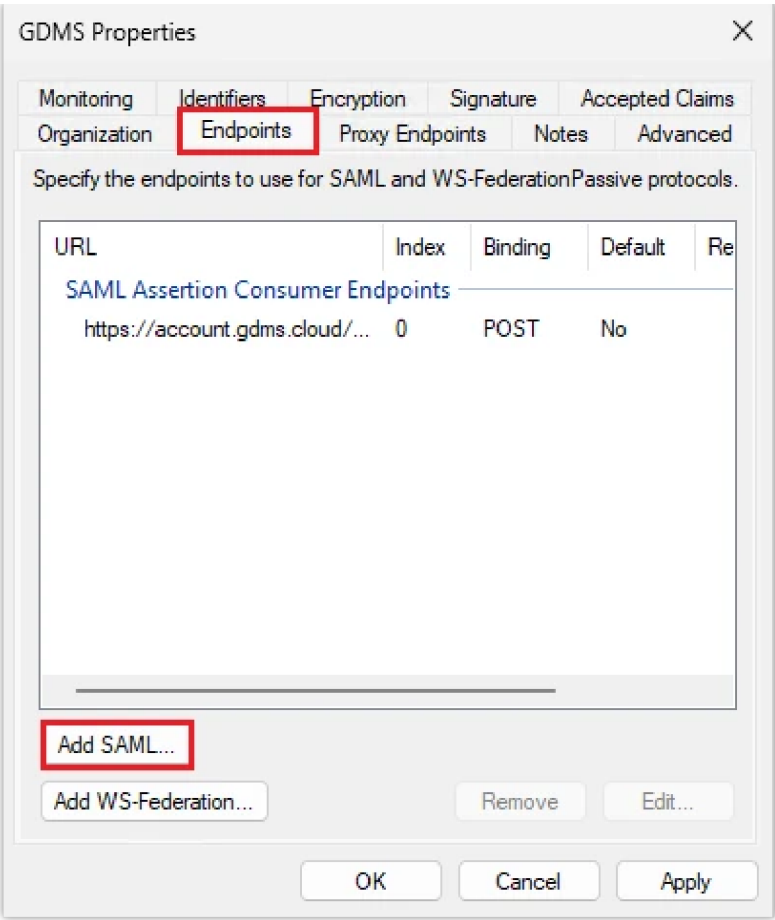
The following AD FS configuration is required for both GDMS and GWN Manager:

1. Open **AD FS Management**.
2. Navigate to **Relying Party Trusts** and right-click the relevant Relying Party Trust (GDMS or GWN Manager) and select **Properties**.



Relying Party Trusts Properties

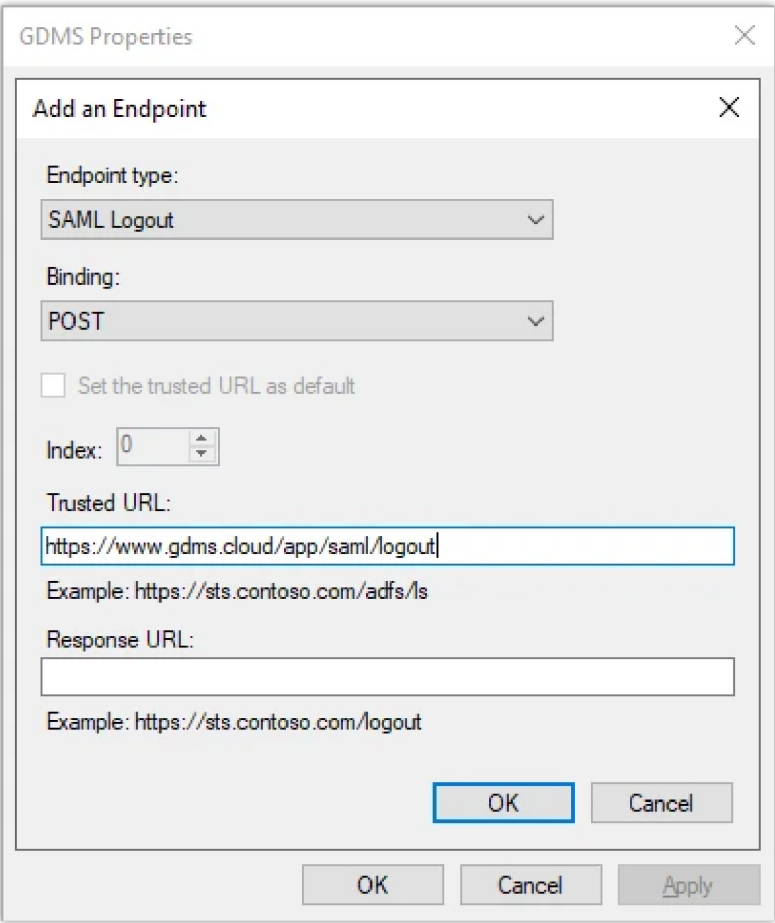
3. Open the **Endpoints** tab and click **Add SAML**.



Relying Party Trusts Endpoints Tab

4. Configure the endpoint as follows:

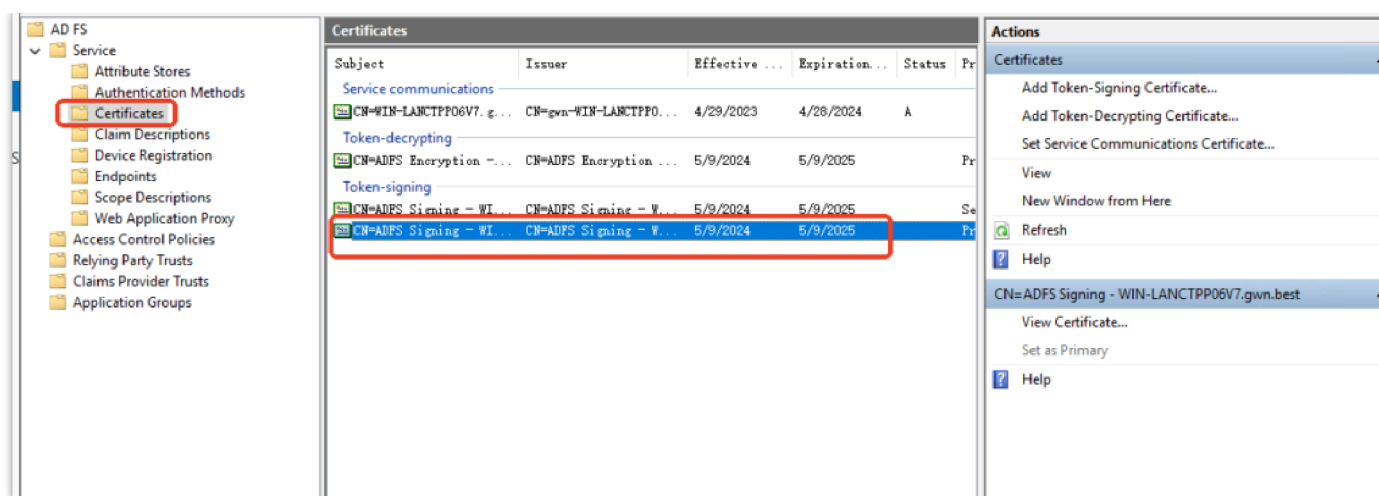
Field	Value
Endpoint Type	SAML Logout
Binding	POST
Trusted URL	• GDMS: https://www.gdms.cloud/app/saml/logout • GWN Manager: <a href="https://<gwn-manager-host>[:port]/user/app/saml/logout">https://<gwn-manager-host>[:port]/user/app/saml/logout



Trusted URL Configuration

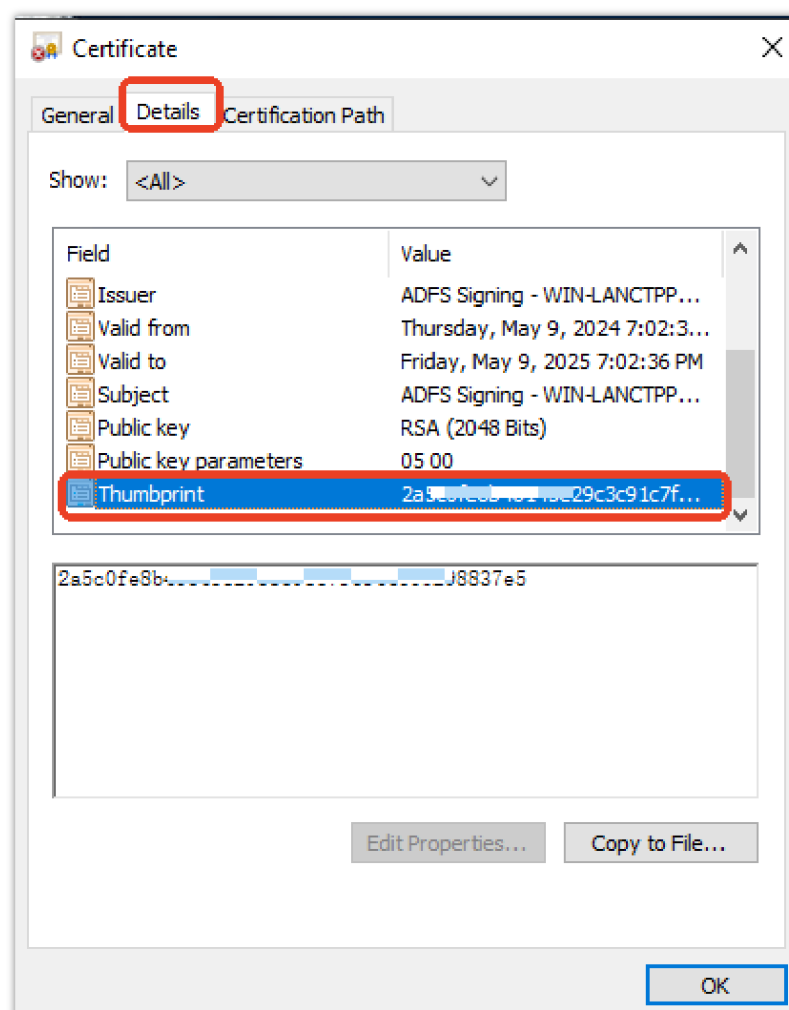
Step 6: Configure Token-Signing Certificate

- 1. In the management console, go to **AD FS**→**Service**→**Certificates**. Select a valid certificate under Token-signing.



Certificates Page

2. Double-click on the certificate under **Token-signing**. Under **Details**→**Thumbprint**, copy this string and paste it into the **X.509 cert SHA1 fingerprint** field in GDMS/GWN Manager.



Certificate Details

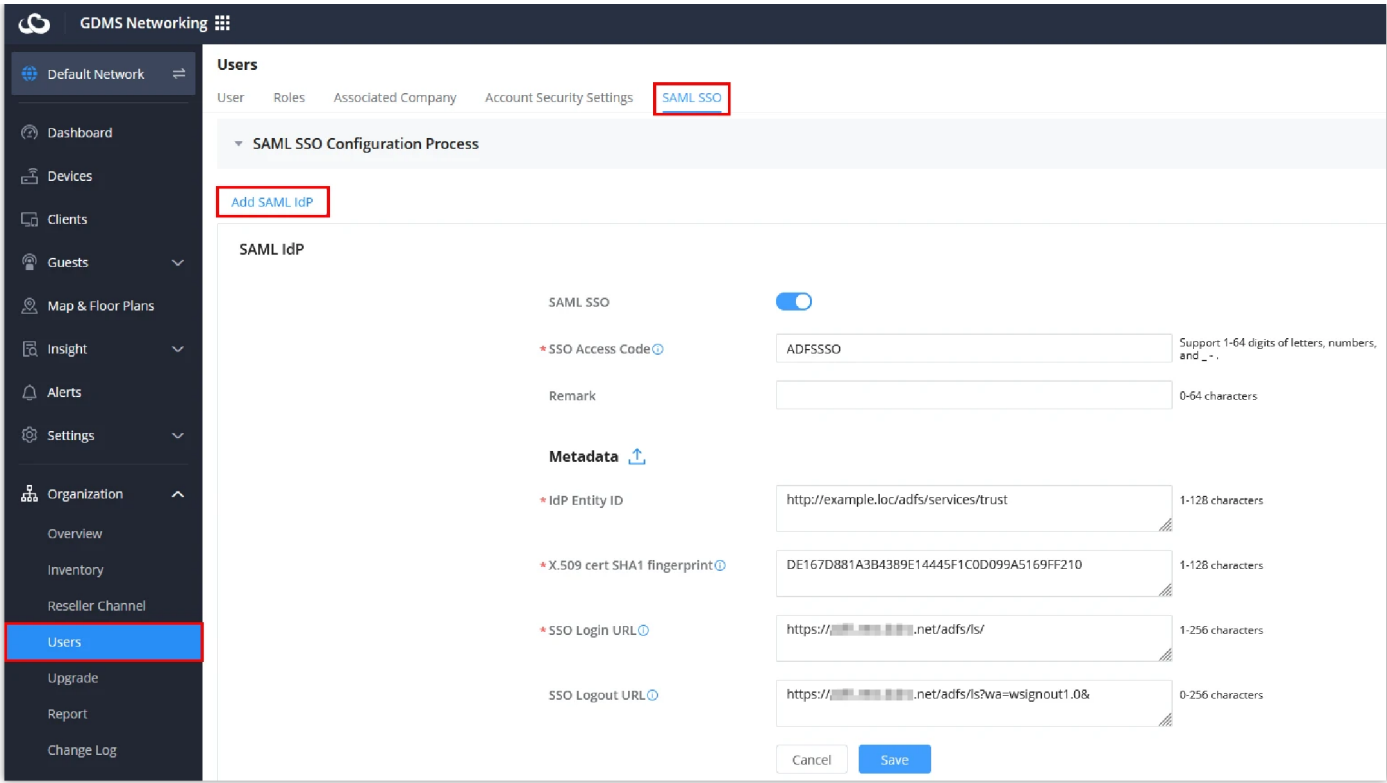
Step 7: SAML SSO in GDMS/GWN Manager

1. The super administrator logs in to the GDMS platform and goes to **Users**→**SAML SSO**.
2. Click **Add SAML IdP** and fill in the information:

Note:

Since both GDMS and GWN Manager support metadata import, administrators can upload the downloaded XML file to automatically populate the IdP configuration fields. To download the metadata, open a browser and go to: <https://<adfs-domain>/FederationMetadata/2007-06/FederationMetadata.xml>

Replace **<adfs-domain>** with the fully qualified domain name of the AD FS server.



GDMS SAML IdP Configuration Page

SAML SSO	Enable or disable. If disabled, users will no longer be able to use the configured SSO authentication to log in.
SSO Access Code	Used to enter this SSO Access Code on the GDMS/GWN Manager login page, and can log in through this IdP service authentication.
Remarks	Enter your remarks.
IdP Entity ID	Must exactly match the ADFS Federation Service Identifier, as advertised in ADFS metadata. By default, ADFS uses: <i>http://<FederationServiceName>/adfs/services/trust</i> <i>Note: This value is a logical identifier and does not need to be publicly reachable. It is recommended to Import ADFS metadata instead of manually entering this value.</i>
X.509 cert SHA1 fingerprint	Fill in the Thumbprint value under the Details of the certificate in ADFS→Certificates→Token-singing
SSO Login URL	URL address for login authentication, fill in: <i>https://<ADFS_server>/adfs/ls/</i> Replace “<ADFS_server>” with the IP address or DNS name of your AD FS server.
SSO Logout URL	When logging out of GDMS/GWN Manager, you can log out of the ADFS redirection address at the same time. Fill in the following information based on the platform: - GDMS: <i>https://<ADFS_server>/adfs/ls?wa=wsignout1.0&</i> - GWN Manager: <i>https://<ADFS_server>/adfs/ls?wa=wsignout1.0&</i> Replace “<ADFS_server>” with the IP address or DNS name of your AD FS server.

3. After adding the IdP, configure the SAML SSO role as described in section [SAML SSO ROLES IN GDMS/GWN MANAGER]. The Role Name must exactly match the role value sent by the IdP.

SAML SSO WITH DUO

Users will have to set up a DUO account first by using this link: <https://signup.duo.com/>

This section describes how to configure DUO SSO as a SAML Identity Provider for GDMS or GWN Manager.

Duo Single Sign-On is a cloud-hosted **SAML 2.0 Identity Provider (IdP)** and **OpenID Connect Provider (OP)** that enables centralized authentication with multi-factor authentication (MFA) and access policy enforcement. Duo can integrate with upstream identity providers such as **Microsoft Entra ID**, allowing organizations to combine enterprise identity management with Duo MFA.

For details, please refer to the DUO manual: <https://duo.com/docs/sso>

The screenshots in this section use GWN Manager as the Service Provider (SP). The configuration steps for GDMS are identical except for the SAML attribute URLs used in the Duo application configuration.

Prerequisite (GWN Manager Only)

When using Duo SAML SSO with GWN Manager, the system clock on the GWN Manager host must be synchronized. If the system time is not synchronized, SAML assertion validation may fail, resulting in erros during login.

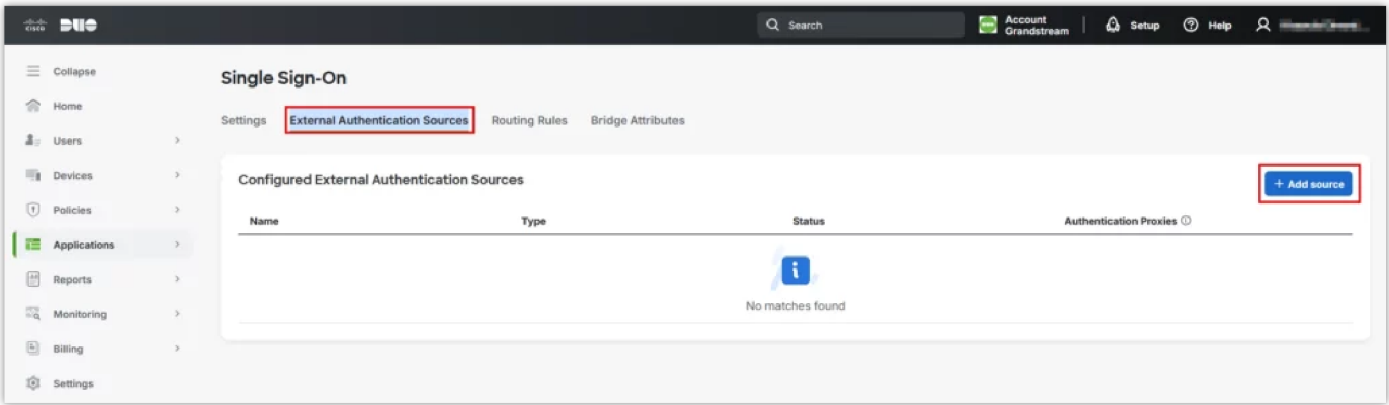
On the GWN Manager host, run the following commands to enable NTP and verify that the system clock is synchronized:

```
# sudo timedatectl set-ntp on
# timedatectl | grep "System clock synchronized"
```

If the configuration is correct, the output should show: *System clock synchronized: yes*

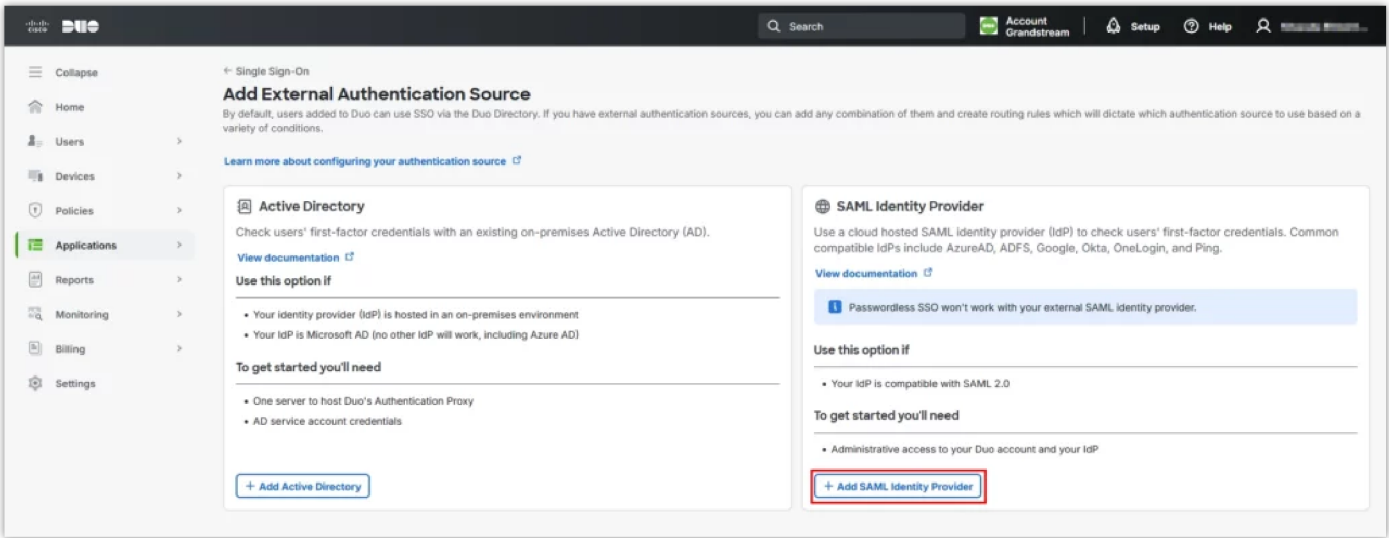
Step 1: Create a DUO Authentication Source

- 1. Log in to the [Duo Admin Panel](#) and navigate to **Applications→SSO Settings**.
- 2. Click **Add source** in the **External Authentication Sources** tab.



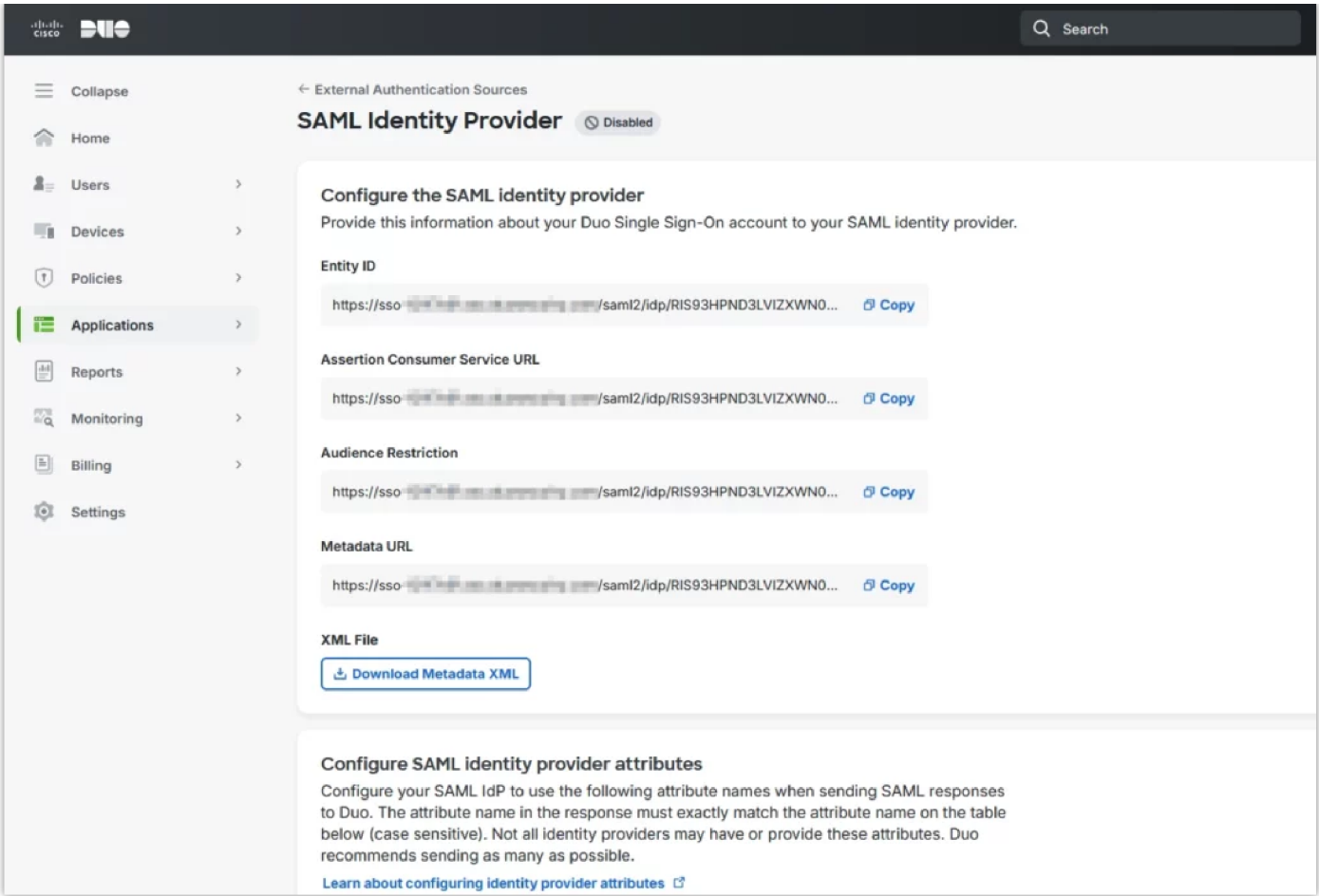
Add DUO External Authentication Source

- 3. Click **Add SAML Identity Provider**.



Add SAML Identity Provider

- 4. This page contains the values that will be used when configuring the upstream identity provider (for example, Microsoft Entra ID).



DUO SAML Identity Provider Configuration

Step 2: Configure the Azure Application

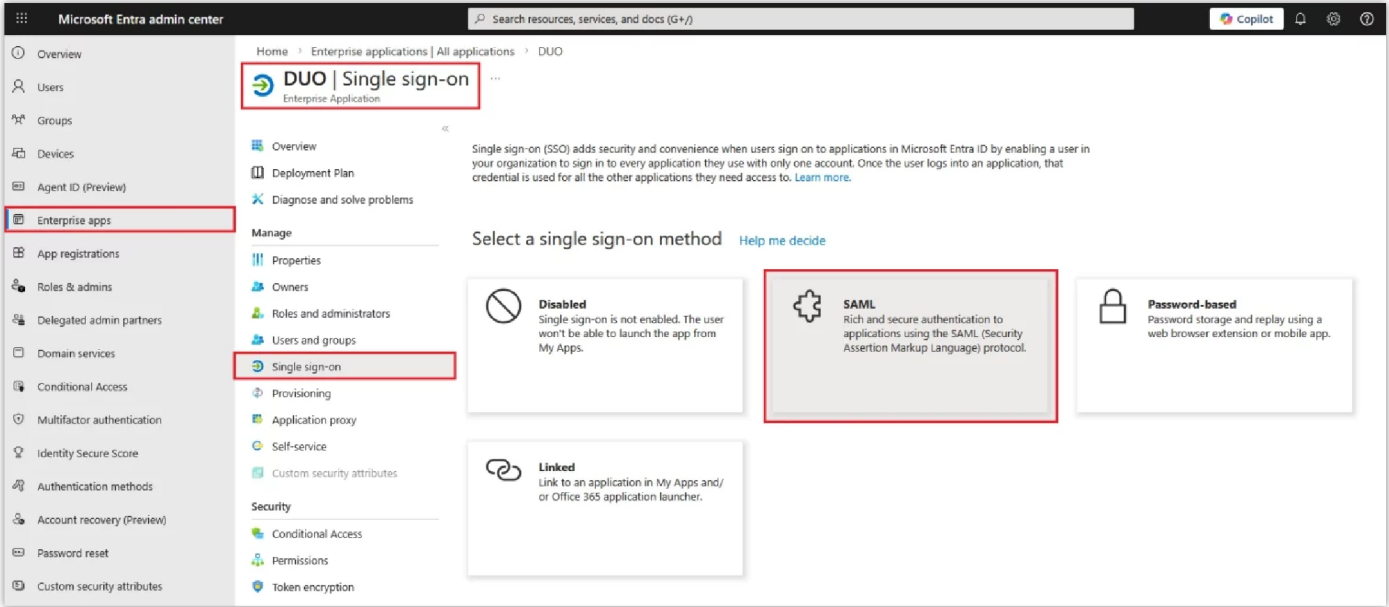
In this deployment model, Entra ID authenticates the user and sends the identity assertion to Duo, which then acts as the IdP for GDMS/GWN Manager.

Please refer to the [first section](#) of the guide for more information on configuring an App on Entra ID.

- 1. Add a new application in Azure.
- 2. Add users to the application in Azure.

Note:
The Azure user’s email address must be the same as the DUO user’s email address.

- 3. Go to **Identity**→**Applications**→**Enterprise applications**, find and click the DUO application you created in the application list.
- 4. Click **Single Sign-on** on the left and click **SAML** on the page.



SSO Page for DUO Entra App

- 5. Within the **Basic SAML Configuration** section, click **Edit**, and configure the following values using the information obtained from Duo.

Identifier (Entity ID)	Duo Entity ID
------------------------	---------------

2

Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
name	user.userprincipalname
emailaddress	user.mail
Email	user.userprincipalname
Unique User Identifier	user.userprincipalname

Manage claim

Save Discard changes Got feedback?

Name *

Email

Namespace

Enter a namespace URI

Choose name format

Source *

Attribute Transformation Directory schema extension

Source attribute *

user.userprincipalname

Claim conditions

Advanced SAML claims options

7. From the **SAML Signing Certificate** section, download the **Federation Metadata XML** or copy the following values:
- Login URL
 - Microsoft Entra Identifier
 - Logout URL
 - Certificate (Base64)

DUO | SAML-based Sign-on

Enterprise Application

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

Upload metadata file

Change single sign-on mode

Test this application

Got feedback?

3

SAML Certificates

Token signing certificate

Active

419C81BA065DACD7A

1/22/2029, 3:32:08 PM

onmicrosoft.com

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

Certificate (Base64)

Download

Verification certificates (optional)

No

0

0

4

Set up DUO

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

Login URL

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

Microsoft Entra Identifier

https://sts.windows.net/f6e24392-14ba-4383-943-...

Logout URL

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

Copying Entra ID URLs and Downloading SAML Certificate

Step 3: Configure Single Sign-On in DUO

1. Log in to the [Duo Admin Panel](#) and navigate to **Single Sign-On**.

Collapse

Home

Users

Devices

Applications

Reports

Monitoring

Billing

Settings

Single Sign-On

Settings External Authentication Sources Routing Rules Bridge Attributes

Configured External Authentication Sources

Using external authentication sources? Routing Rules can support a dynamic SSO environment by dictating which auth sources to use based on a variety of conditions.

Name	Type	Status	Auth
SAML Identity Provider	SAML IdP	Enabled	—

DUO External Authentication Sources Page

2. Select the resource you created in Step 1 (*SAML Identity Provider*).

3. Enter the information copied from Entra ID:

IdP Entity ID	Microsoft Entra Identifier
Single Sign-On URL	Entra Login URL
Single logout URL	Entra Logout URL
Certificate	Upload Entra app Base64 certificate

Configure Duo Single Sign-On

Get this information from your SAML identity provider so Duo Single Sign-On can use it for primary authentication.

Display name *

SAML Identity Provider

Used only to help you identify the identity provider within our interface.

Entity ID *

https://sts.windows.net/f6e24392-14ba-4383-943[REDACTED]

1

The global, unique ID for your SAML entity. This is provided by your identity provider.

Single Sign-On URL *

https://login.microsoftonline.com/f6e24392-14ba-[REDACTED]

2

URL to use when performing a primary authentication.

Single logout URL

https://login.microsoftonline.com/f6e24392-14ba-[REDACTED]

3

URL, provided by your identity provider, that Duo will send Single Logout responses to. It is unused now but may be used in the future.

Logout redirect URL

URL users will be redirected to after logging out of Duo Single Sign-On.

Certificate *

Click or drag file to this area to upload

NEW_DUO.cer

4

Pasting Entra URLs and Uploading SAML Certificate

4. Click Save, and verify that the status of the external source appears as "Enabled".

Single Sign-On

SettingsExternal Authentication SourcesRouting RulesBridge Attributes

Configured External Authentication Sources

+ Add source

Using external authentication sources? Routing Rules can support a dynamic SSO environment by dictating which auth sources to use based on a variety of conditions.

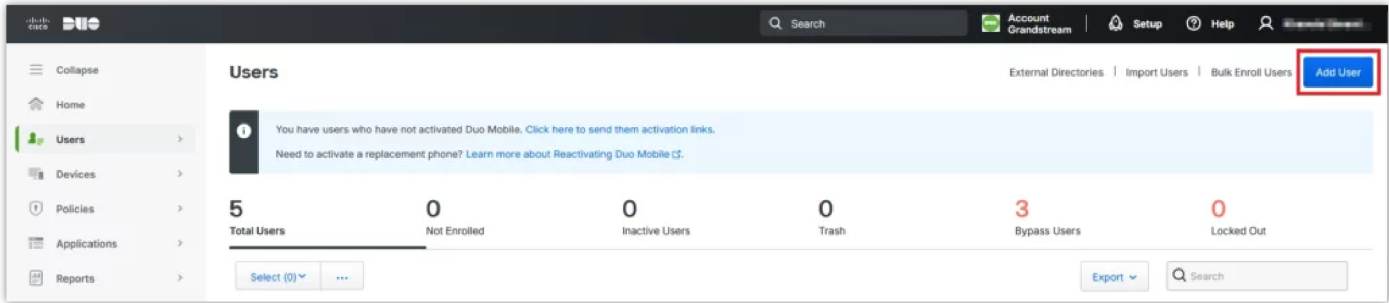
Name	Type	Status	Authentication Proxies ⓘ
SAML Identity Provider	SAML IdP	Enabled	—

External Authentication Source Status

Step 4: Create Users and Groups in DUO

This section describes how to create Duo users and groups for this integration.

- 1. Log in to the **Duo Admin Panel**
- 2. Navigate to **Users→Add User**



Add New DUO User

- 3. Fill in the following fields:

Field	Value
Username	Must match the local part of the Entra ID UPN (value before @)
Email Address	Must match the full Entra ID UPN

Example:

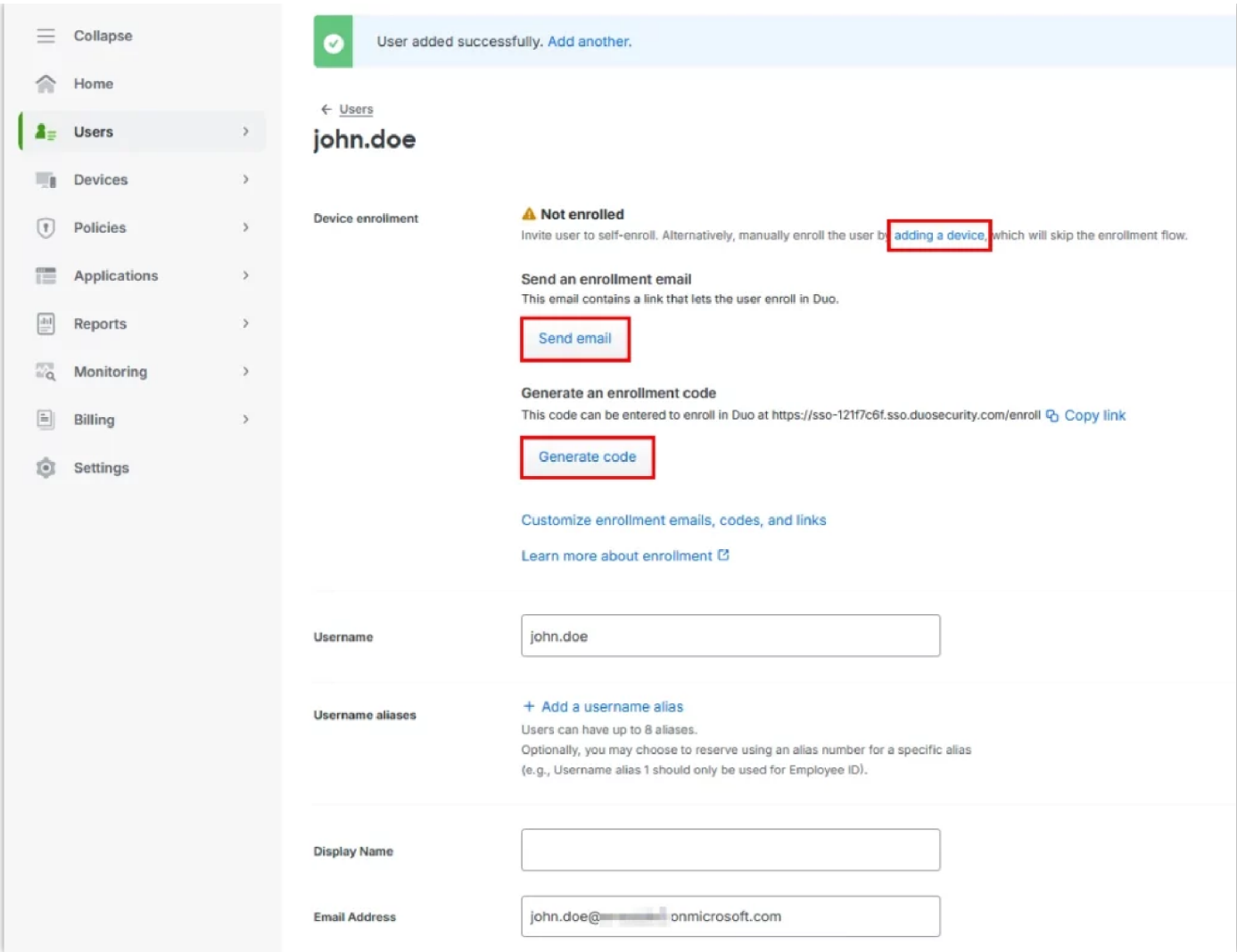
If the Entra ID user UPN is *“test@entra.com”*. Configure the Duo user as:

- **Username:** *test*
- **Email Address:** *test@entra.com*

- 4. After creating the user, complete enrollment using any supported method:
 - Email enrollment
 - Enrollment code
 - Device enrollment

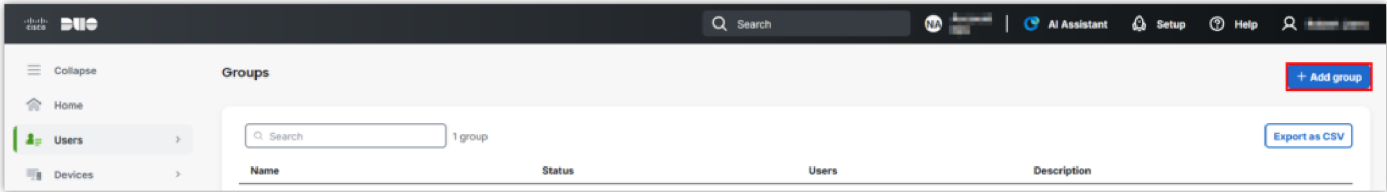
Note:

The enrollment method does not affect SAML attribute matching.



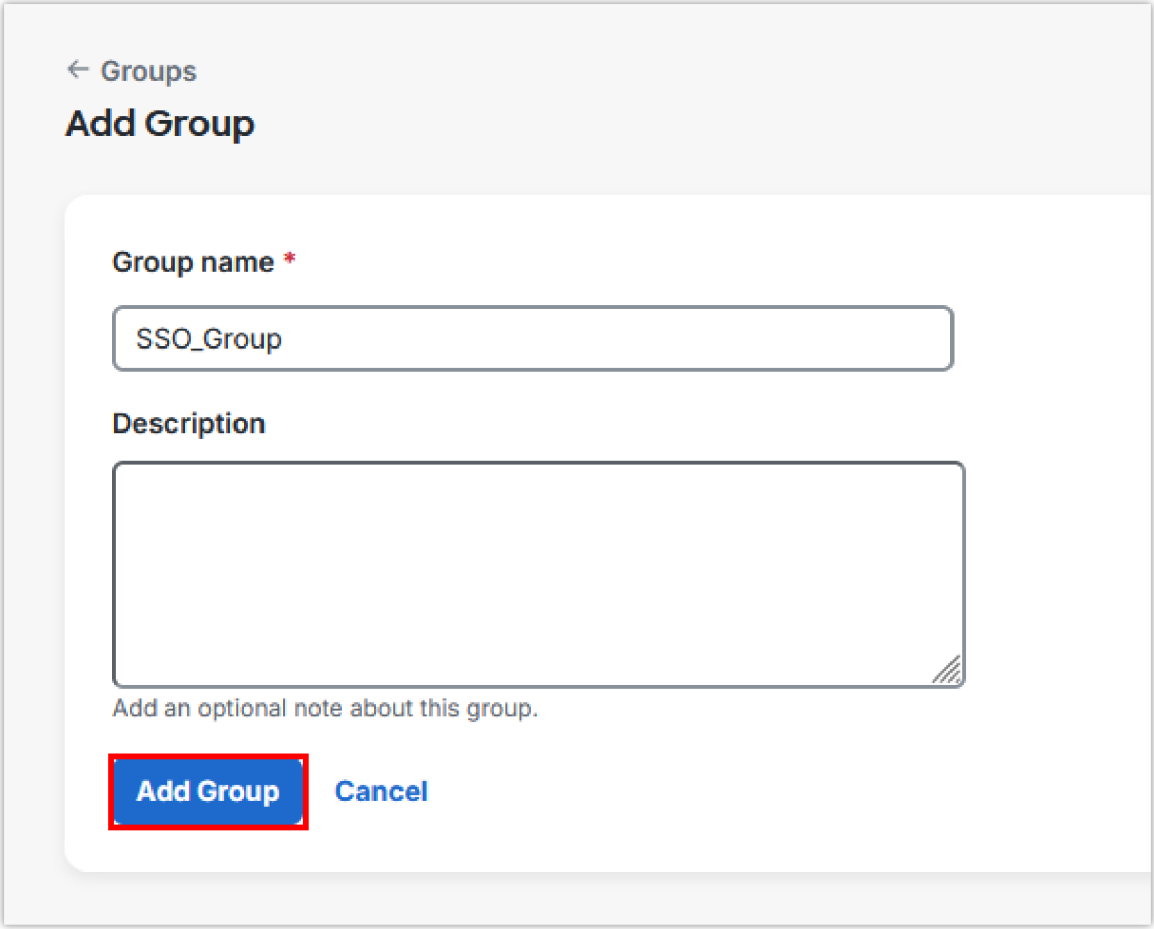
DUO User Enrollment Options

5. Navigate to groups **Users→Groups** and click “Add Group”.



Add DUO User Group

6. Choose a name for the user group and add an optional description.



Configure DUO User Group Name

7. Click on “Add users to group” to configure users allowed to access GDMS/GWN Manager.

Details

Group name

SSO_Group

Description

Group ID

DG6FNTP6HXIFNYO7GYDF

Copy

Status

This controls the two-factor authentication process for users in this group. Changing group status will override the user status of each group member, with the exception of locked out users.

Active

Require two-factor authentication (default).

Bypass

Allow users to skip two-factor authentication and log in with only a password. Passwordless authentication is not skipped.

Disabled

Automatically deny access.

Administrative units

Assign administrative units

Select the administrative units to which this group belongs.

Update Group

Cancel

Search

0 users

+ Add users to group

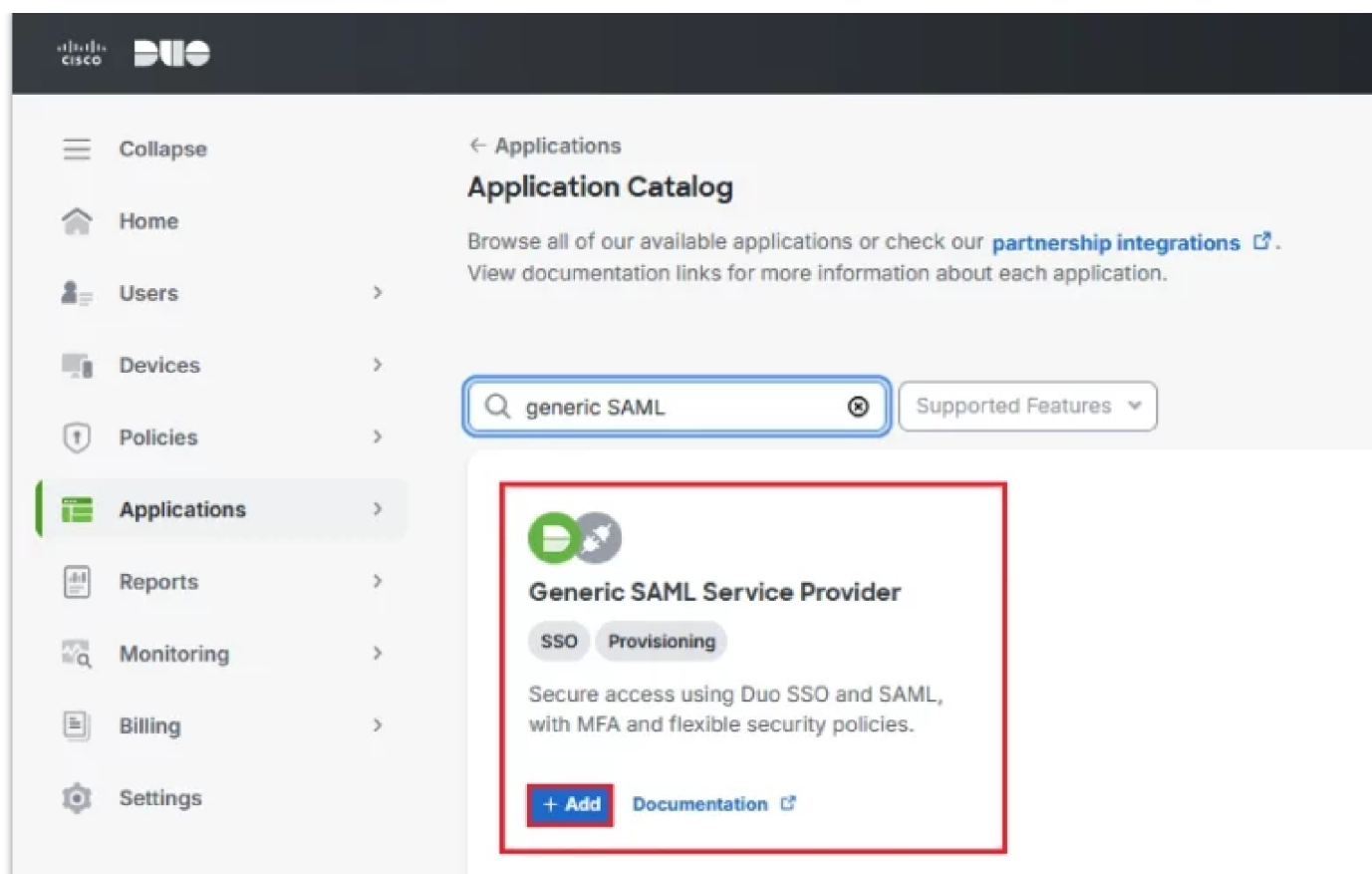
Username	Name	Status	Last Login (UTC)	Actions
----------	------	--------	------------------	---------

Adding Users to DUO Group

Step 5: Create the DUO SAML Application

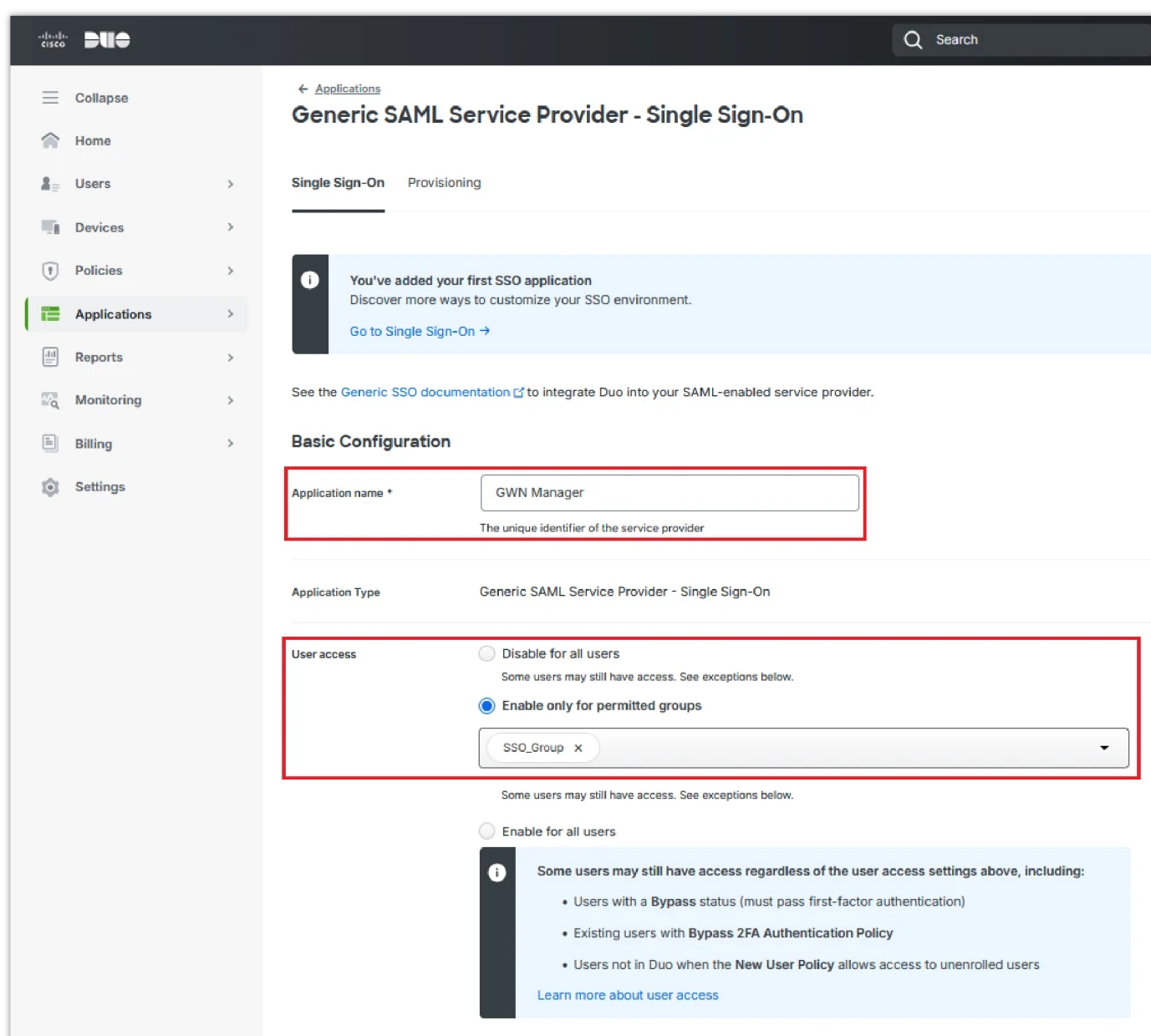
1. Log in to the [Duo Admin Panel](#) and navigate to **Application**→**Application Catalog**.
2. Search for *Generic SAML Service Provider*.

The screenshot shows the Duo Admin Panel interface. On the left is a sidebar with a menu: Collapse, Home, Users, Devices, Policies, Applications (highlighted with a green bar), Reports, Monitoring, Billing, and Settings. The main content area is titled 'Applications' and contains a 'Manage Applications' section. Under this section, 'Application Catalog' is selected and highlighted with a blue bar and a checkmark. Other options listed are 'Authentication Proxy', 'Configure Single Sign-On (SSO)', 'SSO Settings', and 'Duo Central'.



Generic SAML Service Provider Application

3. Configure the application name (example: GWN Manager or GDMS).
4. Enable access for all users or select a specific group to grant application access.



Application Name and User Access Control

5. Configure the **Entity ID** and **ACS URL** by copying them from GDMS/GWN Manager, as shown below:

Service Provider

Metadata Discovery

None (manual input)

Entity ID *

Entity ID

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

Assertion Consumer Service URL

+ Add an ACS URL

The service provider endpoint that receives and processes SAML assertions.

GWN Manager

Default Network

Dashboard

Devices

Clients

Guests

Map & Floor Plans

Insight

Alerts

Settings

Organization

Users

Upgrade

Report

Change Log

Global

Users

User

Roles

Account Security Settings

SAML SSO

Configuration

SAML SSO Role

SAML SSO Configuration Process

Configure IdP Service

Click the Entity ID and ACS URL to copy the data and complete the configuration in the IdP server

Entity ID

ACS URL

1

2

Set up the SAML IdP

Set up the SAML IdP within the GWN Manager using the metadata provided by the IdP

Set up roles

Add the role associated with the SAML IdP configuration

Add SAML IdP

SAML IdP

SAML SSO

SSO Access Code

Remark

Metadata

IdP Entity ID

GWN Manager Entity ID and ACS URL

GDMS Unified Communications

Dashboard

Organization

Default

CloudUCM

VoIP Device

Call Quality

Device Template

Site

Task

Diagnostics

System

Resources

Alerts

Reseller Channel

RPS Management

Users

System Log

API Developer

Users

User

Role

Organization

Associated Company

Account Security Settings

SAML SSO

Configure

SAML SSO role

SAML SSO Configuration Process

Configure IdP Service

Click the Entity ID and ACS URL to copy the data and complete the configuration in the IdP server

Entity ID

ACS URL

1

2

Set up the SAML IdP

Set up the SAML IdP within the GDMS using the metadata provided by the IdP

Set up roles

Add the role associated with the SAML IdP configuration

Add SAML IdP

SAML IdP

SAML SSO

SSO Access Code

remarks

Metadata

IdP Entity ID

GDMS Entity ID and ACS URL

6. Scroll down to continue the configuration. The following three parameters are mandatory and must be configured.

NameID attribute		Select <Email Address>
Map attributes	IdP Attribute	Select <Email Address>
	SAML Response Attribute	Fill in the fixed parameters for: GDMS: https://account.gdms.cloud/saml/attribute/emailaddress GWN Manager: <a href="https://<gwn-manager-host>[:port]/user/saml/attribute/emailaddress">https://<gwn-manager-host>[:port]/user/saml/attribute/emailaddress <i>Note: If GWN Manager is not bound to port 443, the port number must be included in the URI.</i>

Role attributes	Attribute name	Fill in the fixed parameters for: ● GDMS: https://account.gdms.cloud/saml/attribute/role ● GWN Manager: <a href="https://<gwn-manager-host>[:port]/user/saml/attribute/role">https://<gwn-manager-host>[:port]/user/saml/attribute/role <i>Note: If GWN Manager is not bound to port 443, the port number must be included in the URI.</i>
	Service Provider’s Role	Fill in the role value, which must be the same as the SAML SSO Role name in Users→SAML SSO Role , such as “Admin.A”
	Duo Groups	Select the user group to use. Only users who belong to the selected Duo group will be allowed to authenticate using SAML SSO. User groups in Duo can be created and managed under Users→Groups in the Duo Admin Panel.

SAML Response

NameID format *

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

The format that specifies how the NameID is sent to the service provider.

NameID attribute *

<Email Address>

NameID is a SAML attribute that identifies the user. Enter an IdP attribute or select a bridge attribute that automatically chooses the NameID attribute based on the IdP. Create custom bridge attributes or select from the preconfigured options: <Email Address>, <Username>, <First Name>, <Last Name>, <Display Name>.

Map attributes

IdP Attribute

<Email Address>

SAML Response Attribute

https://192.168.6.225:8443/

Map the values of an IdP attribute to another attribute name to be included in the SAML response (e.g. Username to User.Username). Enter in an IdP attribute or select one of Duo's preconfigured user attributes that automatically chooses the SAML response attribute based on the IdP. There are five preconfigured user attributes: <Email Address>, <Username>, <First Name>, <Last Name>, <Display Name> and any additional user attributes that you have configured. <AMR> refers to Authentication Method Reference, which will send authentication information to the service provider. While most service providers use "amr" in the response, you may need to contact them for more information on their attribute names.

Create attributes

Name

Value

Specify attributes with hard-coded values to optionally send in the SAML response (e.g. accountNumber with value of 48152547). Consult your service provider for more information.

Role attributes

Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each role can have multiple groups mapped to it. Optional. [Learn more about Duo groups.](#)

Attribute name

https://192.168.6.225:8443/user/saml/attribute/role

The name of the attribute which will carry the mapped roles.

Service Provider's Role

Admin.D

Duo groups

SSO_Group (3 users)

GWN Manager App Attribute Mapping

7. To enable IdP-initiated login from the Duo dashboard, configure the **Default Relay State** to point to the GDMS or GWN Manager login page.

Collapse

Home

Users

Devices

Policies

Applications

Reports

Monitoring

Billing

Settings

Service Provider Login URL

Service Provider Login URL

Optional: A URL provided by your service provider that will start a SAML authentication. Leave blank if unsure.

Default Relay State

https://192.168.6.225:8443/

Optional: When set, all IdP-initiated requests include this relaystate. Configure if instructed by your service provider.

SAML Response

NameID format *

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

The format that specifies how the NameID is sent to the service provider.

NameID attribute *

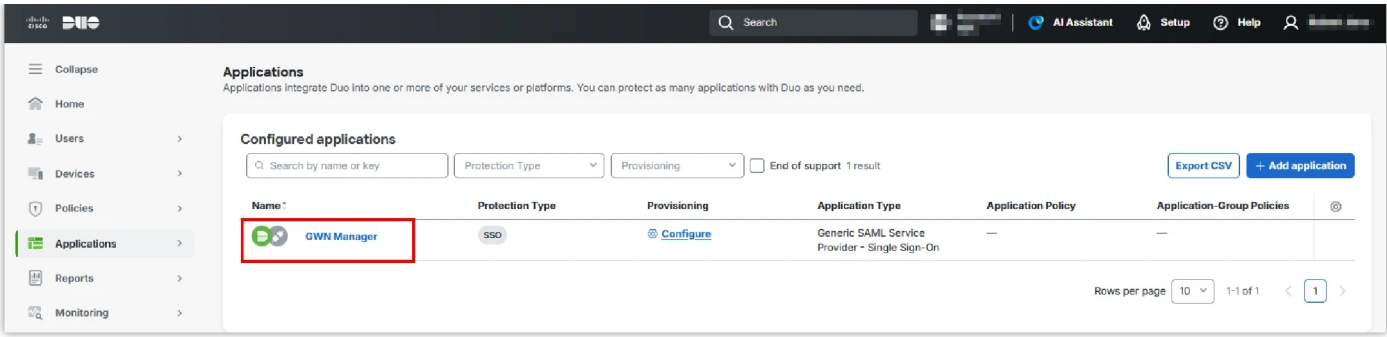
<Email Address>

NameID is a SAML attribute that identifies the user. Enter an IdP attribute or select a user attribute that automatically chooses the NameID attribute to use: <Email Address>, <Username>, <First Name>, <Last Name>, <Display Name>.

DUO App Default Relay State

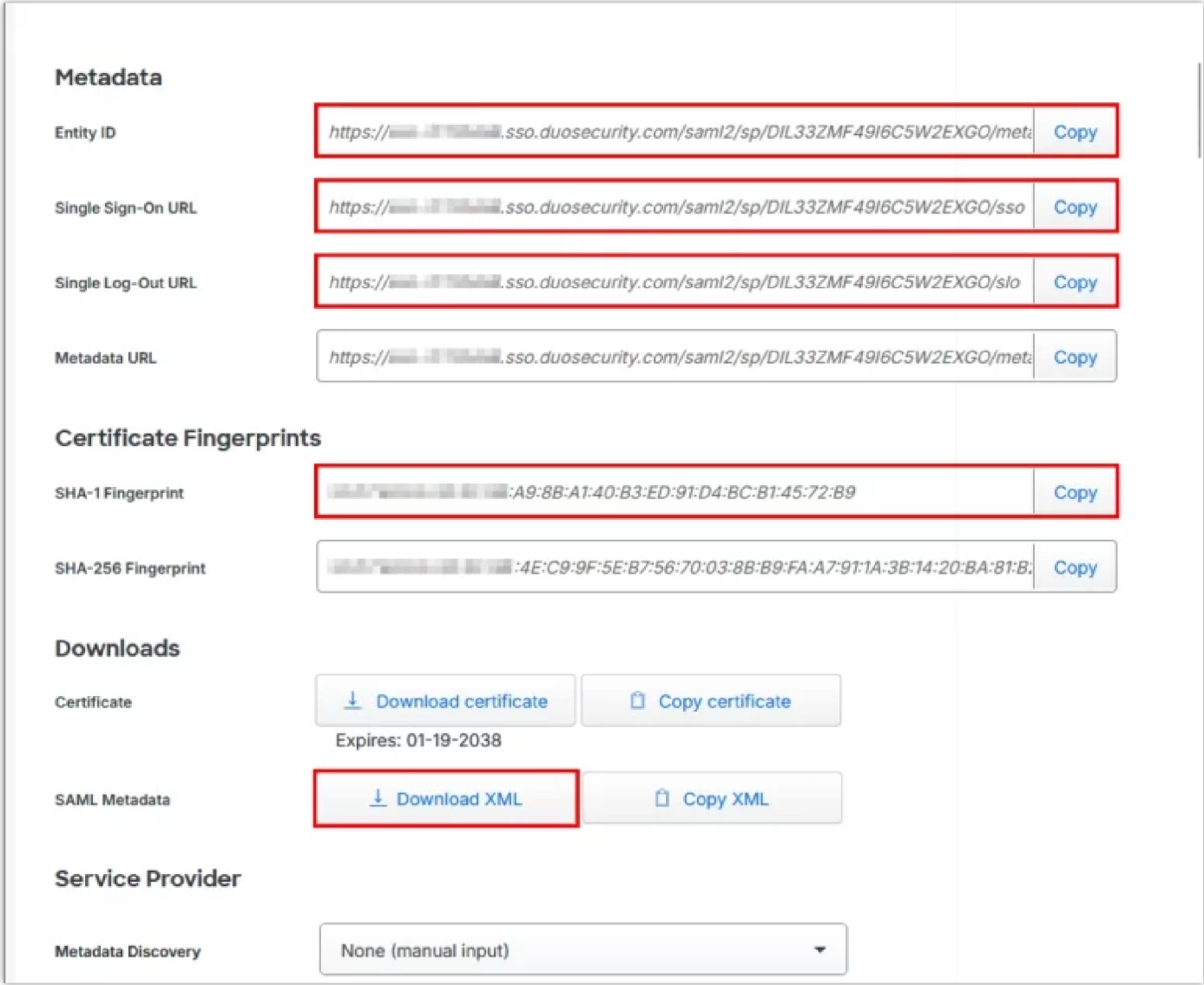
Step 6: SAML SSO in GDMS/GWN Manager

1. Log in to the [Duo Admin Panel](#) and navigate to the GDMS/GWN Manager **Application**.



Duo Admin Panel GWN Manager Application

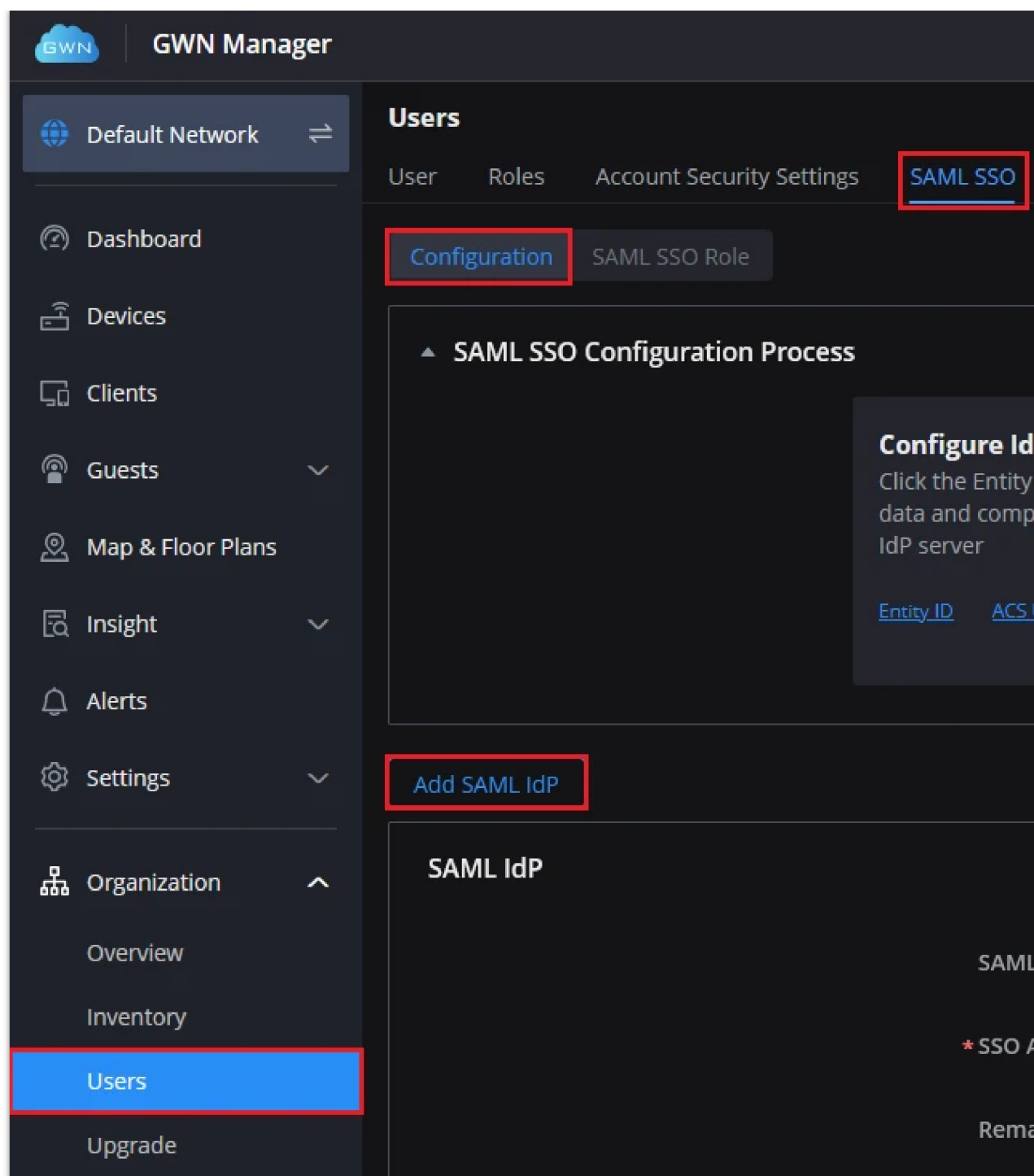
2. Access the application you created, and copy the following information or download the metadata.



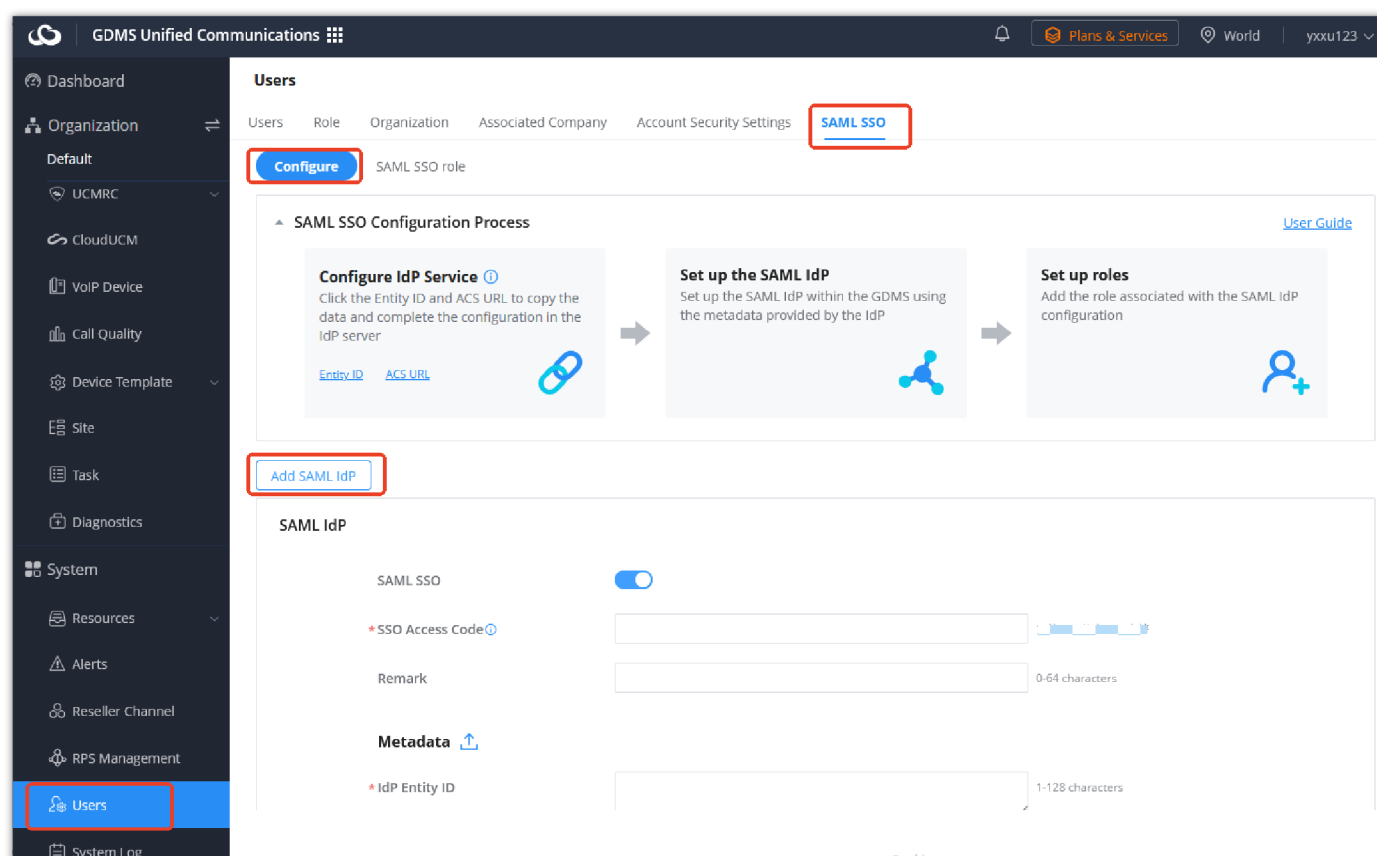
GWN Manager Application Metadata

3. Log in to GDMS or GWN Manager using a Super Administrator account.

4. Navigate to **Users**→**SAML SSO**.

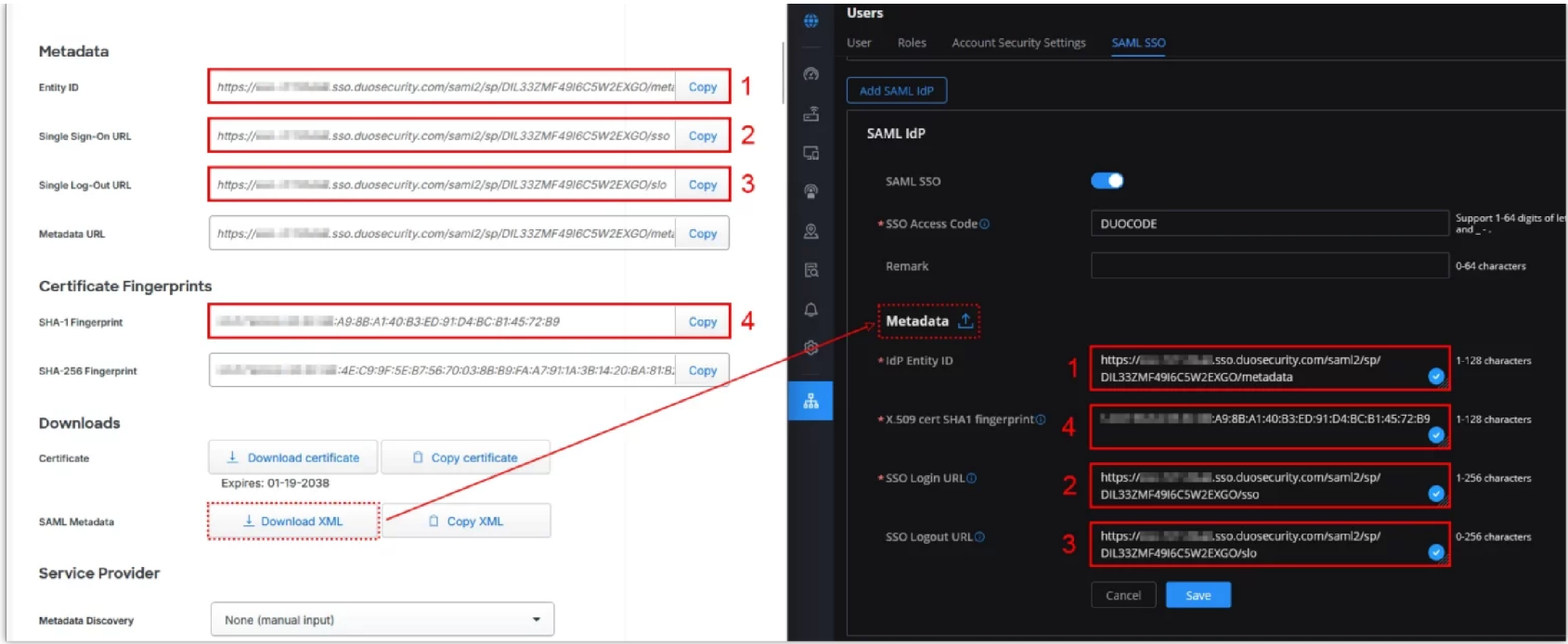


Adding SAML IdP in GWN Manager



Adding SAML IdP in GDMS

5. Click **Add SAML IdP** and fill in the information:



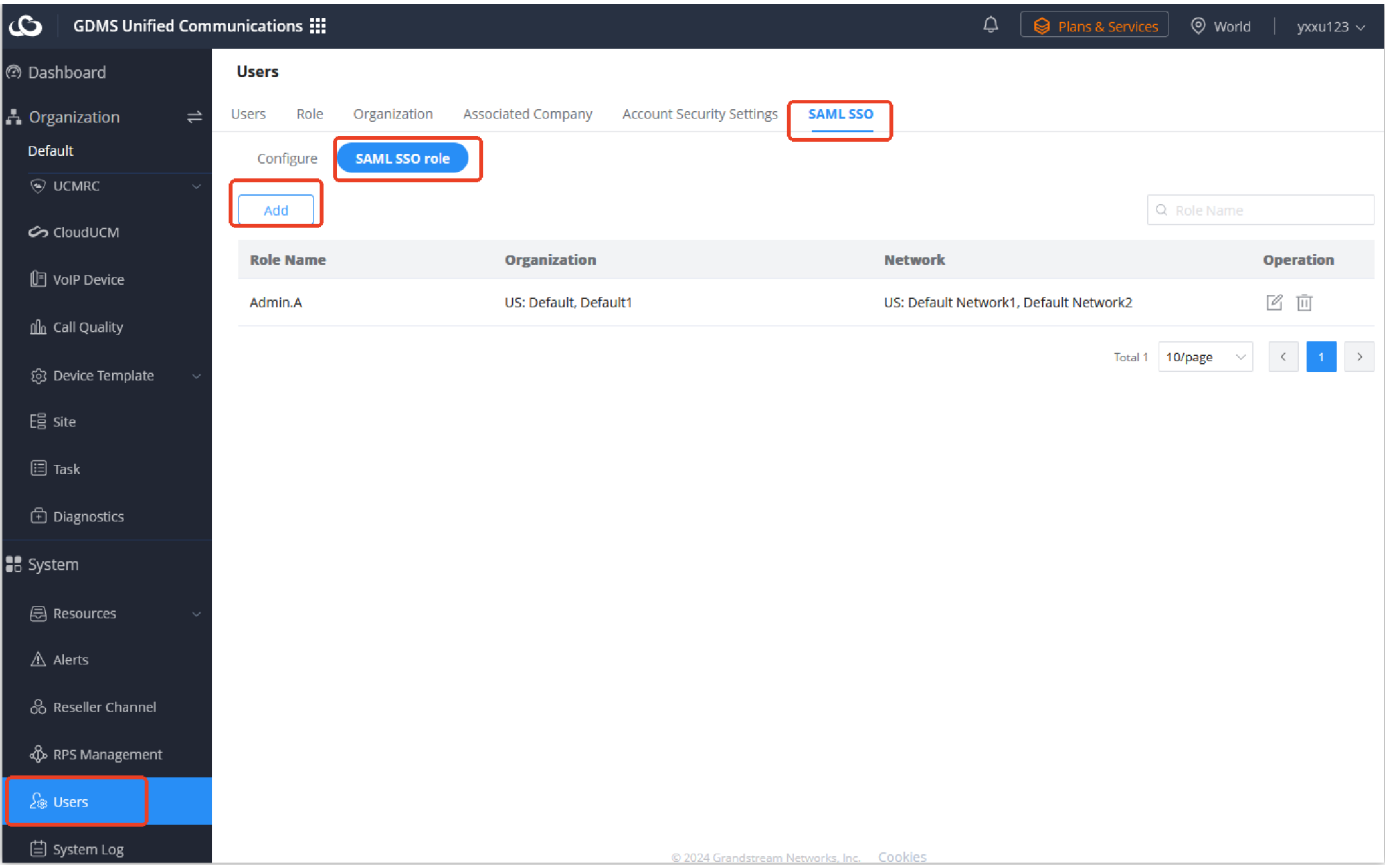
SAML SSO	Enable or disable. If disabled, users will no longer be able to use the configured SSO authentication to log in.
SSO Access Code	Used to enter this SSO Access Code on the GDMS/GWN Manager login page, and can log in through this IdP service authentication.
Remarks	Enter your remarks
Metadata	● Method 1: Click to upload the metadata XML file to parse the fields below. ● Method 2: Manually fill in the fields as follows.
IdP Entity ID	Fill in the Entity ID of the Metadata module in Duo→Application .
X.509 cert SHA1 fingerprint	Fill in the SHA-1 Fingerprint of the Metadata module in Duo→Application .
SSO Login URL	Fill in the Single Sign-on URL of the Metadata module in Duo→Application .
SSO Logout URL	(Optional) Fill in the Single Sign-out URL of the Metadata module in Duo→Application .

6. After adding the IdP, configure the SAML SSO role as described in section [[SAML SSO ROLES IN GDMS/GWN MANAGER](#)]. The Role Name must exactly match the role value sent by the IdP.

SAML SSO ROLES IN GDMS/GWN MANAGER

GDMS Role Configuration

1. Log in as Super administrator logs in to GDMS and goes to **Users→SAML SSO→SAML SSO Role**.



Adding SAML SSO Role in GDMS

2. Click **Add** Role and fill in the following information:

SAML SSO > Add role

General Settings

UC Permissions

Networking Permissions

* Role Name ⓘ

Admin.A

1-64 characters

UC Organization

World

EU Region

China

Default × Default1 ×

Networking

World

EU Region

China

Default Network × test ×

☒ Auto Add New Network ⓘ

Next

Editing SAML SSO Role

Role Name	Enter the name of this role. Note: It must be the same as the value of the application role created in Azure. For example “Admin.A”.
UC Organization	(Optional) Assigned to the Unified Communications organizations that this role can manage.
Networking	(Optional) Assign networkings that this role can manage.

3. Click **Next** to configure the permissions for the GDMS UC system. If this role does not have permissions for the GDMS UC system, you do not need to select any permissions.

SAML SSO > Add role

General Settings

UC Permissions

Networking Permissions

< Basic

UCMRC

CloudUCM

Resources

Alerts

Reseller Channel

RPS Management

Users

Syster >

☐ All

☐ Dashboard

☐ Overview

☐ Extension - SIP Account

☐ Account List

☐ Add Account

☐ Import Account

☐ Export Account

☐ Edit Account

☐ Delete Account

☐ Modify SIP Server

☐ Go to PBX/CloudUCM Web UI to edit extension

☐ Extension - SIP Server

☐ SIP Server List

☐ Add Server

☐ Delete Server

☐ Edit Server

☐ VoIP Device

☐ Device List

☐ Transfer Device

☐ Add Device

☐ Authorization Management

☐ Import Device

☐ Export Device

☐ Edit Device

☐ Delete Device

☐ Open Subscription

☐ Upgrade Firmware

☐ Reboot Device

☐ Factory Reset

☐ Device Diagnostics

☐ Site Assignment

☐ Set Parameters

☐ Account Configuration

☐ Operation Logs

☐ Task History

☐ Reconfigure

☐ Device Details

Back

Next

Configuring UC Permissions for SAML SSO Role

4. Click **Next** to configure the permissions for the GDMS Networking system.

◦ If you select Platform Administrator, you must select Manage All Networking in the previous step, otherwise you cannot select Platform Administrator.

◦ If this role has permissions for the GDMS Networking system, you can select "None".

SAML SSO > Add role

General Settings

UC Permissions

Networking Permissions

Permissions

Organization

Network

☐ All Organization Privilege

☐ Overview

☐ Network Overview (Read-only)

☐ Configure Map Component

☐ Inventory

☐ Device Information (Read-only)

☐ Export Device Information

☐ Reseller Channel

☐ Reseller Channel List (Read-only)

☐ Configure Reseller Channel Info

☐ Users

☐ User List (Read-only)

☐ Role List (Read-only)

☐ Associated Company (Read-only)

☐ Configure User

☐ Configure Role

☐ Configure Associated Company

Custom

Platform Administrator

Platform Administrator (Read-only)

Network Administrator

Network Administrator (Read-only)

Guest Editor

Custom

Network Sort

Back

Finish

Configuring Networking Permissions for SAML SSO Role

5. Click **Finish** to successfully create the SSO role.

Configure

SAML SSO role

Add

Role Name

Organization

Network

Operation

Admin.A

US: Default, Default1

US: Default Network1, Default Network2

Total 1

10/page

<

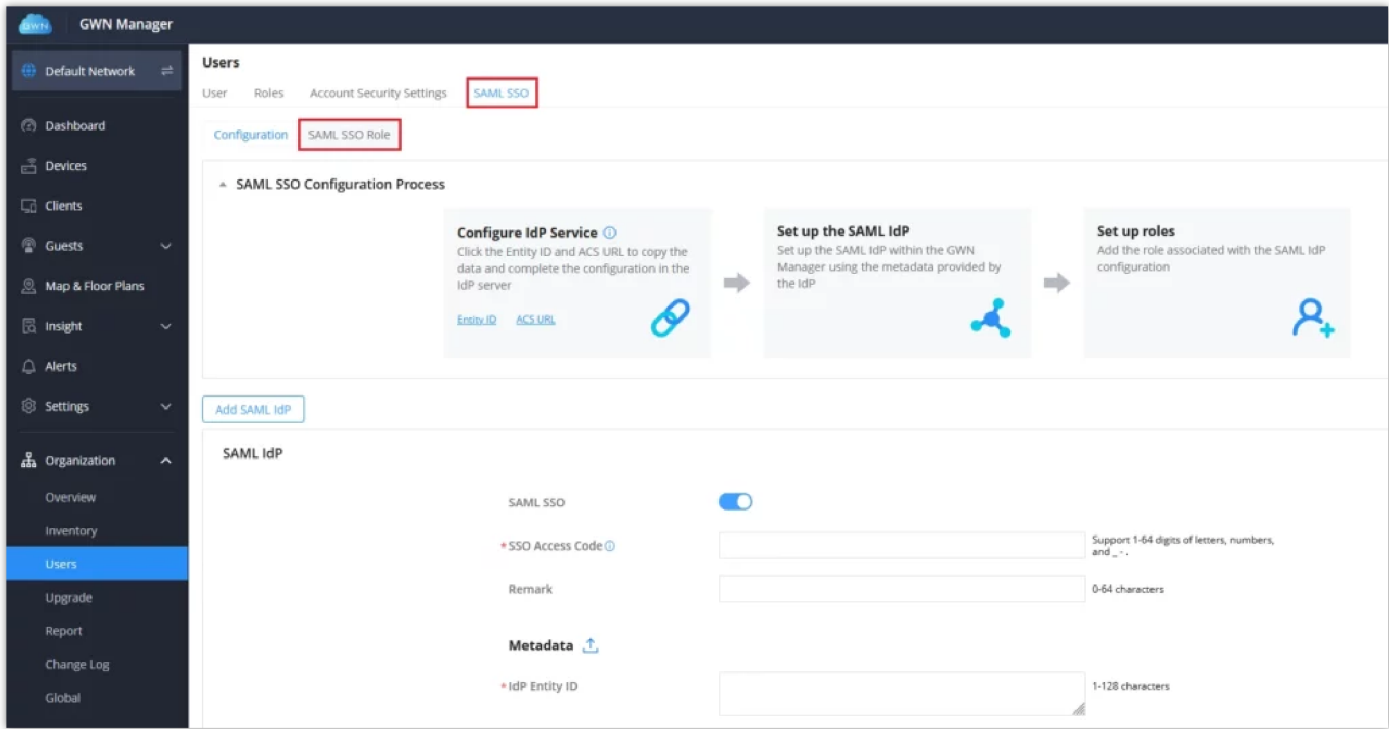
1

>

Created SAML SSO Role

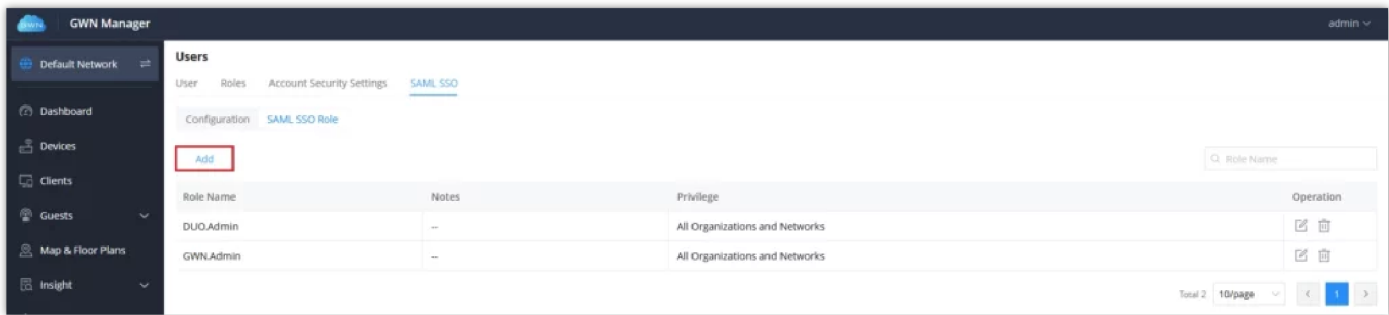
GWN Manager Role Configuration

- 1. Log in to GWN Manager using a local administrator account.
- 2. Navigate to **Organization**→**Users**→**SAML SSO**.
- 3. Select the **SAML SSO Role** tab.



GWN Manager SAML Role Page

- 4. Click **Add** to create a new SAML SSO role.



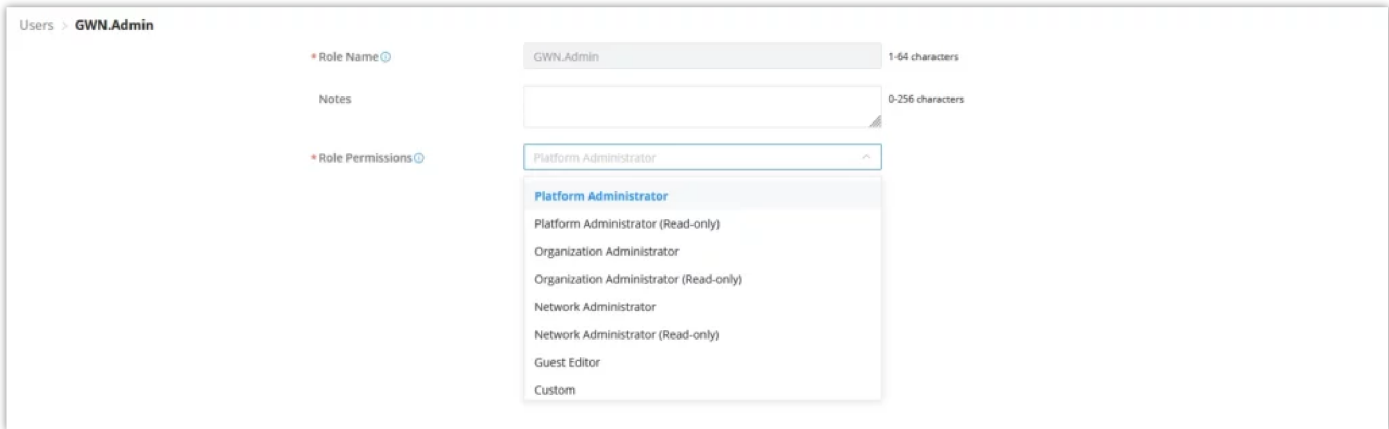
Add GWN Manager SAML Role

- 5. Enter the name of the SAML SSO role. This value must exactly match the role value sent by the IdP in the SAML assertion.

Note:

If the role name does not match exactly, GWN Manager will reject the login even if authentication is successful.

- 6. After defining the Role Name, configure the permissions associated with this role. Each option corresponds to a predefined permission scope within GWN Manager.
- 7. If Custom is selected, granular permissions can be assigned manually.



SAML Role Permissions

Users

UserRolesAccount Security SettingsSAML SSO

Add

Role Name	Creator	Description	Operation
Super Administrator	GWN Manager	Grants read/write permissions for all organizations, networks, and sub-accounts under the enterprise along with the ability to cr...	
Platform Administrator	GWN Manager	Grants read/write permissions for all organizations, networks, and sub-accounts under the enterprise along with the ability to cr...	
Platform Administrator (Read-only)	GWN Manager	Grants read-only permissions for all organizations, networks, and sub-accounts under the enterprise.	
Organization Administrator	GWN Manager	Read/write permissions for all organizations, networks, and sub-accounts under the account. Can also create new networks and ...	
Organization Administrator (Read-only)	GWN Manager	Read-only permissions for all networks under the account	
Network Administrator	GWN Manager	Grants read/write permissions for all networks under this account along with the ability to create guest administrators for their ...	
Network Administrator (Read-only)	GWN Manager	Grants read-only permissions for networks under the account	
Guest Editor	GWN Manager	Grants read/write permissions for all guests along with the ability to create and manage vouchers.	

Total: 810/page

GWN Manager User Roles

8. Click Save to complete role creation. The newly created role will appear in the SAML SSO Role list.

GWN Manager

admin

Default Network

Dashboard

Devices

Clients

Guests

Map & Floor Plans

Insight

Users

UserRolesAccount Security SettingsSAML SSO

ConfigurationSAML SSO Role

Add

G: Role Name

Role Name	Notes	Privilege	Operation
DUO.Admin	--	All Organizations and Networks	
GWN.Admin	--	All Organizations and Networks	

Total: 210/page

GWN Manager Role List

SAML SSO TESTING AND VALIDATION

This section describes how to validate SAML SSO authentication and logout behavior when GDMS or GWN Manager is integrated with an Identity Provider.

Testing should verify both authentication flows:

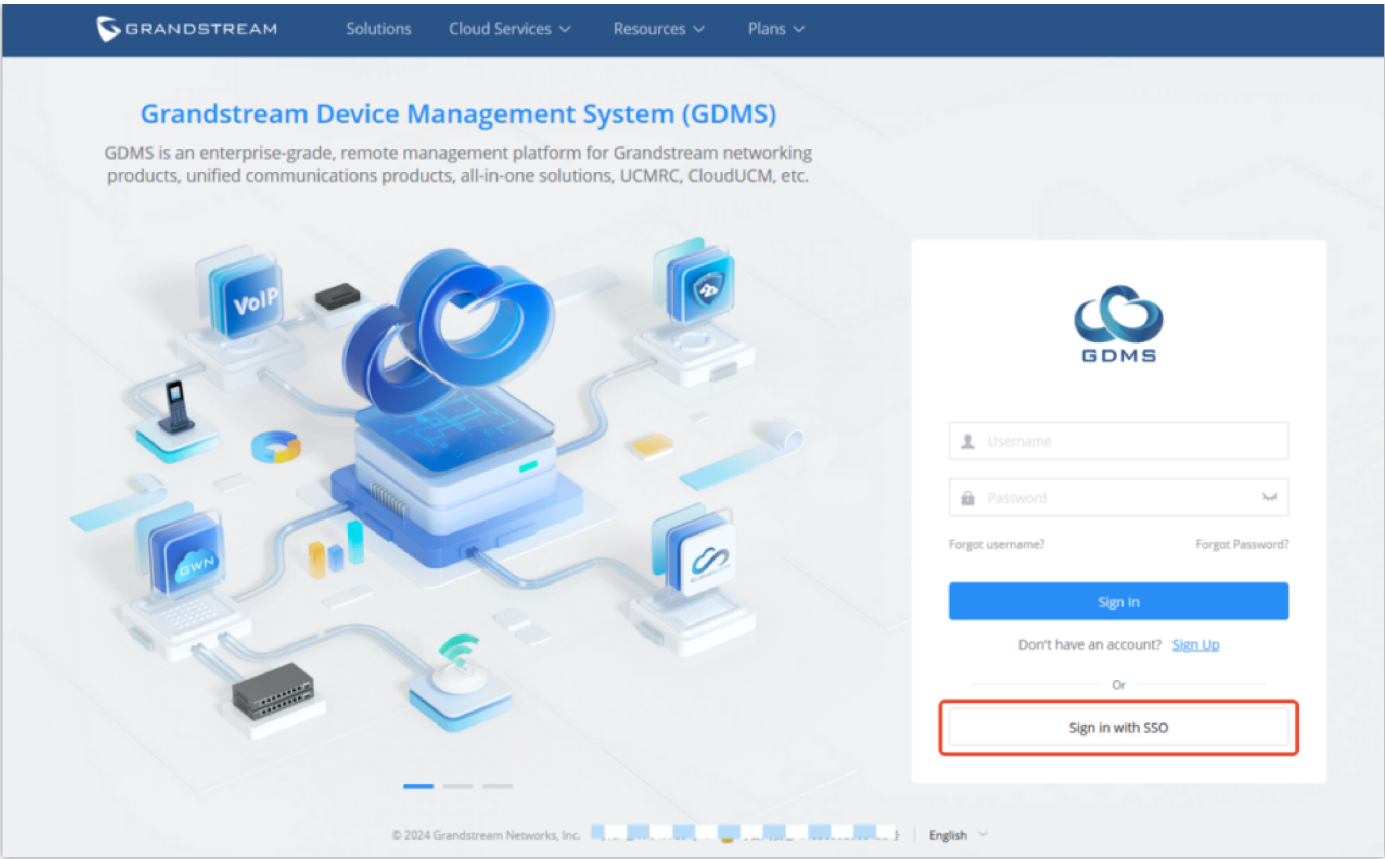
- **SP-initiated login:** authentication starts from the GDMS or GWN Manager.
- **IdP-initiated login:** authentication starts from the Identity Provider portal (Entra ID, Duo).

SP-Initiated Login Test

Web Login Test

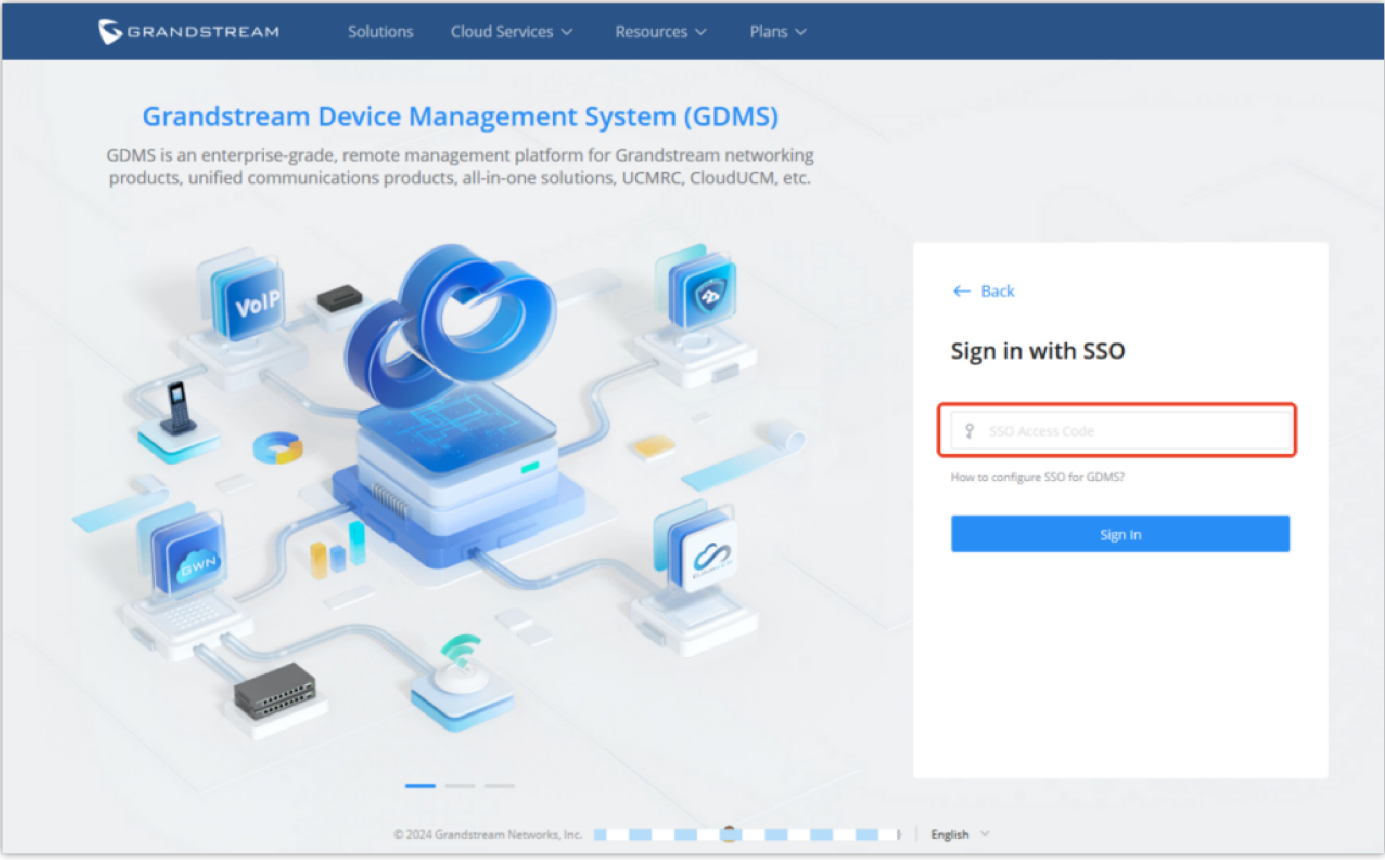
This test verifies authentication initiated from GDMS or GWN Manager.

1. Open a web browser.
2. Navigate to:
 - **GDMS:** `https://www.gdms.cloud`
 - **GWN Manager:** `https://<gwn-manager>:<port>`
3. Click **Sign in with SSO** at the bottom of the GDMS/GWN Manager login page.

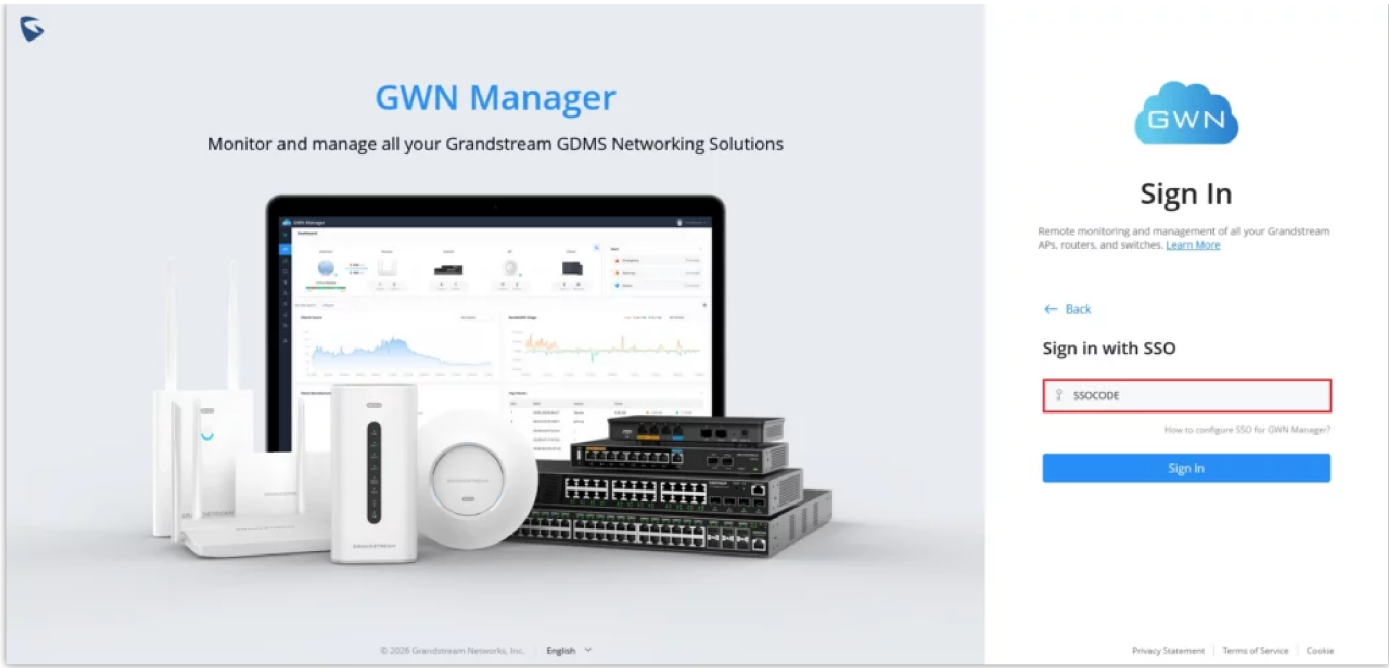


GWN Manager Login Page

4. Enter the **SSO Access Code** configured by the administrator.

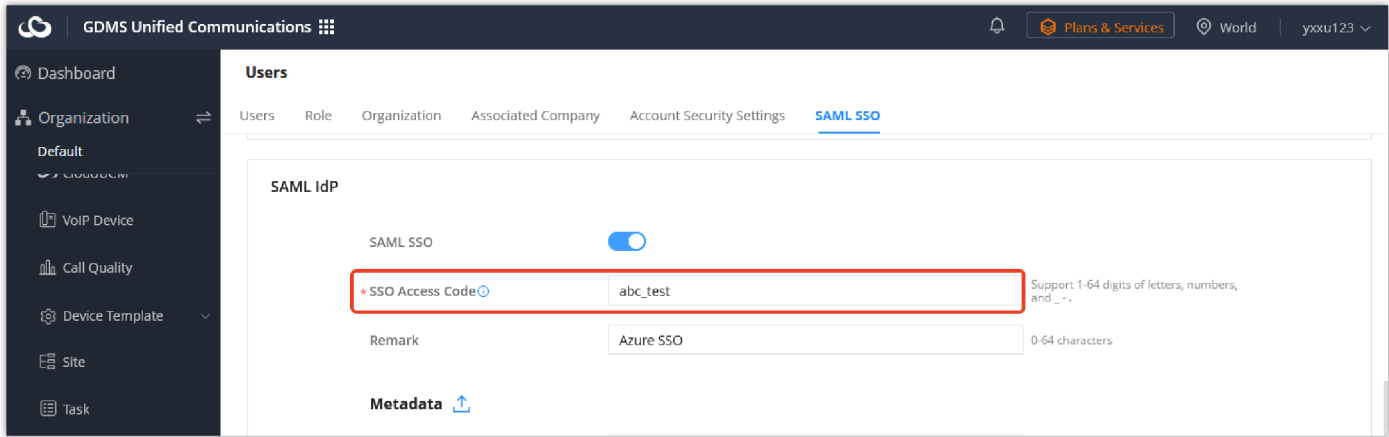


GDMS SSO Access Code Prompt



GWN Manager SSO Access Code Prompt

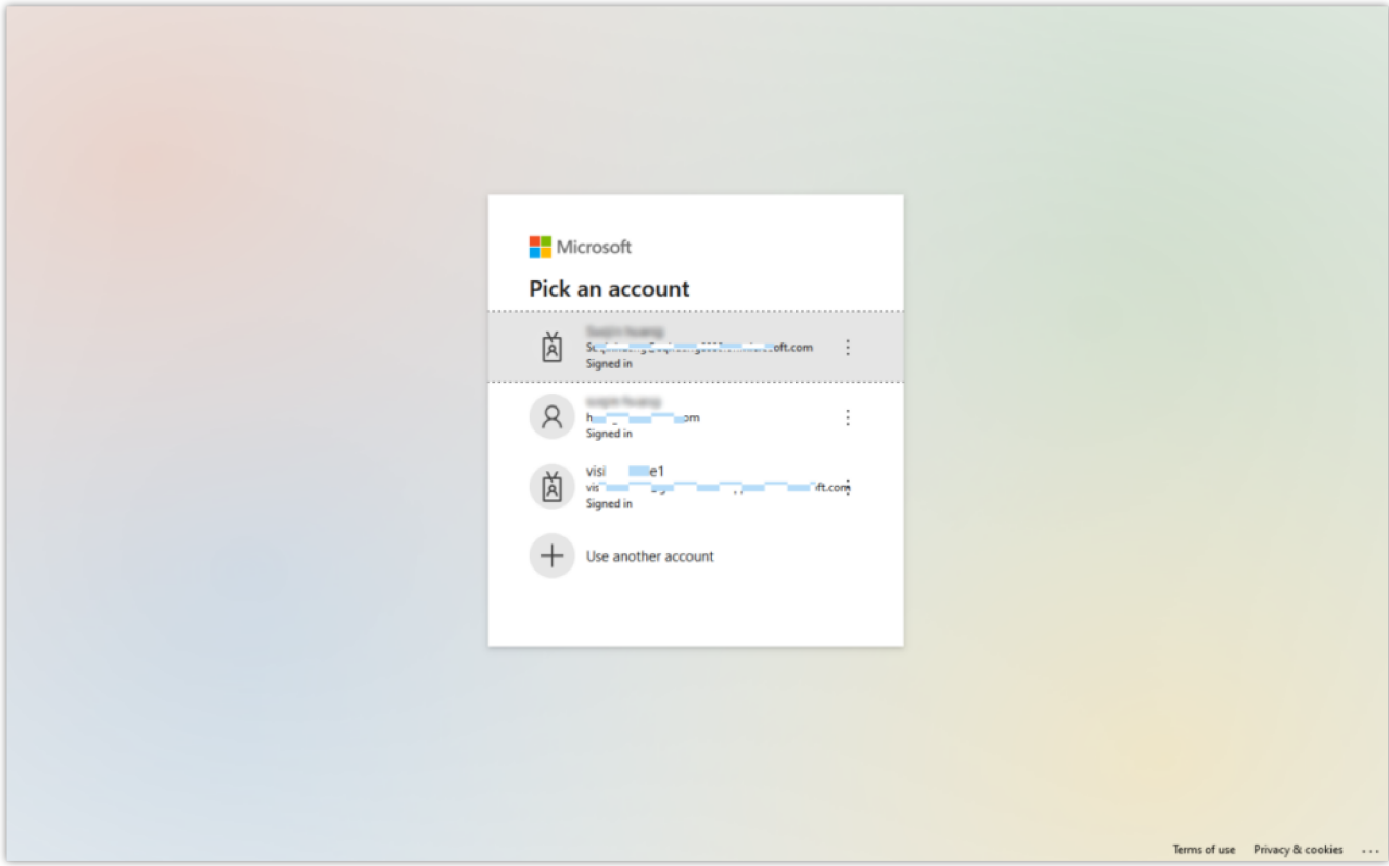
5. The **SSO Access Code** from the GDMS/GWN Manager can be configured on the SAML SSO page as follows:



SSO Access Code Configuration

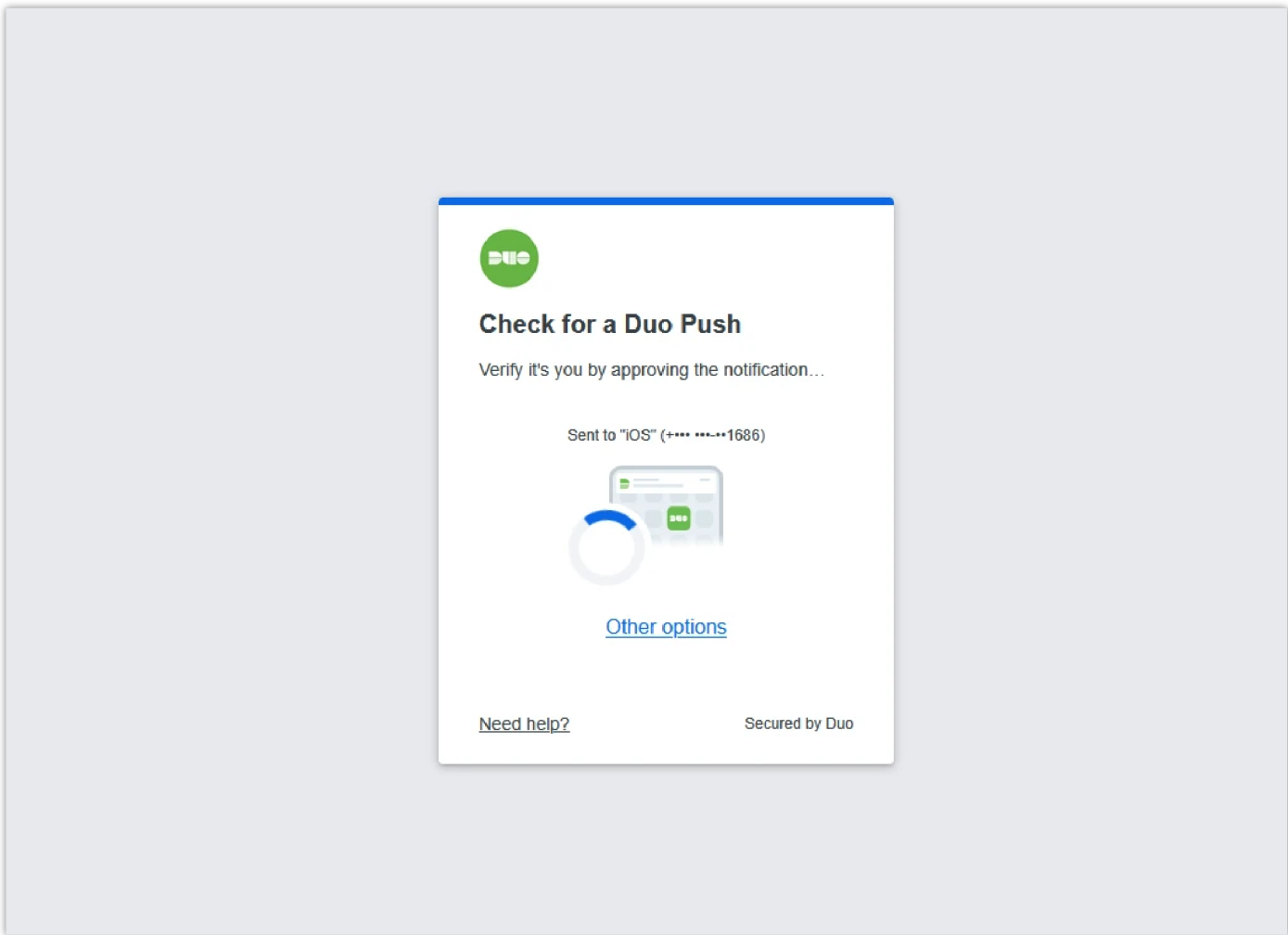
6. The browser must redirect to the configured IdP login page:

- o Microsoft Entra ID login page
- o AD FS login page
- o Duo authentication page



Microsoft Entra ID login page



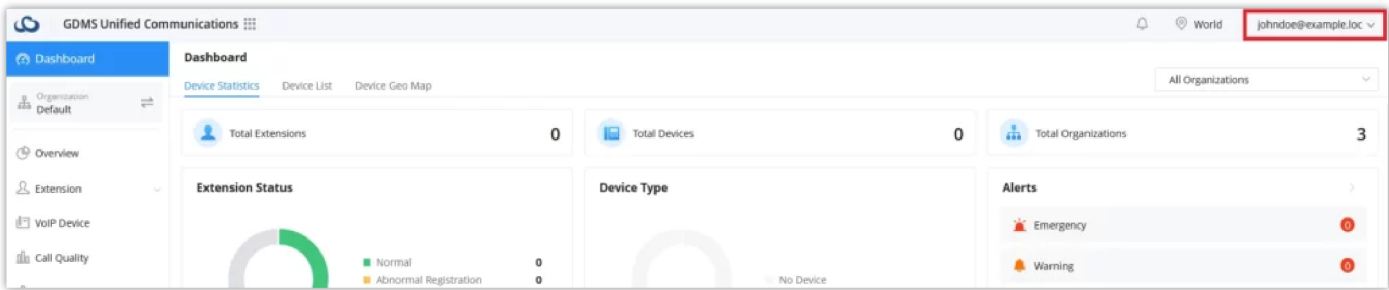


Duo Authentication Page

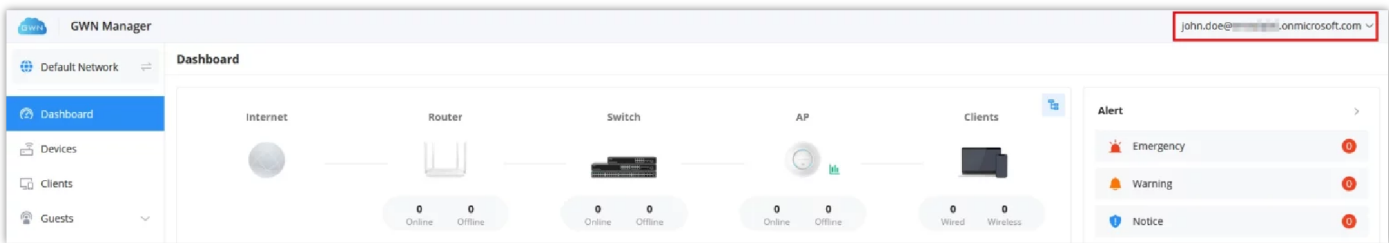
Note:

For GWN Manager, if login fails with an HTTP 500 error, verify that the GWN Manager system time is synchronized.

6. After successful authentication, verify that:
- You are redirected back to the application
 - Login completes successfully
 - The correct SAML SSO role is applied

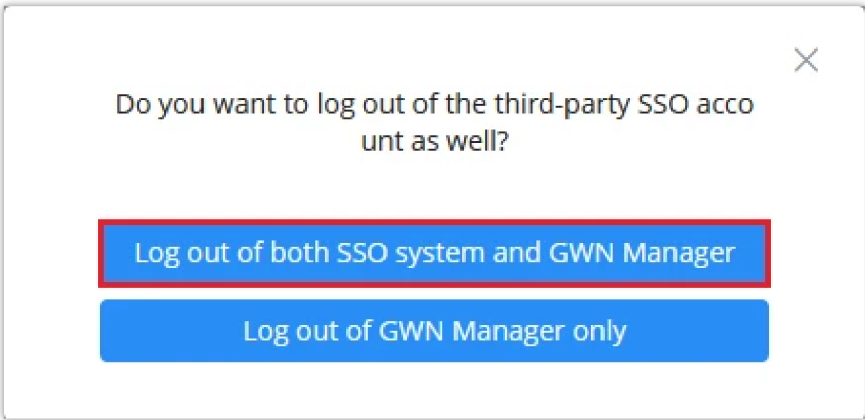


GDMS Login Example with AD User



GWN Manager Login Example with Microsoft User

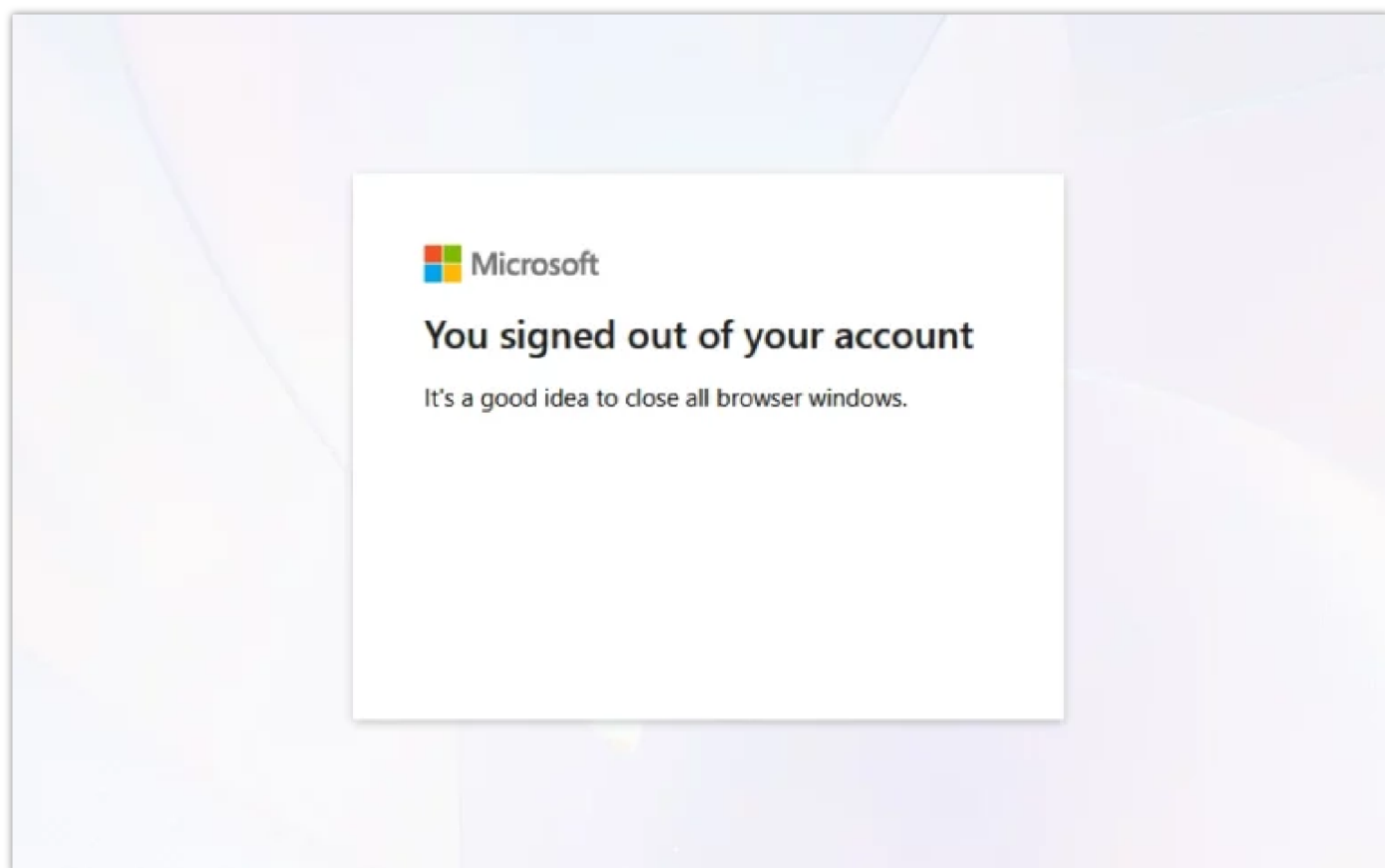
7. (Optional) If SAML Single Logout (SLO) is configured, click Logout from both the application and the SSO system.



GDMSGWN Manager Logout Prompt

8. Verify that:

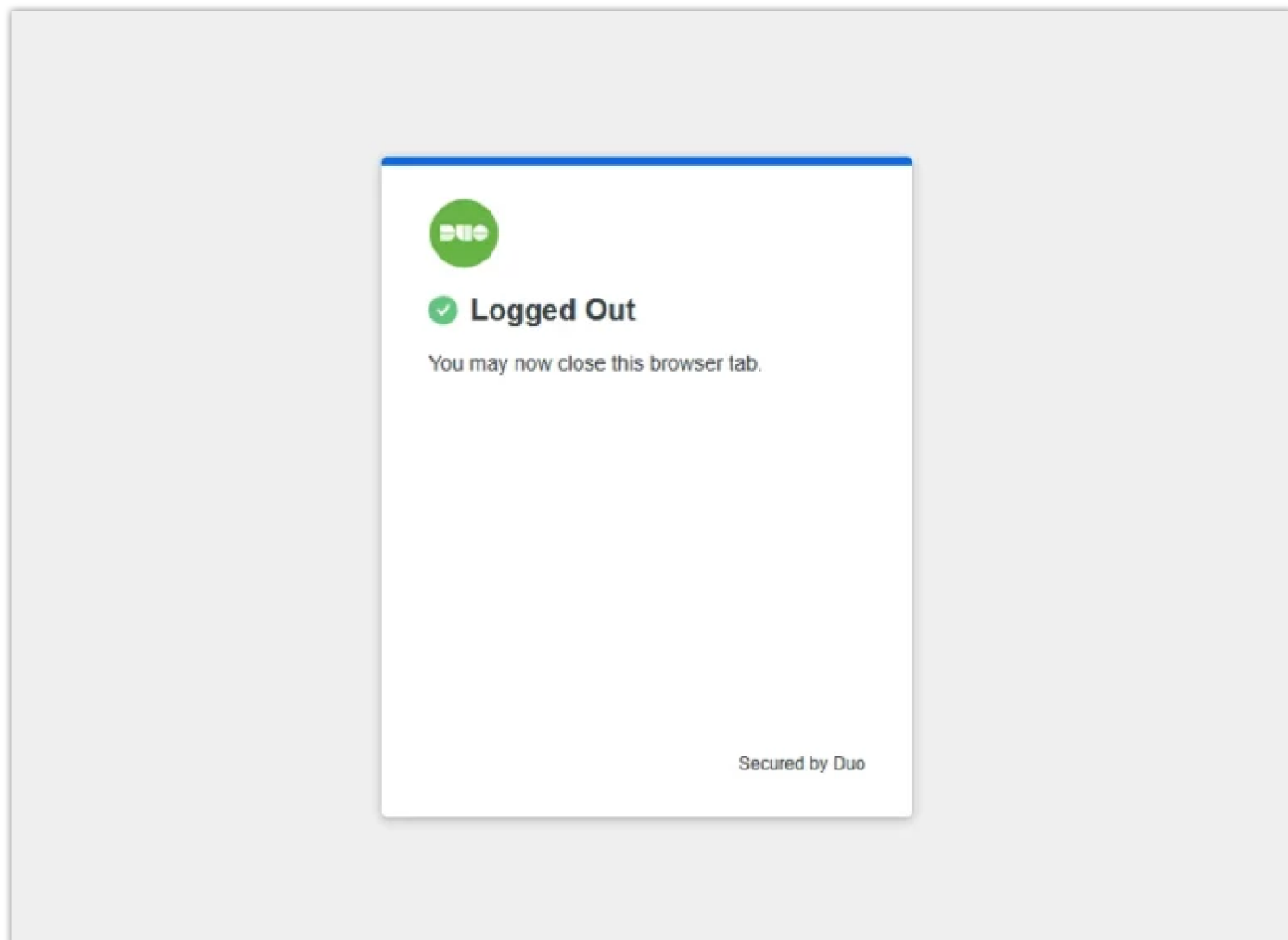
- The GDMS/GWN Manager session is terminated
- The SSO system is terminated



Microsoft Logout Page



AD Logout Page



DUO Logout Page

Mobile App Login Test

1. Click **Sign in with SSO** at the bottom of the GDMS login page, and then enter the SSO Access Code configured by the administrator.

<



Username

Password

Sign In

Custom Domain Login

More sign in methods

Sign in with SSO

Sign in with Google

<



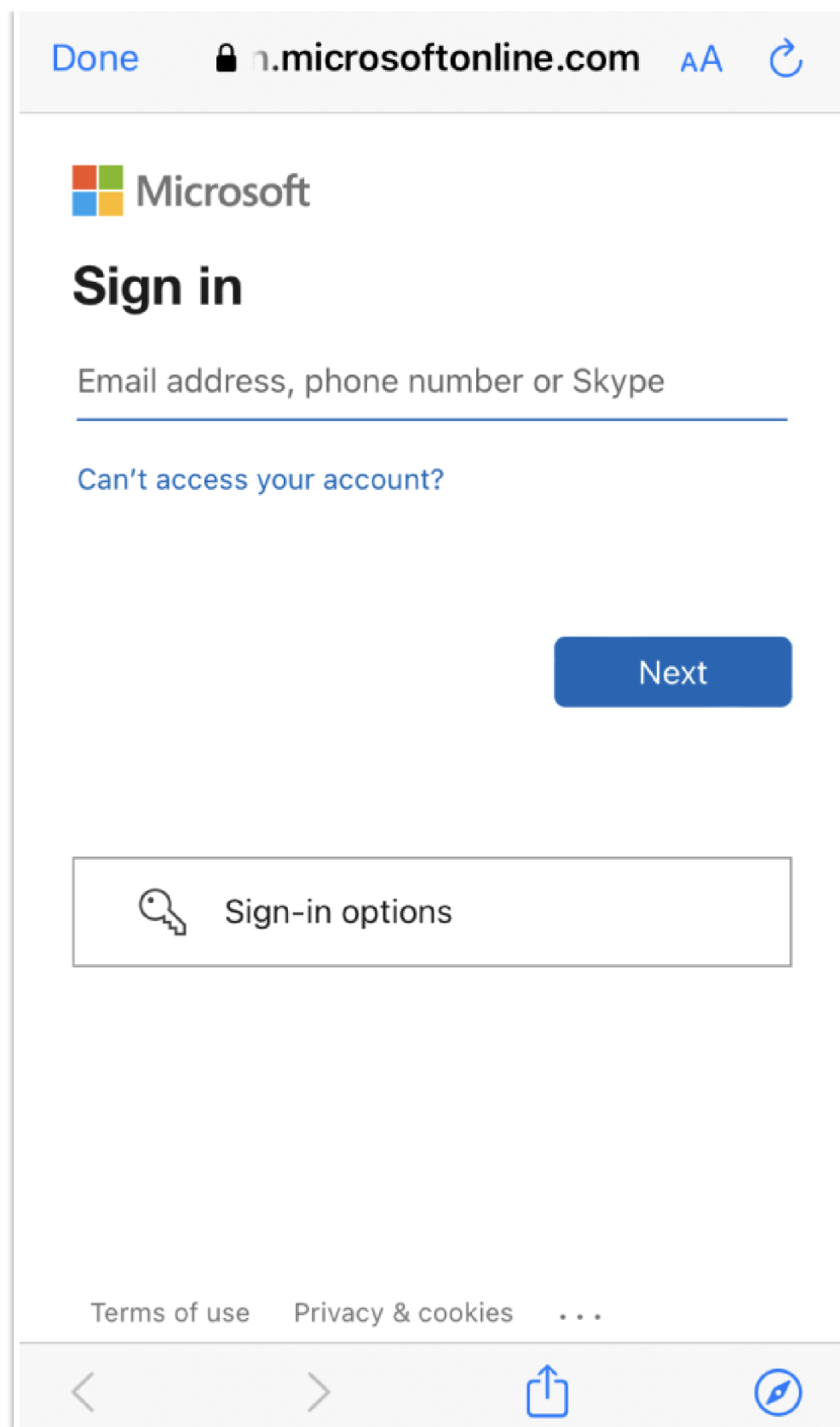
How to set up SSO for GDMS?

Sign In

Back

GDMS App Login

2. Go to the configured IdP service provider authentication page, such as Microsoft Azure, ADFS, and DUO.



Microsoft Authentication Page

3. After authentication, log in to the GDMS APP with the corresponding SAML SSO role.

IdP-Initiated Login Test

This test verifies authentication initiated directly from the Identity Provider portal.

In IdP-initiated authentication, the IdP generates the **SAML assertion** and redirects the user to the Service Provider without first accessing the GDMS or GWN Manager login page.

Important:

For IdP-initiated login to function correctly, the **Default Relay State** (or Relay State URL) must be configured in the IdP. This value must point to the base URL of the Service Provider (for example, *https://www.gdms.cloud* or *https://<gwn-manager-domain>:<port>*). Before testing, ensure the Relay State has been configured as described in the relevant IdP configuration section.

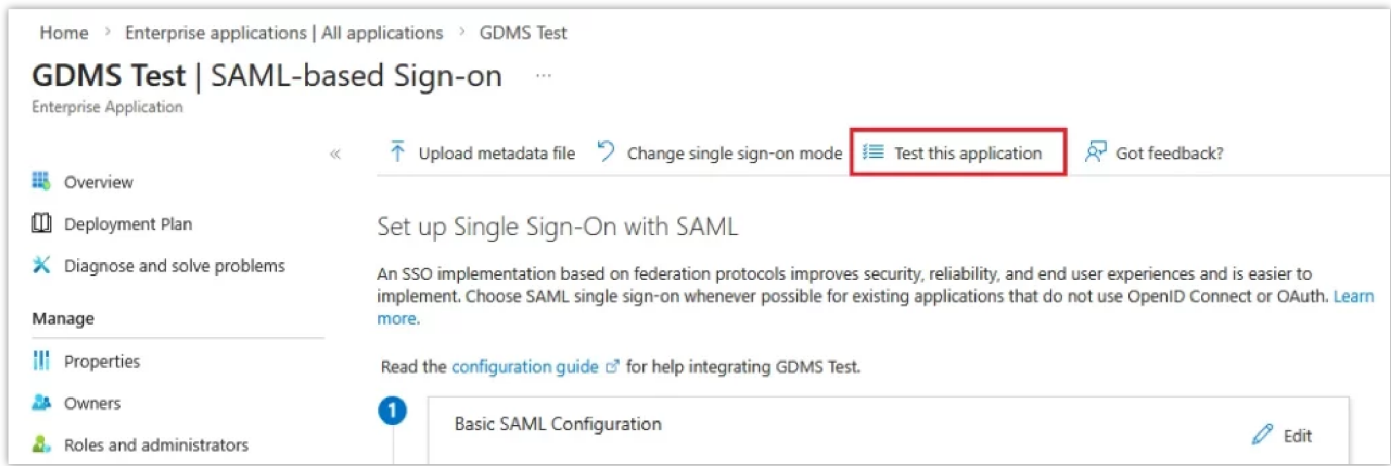
Microsoft Entra ID

SAML SSO can be validated from Microsoft Entra ID using either:

- The Application Test option
- The Microsoft MyApps portal

Access using the Application Test Option

1. Log in to the **Microsoft Entra Admin Center**.
2. Navigate to **Enterprise applications** and select the configured GDMS/GWN application.
3. Go to **Single Sign-on**→**SAML**.
4. Click **Test this application**.

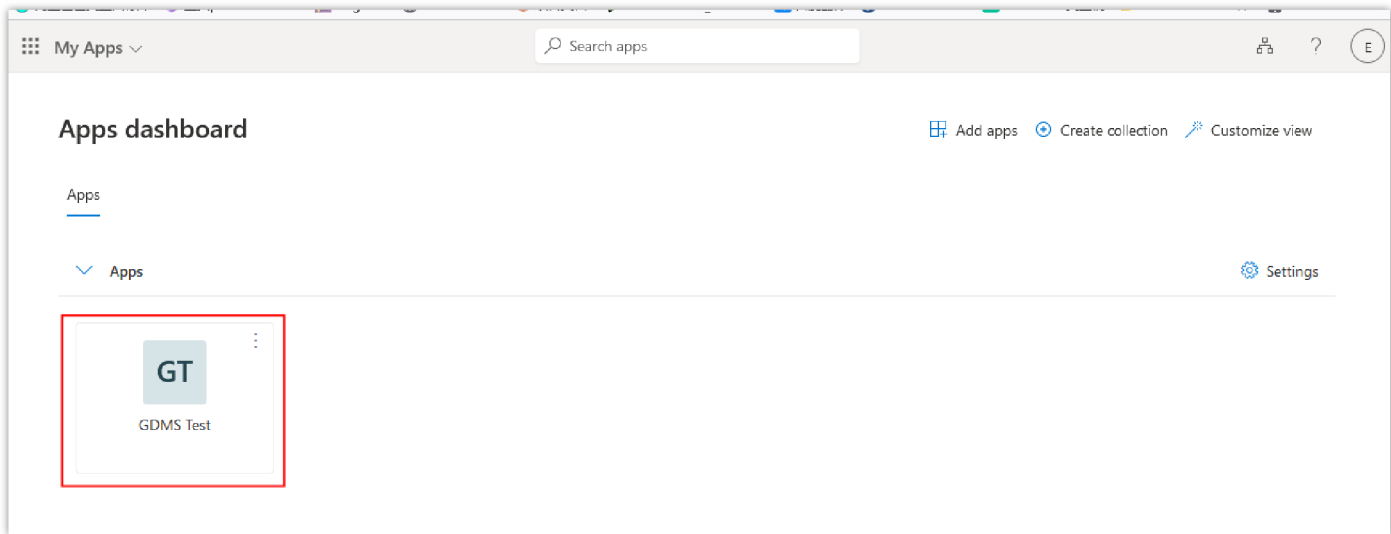


Testing Microsoft Entra ID Application

If the configuration is correct, the authentication completes successfully, and the browser redirects to GDMS or GWN Manager

Access from Microsoft MyApps Portal

1. Open [Microsoft MyApps](#).
2. Sign in using an Entra ID account with permission to access the GDMS/GWN application.
3. Click the configured GDMS/GWN application tile.
4. Authenticate if prompted, and verify successful redirection and correct role assignment.



Application Dashboard

For more information about the My Apps, see Introduction to [Microsoft My Apps](#).

AD FS

Before testing, verify that the IdP-initiated sign-on page is enabled on the AD FS server. Open PowerShell as Administrator and run:

```
Get-AdfsProperties | Select-Object EnableIdpInitiatedSignonPage
```

If the output shows *“False”*, enable it:

```
Set-AdfsProperties -EnableIdpInitiatedSignonPage $true
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-AdfsProperties | Select-Object EnableIdpInitiatedSignonPage

EnableIdpInitiatedSignonPage
-----
False

PS C:\Users\Administrator>
```

EnableIdpInitiatedSignonPage Output Shows False

Run the check command again to confirm the value now shows “True”.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-AdfsProperties | Select-Object EnableIdpInitiatedSignonPage

EnableIdpInitiatedSignonPage
-----
False

PS C:\Users\Administrator> Set-AdfsProperties -EnableIdpInitiatedSignonPage $true
PS C:\Users\Administrator> Get-AdfsProperties | Select-Object EnableIdpInitiatedSignonPage

EnableIdpInitiatedSignonPage
-----
True

PS C:\Users\Administrator>
```

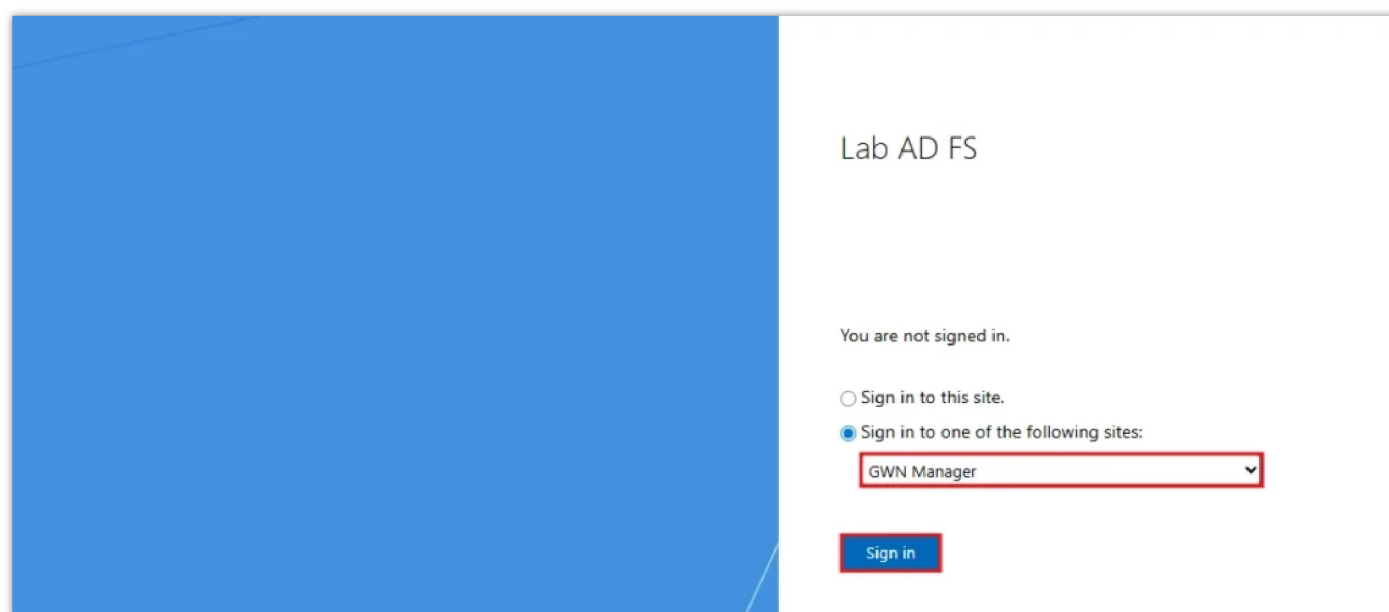
EnableIdpInitiatedSignonPage Output Shows True

Access via AD FS IdP Sign-On Page

1. Open a browser and navigate to:

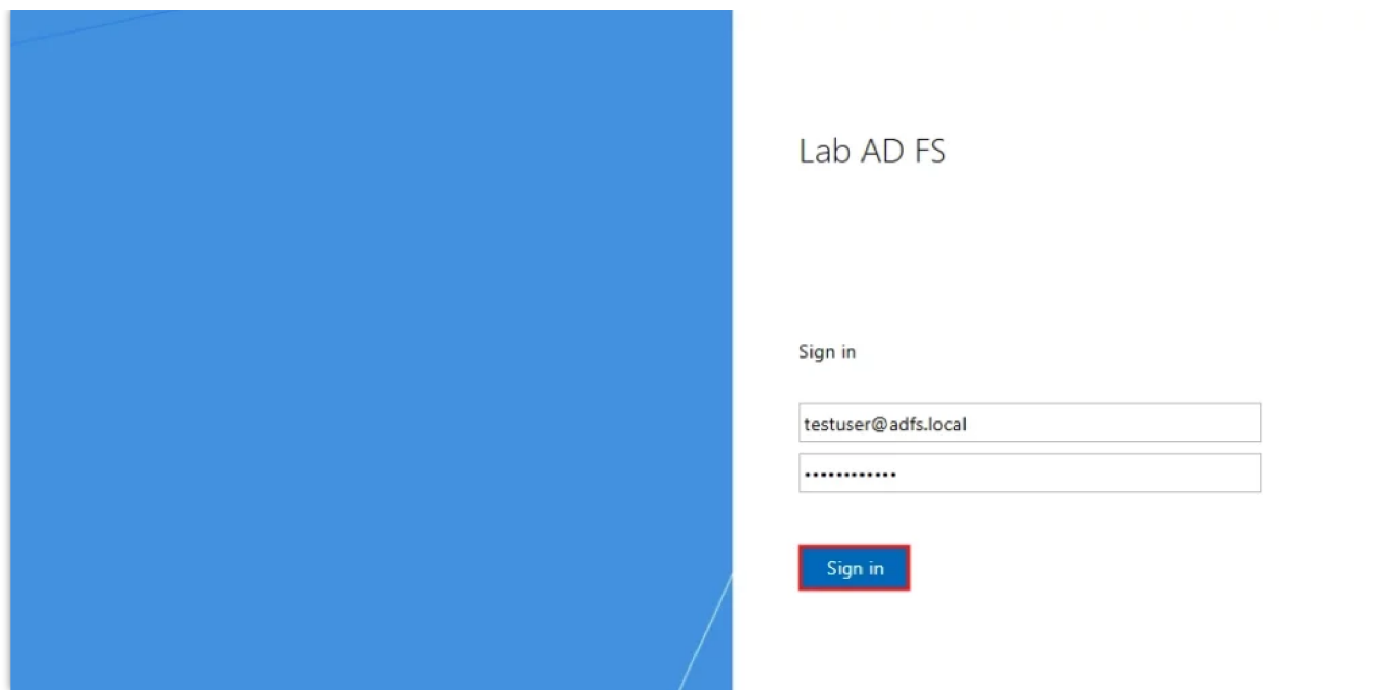
`https://<adfs-server>/adfs/ls/idpinitiatedsignon.aspx`

2. From the application dropdown, select the configured application (**GDMS** or **GWN Manager**).



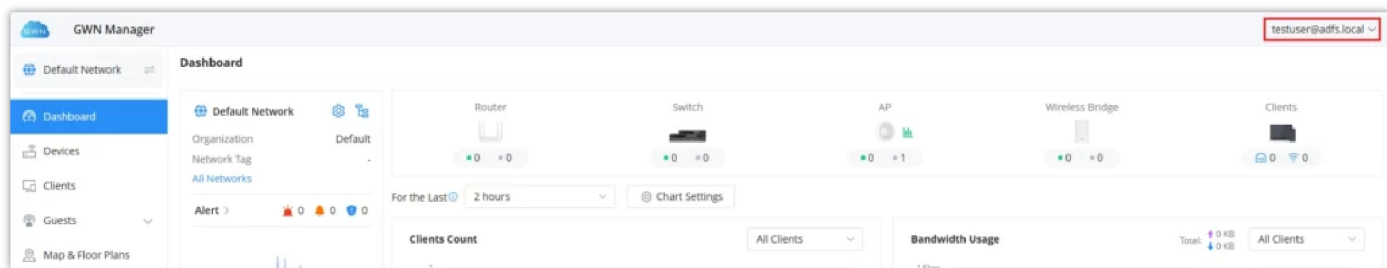
AD FS IdP Sign On Page Target Application

3. Sign in using a domain user account that is a member of the AD group mapped to the GDMS or GWN Manager SAML SSO role.



AD FS IdP Sign On Page Domain User Credentials

4. After successful authentication, verify that:
 - o The browser redirects to GDMS or GWN Manager automatically
 - o Login completes without prompting for the SSO Access Code
 - o The correct SAML SSO role is applied to the session



Successful IdP Initiated Login with AD FS User

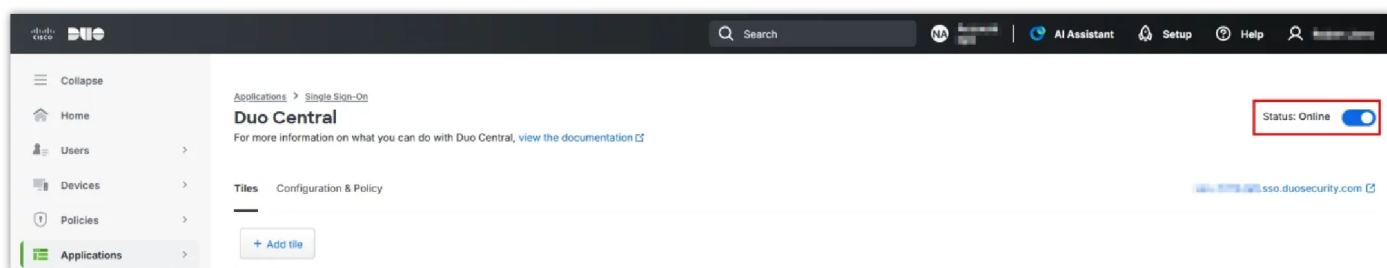
DUO

When Duo is configured as the SAML Identity Provider, IdP-initiated login can be performed using Duo Central or through the upstream identity provider (for example, Microsoft Entra ID).

Unlike Microsoft Entra ID, Duo does not automatically create a user application tile for SAML applications. Administrators must manually add the application to Duo Central.

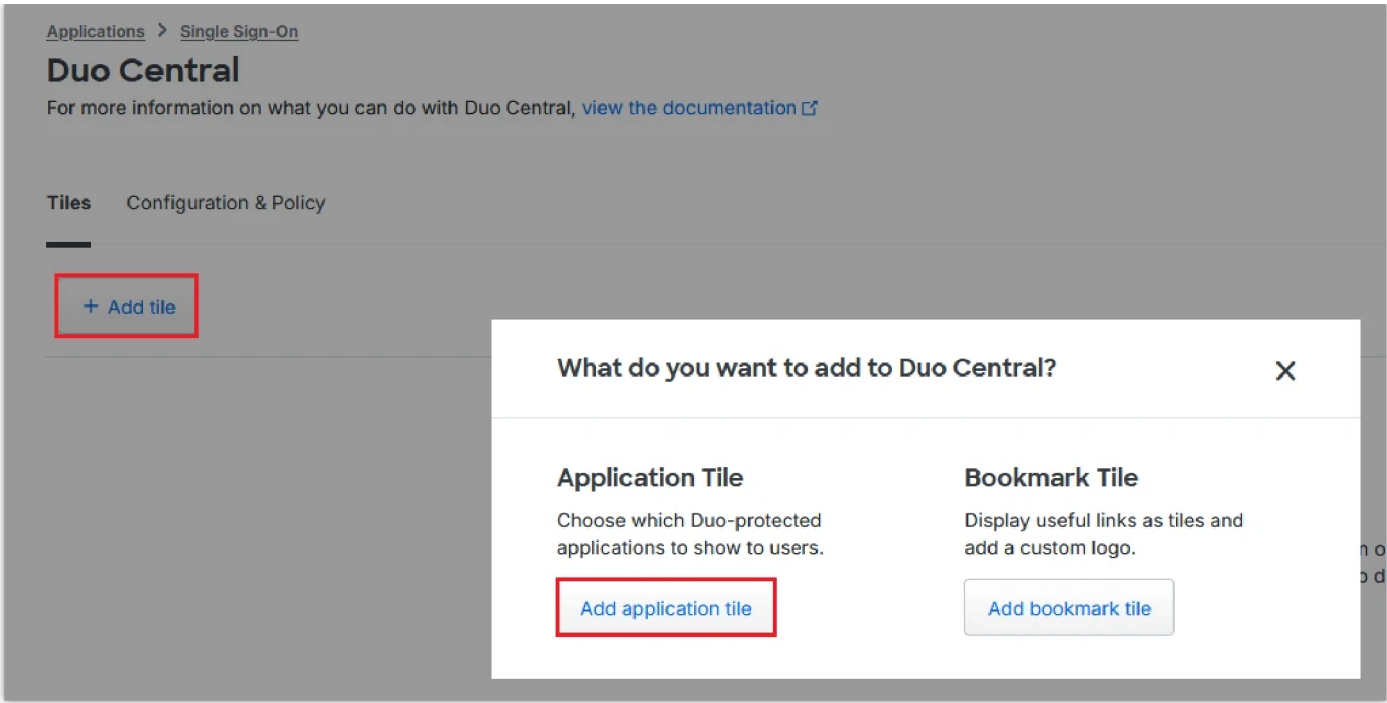
Access via Duo Central

1. Log in to the Duo Admin Panel.
2. Navigate to **Applications**→**Duo Central**.
3. Ensure the **Status** is set to **Online**. If Duo Central is Offline, tiles will not be available.



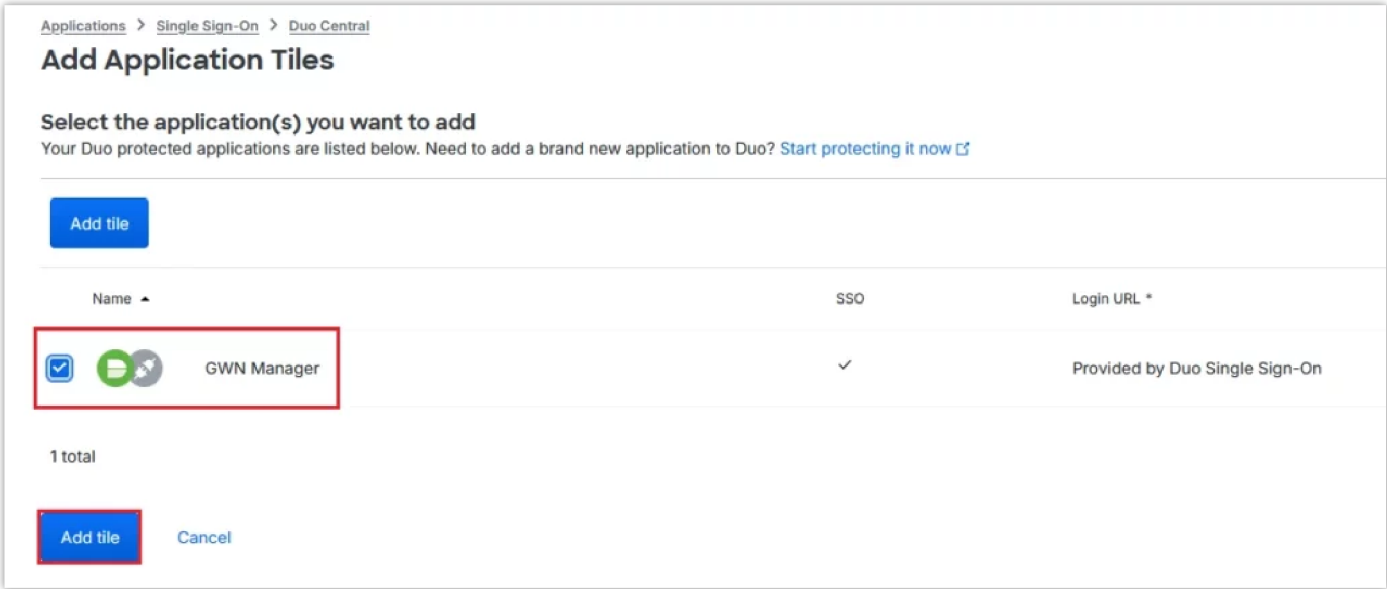
DUO Central Status

4. Click **Add tile**.
5. Select **Add application tile**.



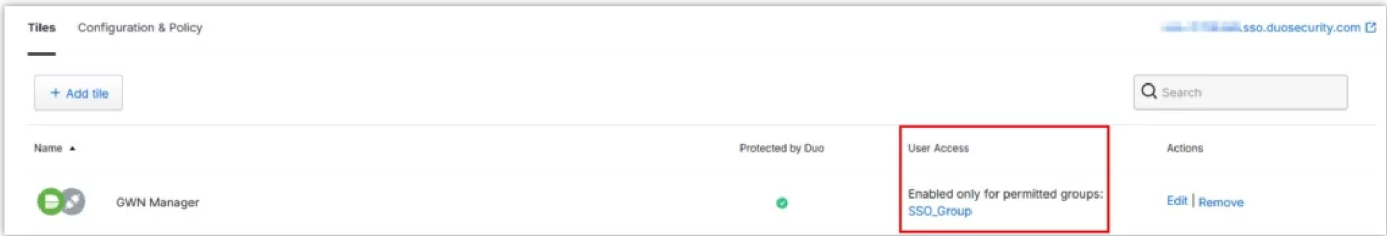
Adding Application Tile on DUO

- 6. Locate the configured **SAML application** (for example, GDMS or GWN Manager).
- 7. Select the checkbox next to the application.
- 8. Click **Add Tile**.



Adding Tile for GWN Manager Application on DUO

- 9. The application will now appear in the Duo Central Tiles list. Confirm the application tile shows *Enabled only for permitted groups*, or *Available to all users*.



User Access Permission or GWN Manager App

Once the tile has been successfully configured, users can follow these steps to log in from DUO Central:

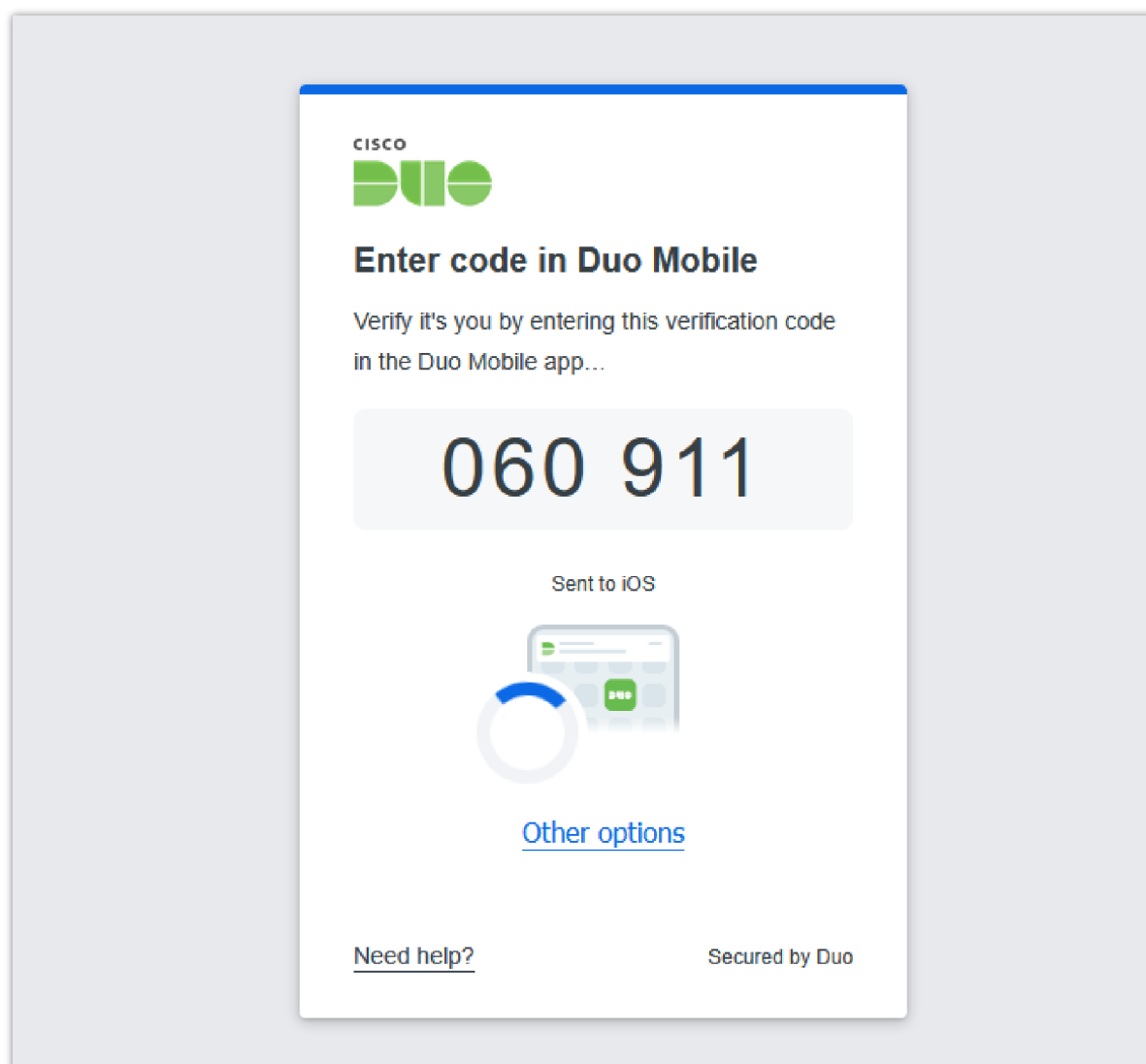
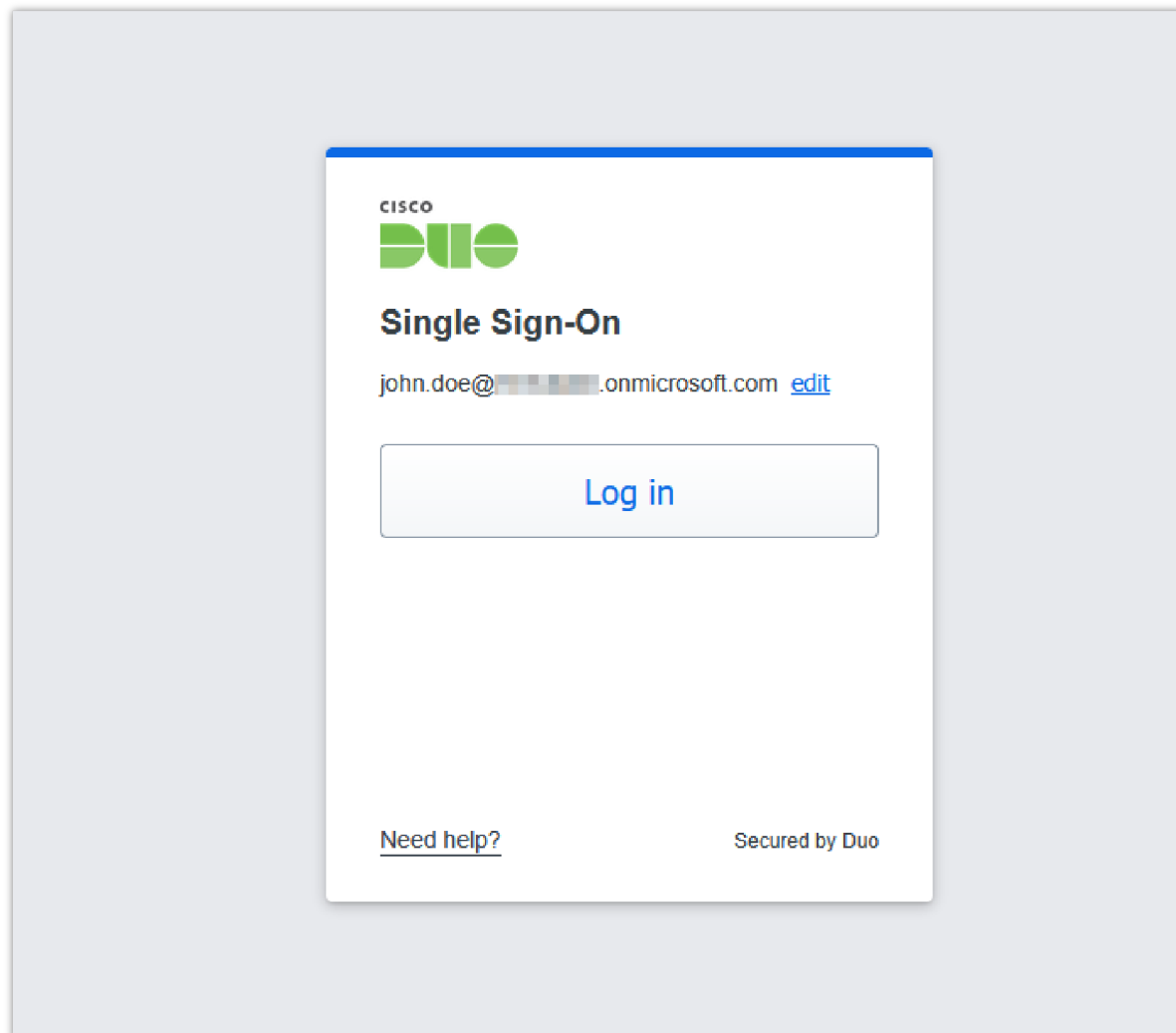
- 1. Open a browser and navigate to the Duo Central portal:

`https://<your-subdomain>.sso.duosecurity.com`

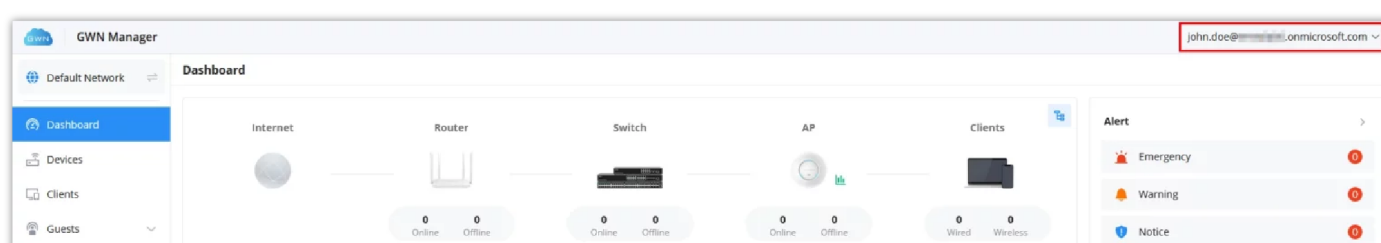
- 2. Sign in using a user account with access to the configured SAML application.
- 3. After login, the application tile will be displayed.



- Click the application tile to initiate IdP-initiated SAML authentication.
- Enter valid credentials and complete Duo MFA verification if required.



- After successful authentication, you will be redirected to the configured GDMS or GWN Manager and logged in automatically.



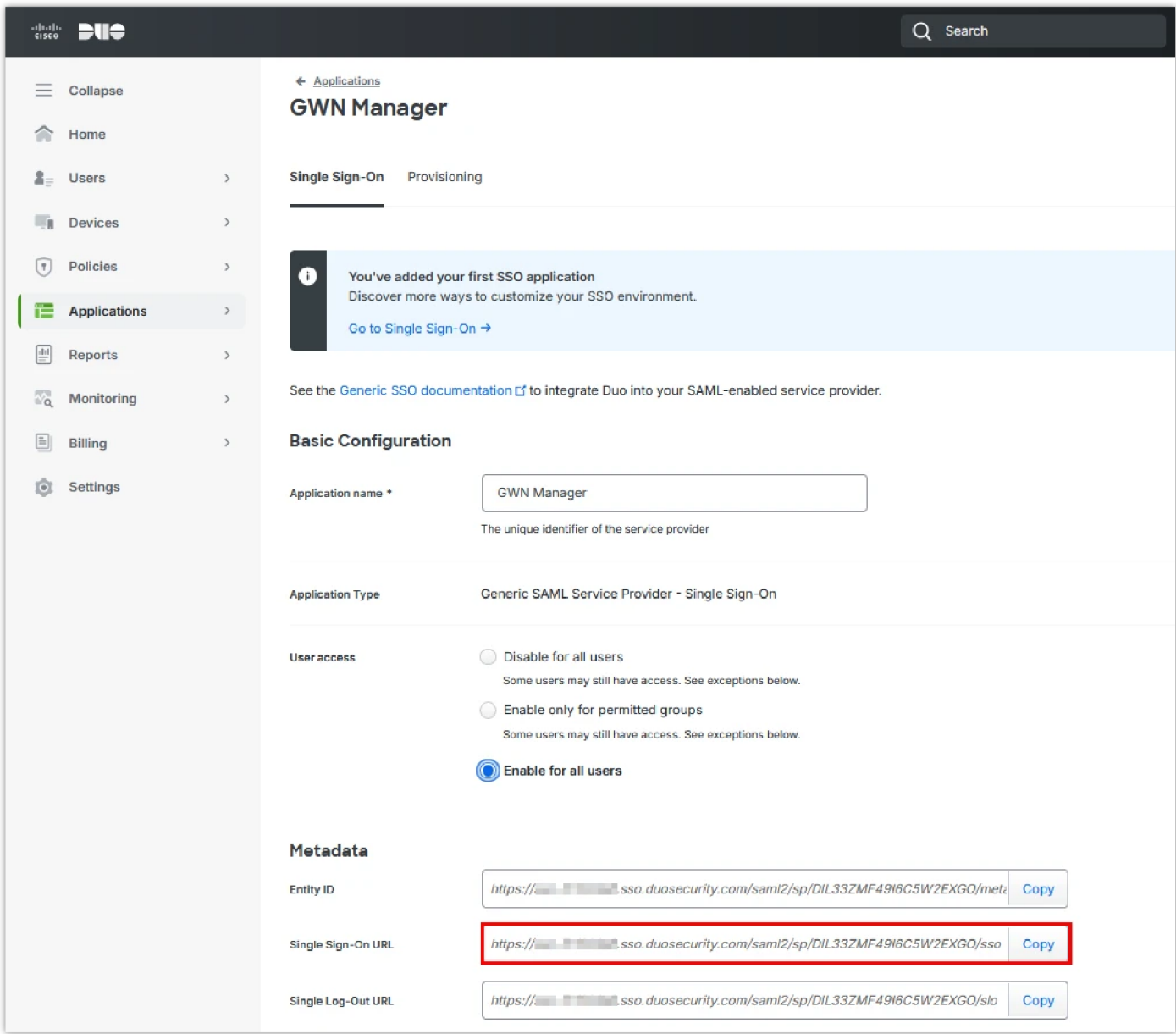
GWN Manager Successful Login from Duo

Access via Upstream IdP (Entra ID)

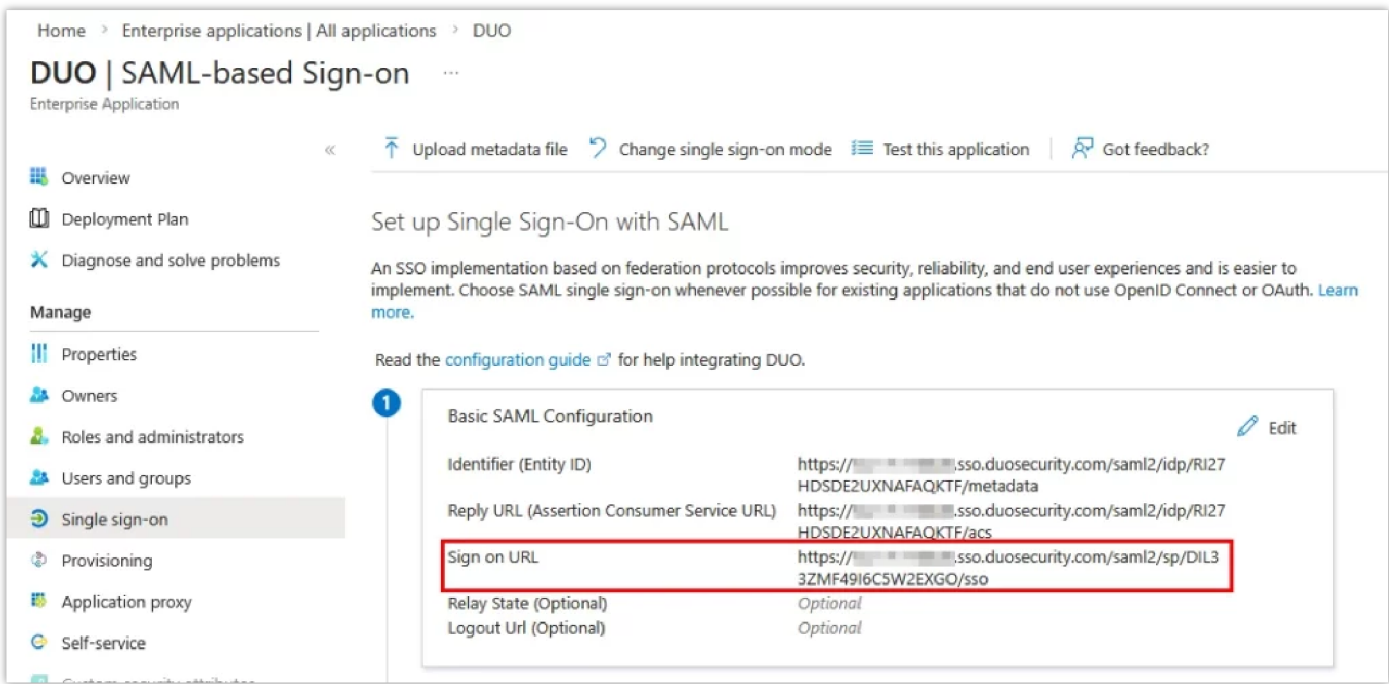
When Duo uses Microsoft Entra ID as the upstream identity provider, users may also initiate login from Microsoft MyApps.

For IdP-initiated login to work correctly in this scenario, the **Sign-on URL** must be configured in the Entra ID application.

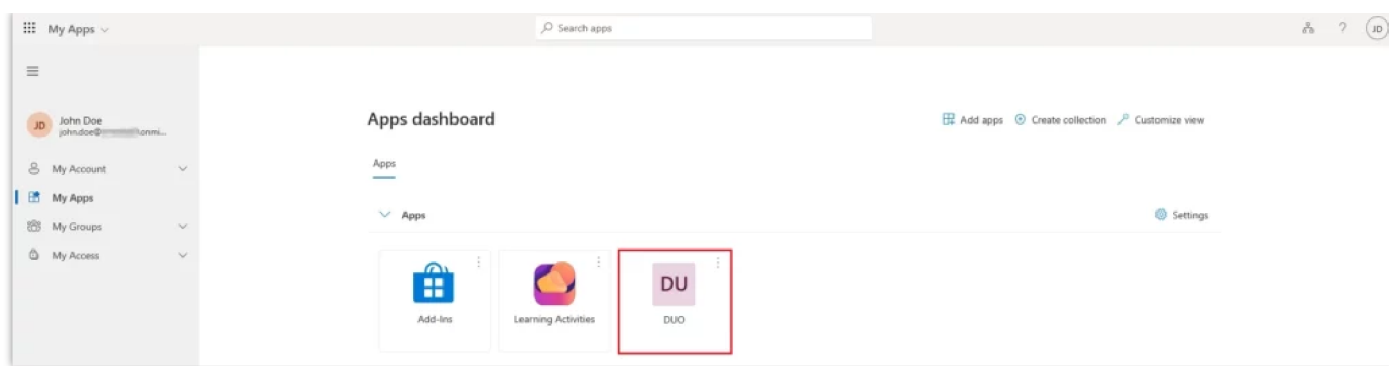
- 1. Log in to the **Duo Admin Panel**.
- 2. Open the configured SAML application and copy the Single Sign-On URL from the application metadata.



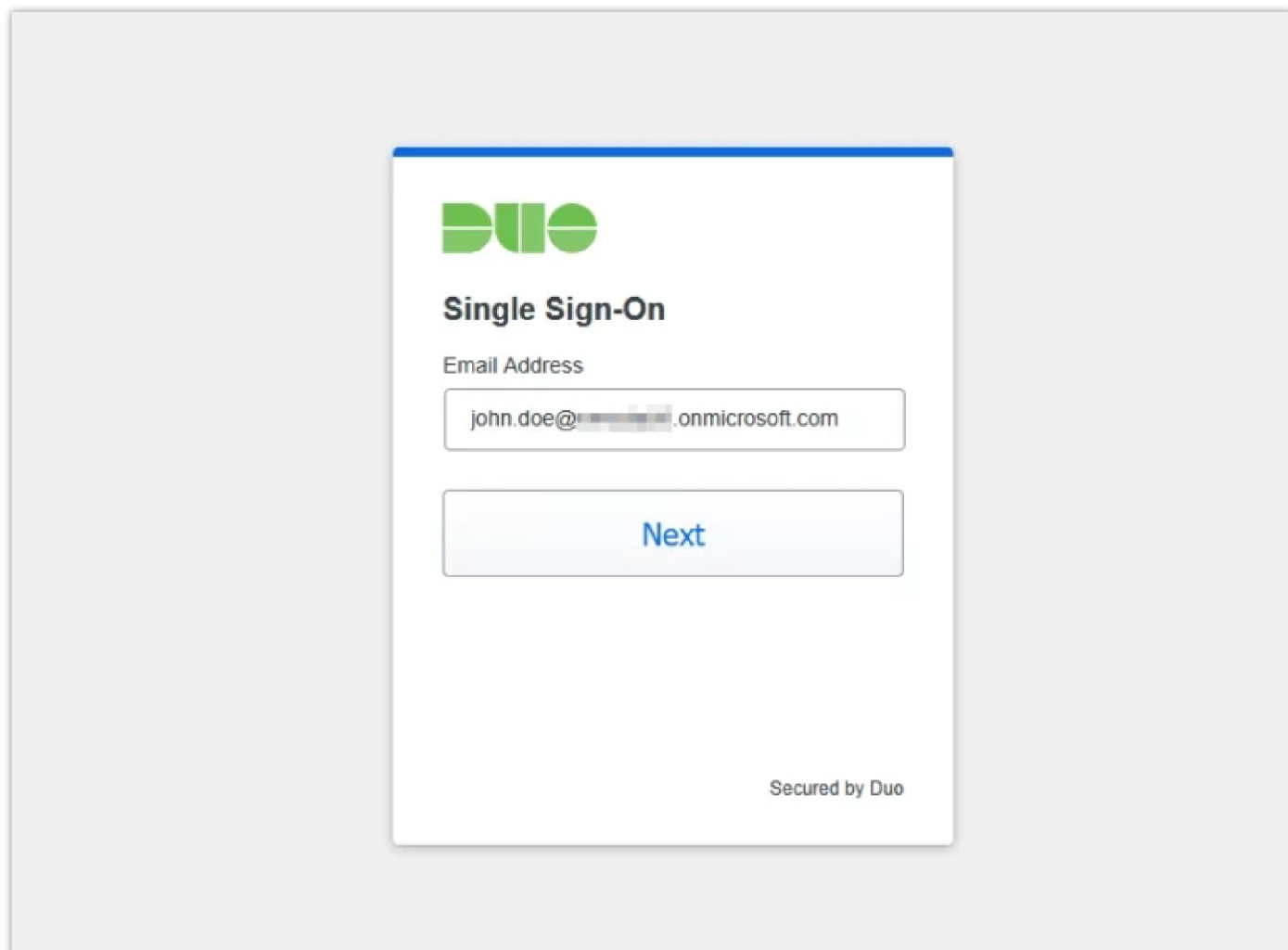
- 3. Log in to the Microsoft Entra Admin Center.
- 4. Navigate to the Duo application created earlier.
- 5. Under Basic SAML Configuration, paste the copied URL into the Sign-on URL field.



- 6. Open **Microsoft MyApps**, and sign in using the Microsoft Entra ID account configured in Duo.
- 7. Click the Duo application tile.



8. The browser redirects to the Duo authentication page. Enter the correct credentials and complete Duo MFA verification.



If the configuration is correct, the browser redirects to GDMS or GWN Manager, and the user is automatically logged in with the appropriate role.

SAML SSO LOGS

Administrators can review authentication activity for SAML SSO users using system logs, which can be reviewed in the following systems:

- GDMS
- GWN Manager
- Microsoft Entra ID
- AD FS
- Duo

Reviewing logs from both the Service Provider and Identity Provider can help identify configuration or authentication issues.

Viewing Logs in GDMS

GDMS records SAML login and logout events in the System Log.

1. Log in to GDMS using an administrator account.
2. Access the Account Center logs using one of the following paths, depending on the module in use:
 - **UC Module:** Navigate to **System**→**System Log**→**Account Center**.
 - **Networking Module:** Navigate to **Organization**→**Change Log**→**Account Center**.

GDMS Unified Communications

Plans & ServicesWorldyxxu123

DashboardOrganizationDefaultVoIP DeviceCall QualityDevice TemplateSiteTaskDiagnosticsSystemResourcesAlertsReseller ChannelRPS ManagementUsersSystem LogAPI Developer

System Log

System LogAccount Center

All LevelsAll OperationsOperator / IPFilter

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...	192.168.126.122	Notice	Sign Out
2024/10/31 20:17	h...	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 10110/page123456...11

© 2024 Grandstream Networks, Inc. Cookies

GDMS SAML SSO Logs

Viewing Logs in GWN Manager

GWN Manager also records SAML authentication events in its system log.

- 1. Log in to GWN Manager using an administrator account.
- 2. Navigate to **Organization→Change Log→Account Center**.

GWN Manageradmin

Default NetworkDashboardDevicesClientsGuestsMap & Floor PlansInsightAlertsSettingsOrganization

Change Log

System LogAccount Center

2026-02-042026-03-06Operator / IP

Time	Operator	IP Address	Details
2026-03-06 14:49	admin	192.168.5.194	Login success
2026-03-06 14:49	admin	192.168.5.194	Login failed 1 times (Password error)
2026-03-06 14:49	john.doe@...onmicrosoft.com	192.168.5.194	Sign Out
2026-03-06 14:40	sarah.grey@...onmicrosoft.com	192.168.5.194	Login success
2026-03-06 14:39	admin	192.168.5.194	Sign Out
2026-03-06 14:25	admin	192.168.5.194	Login success
2026-03-06 14:25	admin	192.168.5.194	Login failed 1 times (Password error)
2026-03-06 13:33	angela.wright@...onmicrosoft.com	192.168.5.194	Login success
2026-03-06 12:27	john.doe@...onmicrosoft.com	192.168.5.194	Sign Out
2026-03-06 12:27	john.doe@...onmicrosoft.com	192.168.5.194	Login success

GWN Manager SAML SSO Logs

Viewing Logs in Microsoft Entra ID

Microsoft Entra ID records SAML authentication activity in the Sign-in Logs.

- 1. Log in to the **Microsoft Entra Admin Center**.
- 2. Under Enterprise Applications, select the service provider app.
- 3. Navigate to **Identity→Monitoring→Sign-in logs**.

HomeEnterprise applicationsAll applicationsDUO

DUO | Sign-in logs

DownloadExport data SettingsTroubleshootRefreshManage viewGot feedback?

Want to switch back to the legacy sign-in logs experience? Click here to leave the preview.

Add filterShow dates as: UTCDate range: Last 24 hoursApplication contains 14a4e350-f8c7-4b77-a75d-1b49f42a0322Reset filters

User sign-ins (interactive)

User sign-ins (non-interactive)

Service principal sign-ins

Managed identity sign-ins

Date	Request ID	User principal name	Application	Status	IP address	Resource	Resource ID
2026-03-06T11:36:08Z	449dc49f-57c0-4282-a0d0-198fe...	john.doe@...on...	DUO	Success	...	Windows Azure Active ...	00000002-0
2026-03-06T11:33:14Z	a63e640-fe06-4801-bac1-1478...	angela.wright@...	DUO	Success	...	Windows Azure Active ...	00000002-0
2026-03-06T09:53:02Z	13503163-da2c-48c3-be50-2b79...	sarah.grey@...o...	DUO	Success	...	Windows Azure Active ...	00000002-0

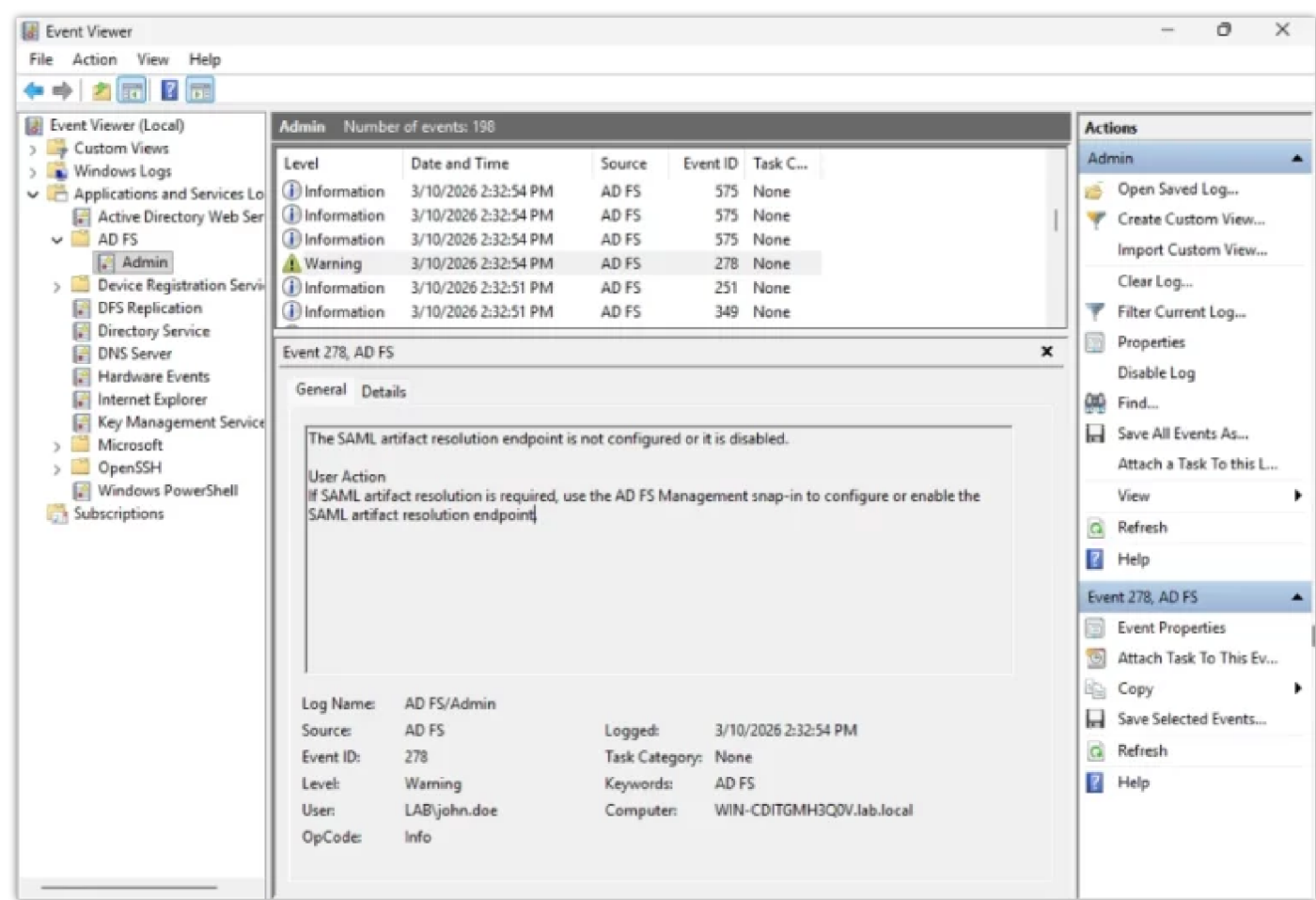
Microsoft Entra ID SAML SSO Logs

Viewing Logs in AD FS

When AD FS is used as the Identity Provider, SAML authentication events are recorded in the Windows Event Viewer.

1. Log in to the AD FS server, open **Event Viewer** by running eventvwr.msc or searching for “Event Viewer” in the Start menu.
2. In the left pane, navigate to **Applications and Services Logs→AD FS→Admin**.
3. Review the events listed.

You can use the Find function to reach for “SAML” events.

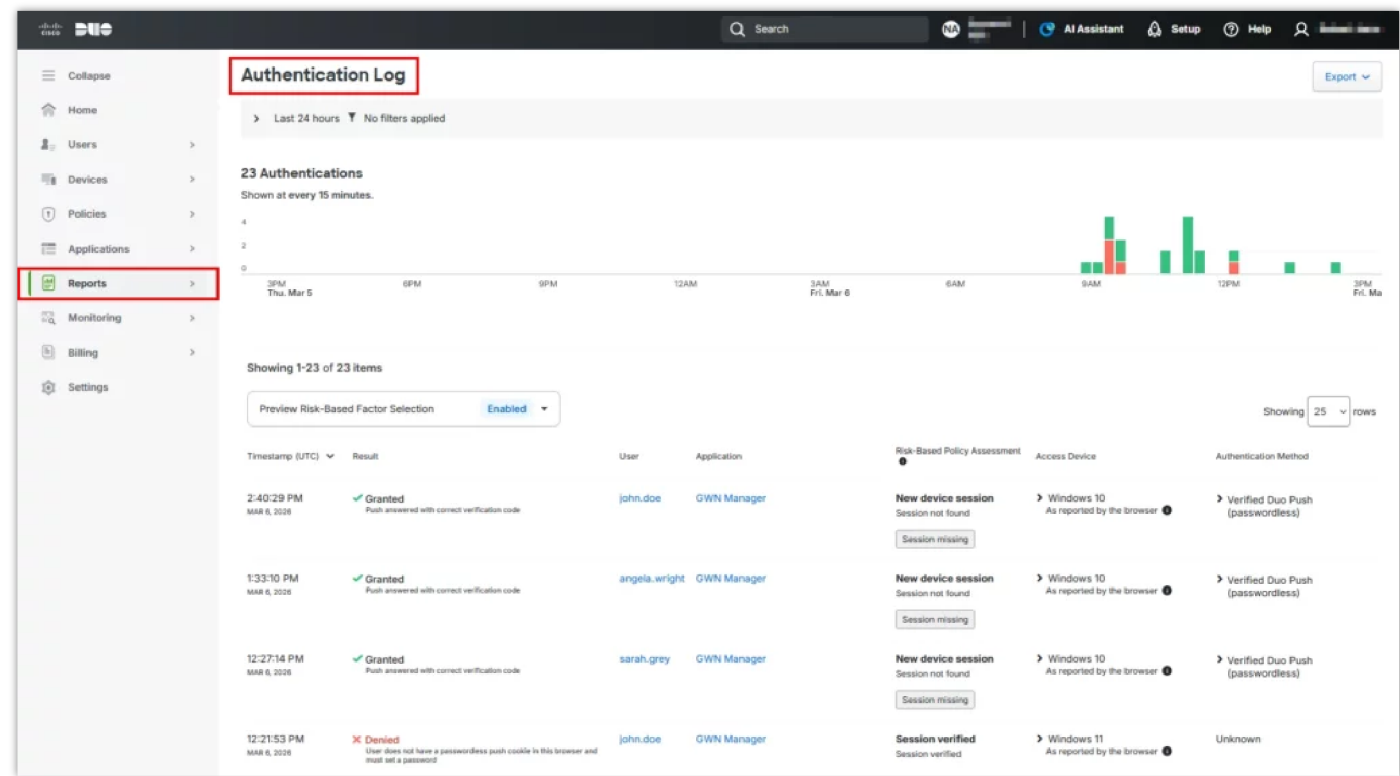


AD FS SAML SSO Logs

Viewing Logs in Duo

Duo records authentication activity in the Authentication Log, which includes SAML authentication events.

1. Log in to the Duo Admin Panel.
2. Navigate to **Reports→Authentication Log**.
3. Use the search filters to locate events related to the configured SAML application.



DUO SAML SSO Logs