https://cloudblue.com

Documentation Modules Account Settings Single Sign-On

Azure Active Directory

This article has been generated from the online version of the documentation and might be out of date. Please, make sure to always refer to the online version of the documentation for the up-to-date information.

Auto-generated at February 12, 2026

Azure Active Directory represents an Identity and Access Management as a service (IDaaS) solution that can be used as your Single Sign-On domain on the CloudBlue Connect platform.

The following provides instructions on how to deploy your configured Azure Active Directory on the Connect platform. The guidelines below also showcase how to create a new Active Directory on the Microsoft Azure portal, how to successfully configure your Azure enterprise application, and more.

Active Directory Creation

Create your Azure Active Directory via the Microsoft Azure Portal as described below. Skip to Connect Domain Verification in case your Active Directory and custom domain are already configured on the Microsoft Azure portal.

By creating an Active Directory, the Microsoft Azure portal requires you to specify your tenant details. A tenant represents an organization and dedicated instance of Azure AD. The following steps showcase how to successfully create a new Azure Active Directory and configure your new tenant:

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

1. Click the **Create New Resource** button from the **Microsoft Azure** portal.
2. Locate *Azure Active Directory* from the provided list.

3. Click the **Create** button once Azure Active Directory is located successfully.
4. The portal prompts you to select a tenant type. Specify your required type and click **Next: Configuration** to continue.
5. Specify your organization name, initial domain name, and country/region in the following **Configuration** form. Click **Next: Review + create** to continue.
6. Once your configured tenant validation is passed, click the **Create** button to finalize your Active Directory creation.

Therefore, the Azure portal starts to process your tenant configuration. In case this processing is successfully complete, the Azure portal allows you to access your created Active Directory.

Azure Custom Domain

Verify your domain name within your Azure Active Directory. Skip to Connect Domain Verification in case your custom domain is already configured on the Microsoft Azure portal.

Follow the steps below to add your custom domain to your Azure Active Directory and successfully verify it.

Step 1

Step 2

Step 3 & 4

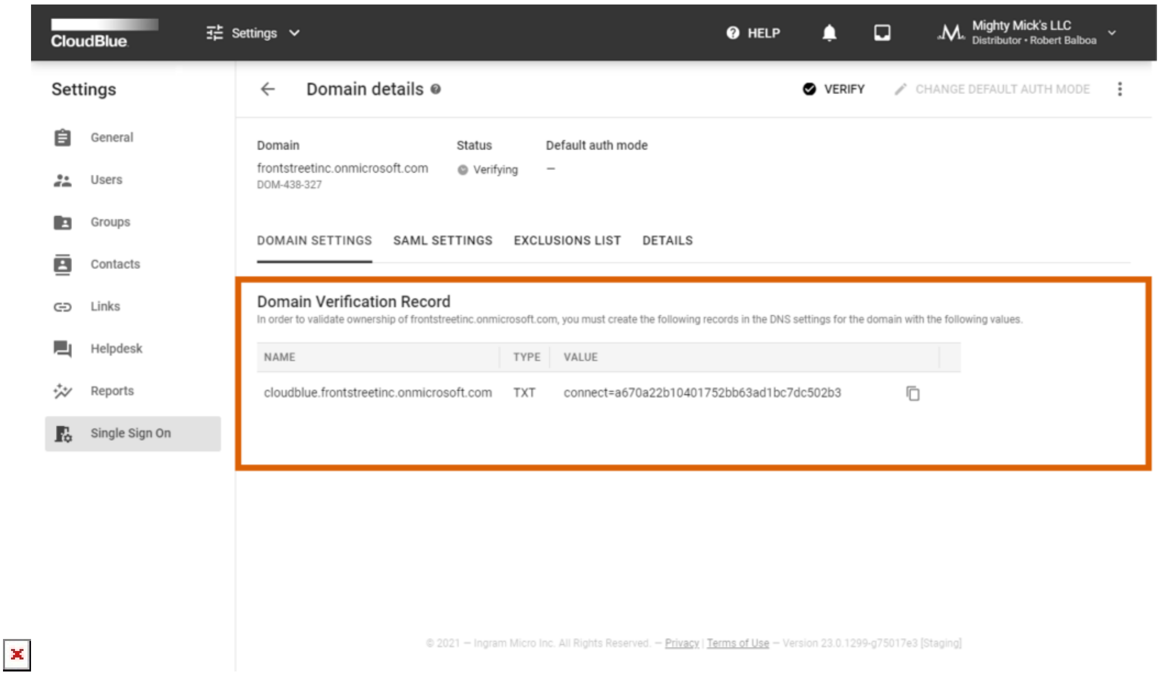
1. Access the **Custom Domain Names** section from the left-hand panel of your created Azure Active Domain.
2. Click the **Add custom domain** button to specify your domain name.
3. Enter your domain to the appeared form and click the **Add domain** button.
4. The Azure portal prompts you to specify create a new TXT record with your domain name registrar using the provided information. Click **Verify** once your TXT with required information is successfully created.

As a result, the Azure portal starts to process your domain configuration. If this processing is complete, the Azure portal will successfully verify your added domain.

Connect Domain Verification

Create a domain on the CloudBlue Connect platform. Once your domain instance is created, Connect prompts users to create a domain verification record via the domain details screen.

Create an Azure Active Directory record set with required data as follows:



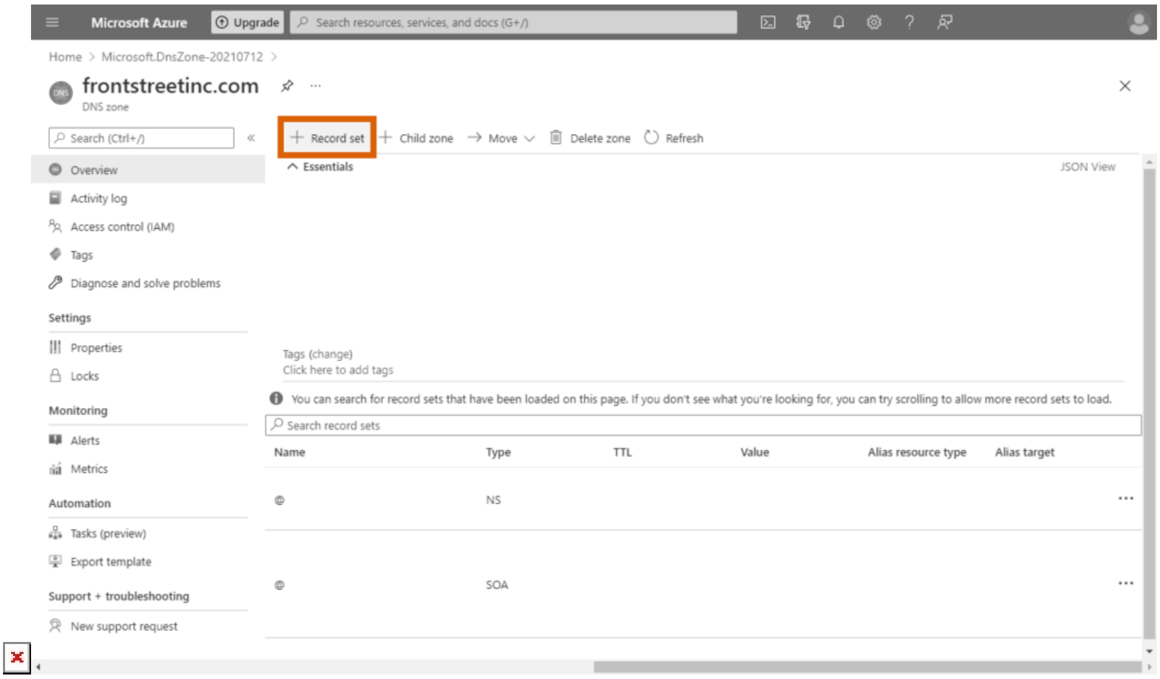
Domain: frontstreetinc.onmicrosoft.com
DOM-438-327
Status: Verifying
Default auth mode: –

Domain Verification Record

In order to validate ownership of frontstreetinc.onmicrosoft.com, you must create the following records in the DNS settings for the domain with the following values.

NAME	TYPE	VALUE
cloudblue.frontstreetinc.onmicrosoft.com	TXT	connect=a670a22b10401752bb63ad1bc7dc502b3

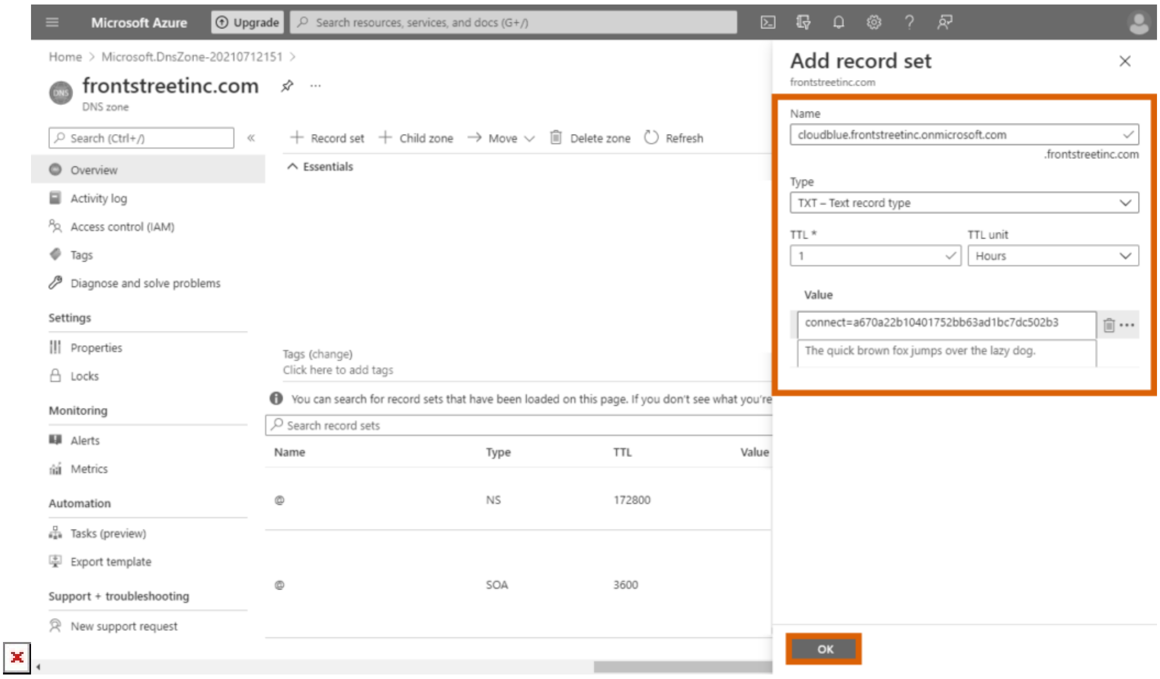
Step 1



You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Name	Type	TTL	Value	Alias resource type	Alias target
@	NS				
@	SOA				

Step 2



You can search for record sets that have been loaded on this page. If you don't see what you're

Search record sets

Name	Type	TTL	Value
@	NS	172800	
@	SOA	3600	

Add record set
frontstreetinc.com

Name: cloudblue.frontstreetinc.onmicrosoft.com
.frontstreetinc.com

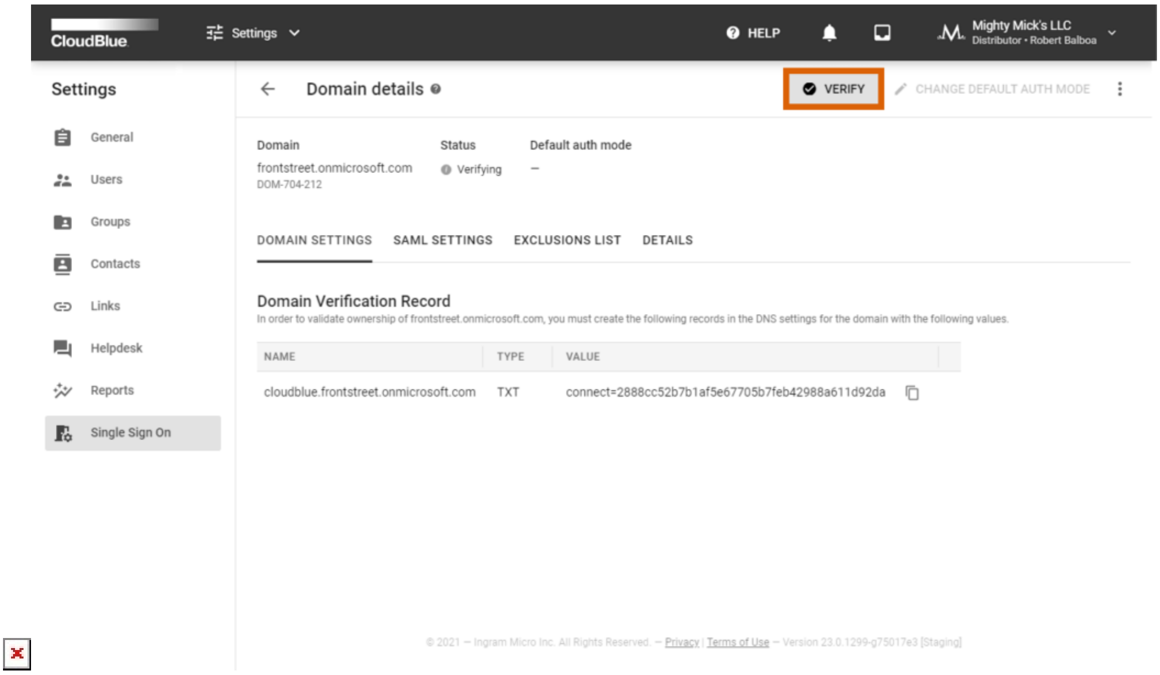
Type: TXT – Text record type

TTL *: 1

TTL unit: Hours

Value: connect=a670a22b10401752bb63ad1bc7dc502b3
The quick brown fox jumps over the lazy dog.

Step 3 & 4



Domain details

Domain: frontstreet.onmicrosoft.com
DOM-704-212

Status: Verifying

Default auth mode: –

Domain Verification Record

In order to validate ownership of frontstreet.onmicrosoft.com, you must create the following records in the DNS settings for the domain with the following values.

NAME	TYPE	VALUE
cloudblue.frontstreet.onmicrosoft.com	TXT	connect=2888cc52b7b1af5e67705b7feb42988a611d92da

© 2021 – Ingram Micro Inc. All Rights Reserved. – Privacy | Terms of Use – Version 23.0.1299-g75017e3 [Staging]

Step 5

1. Copy your provided domain and value from the **Domain Settings** tab on Connect.
2. Create a new **Record Set** within the DNS zone section on the Microsoft Azure portal.

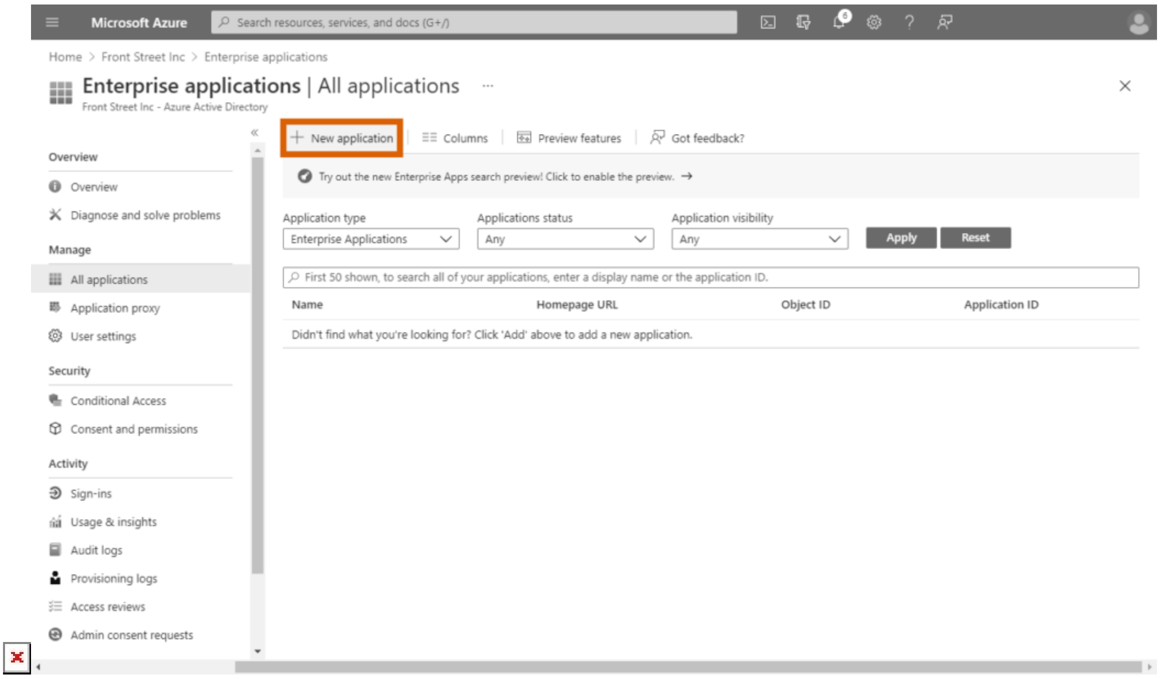
3. Paste your copied domain and value to the appeared form. Note that it is also necessary to specify a record type as displayed within *Domain Settings* on Connect.
4. Click **OK** to save your record configurations.
5. Verify your domain on the Connect platform by clicking the **Verify** button at the top right corner of your domain details screen.

Thus, the system should successfully verify your domain instance on the Connect platform. Note, however, that sometimes DNS changes can take a while to appear. Please wait a few hours, then reopen your domain instance and try to verify it again. In case the verification operation keeps failing, try to add a different DNS TXT record and make sure that all provided values are correct.

> ●
>
> One Domain & Multiple Accounts
>
> In case you have the same domain for two different Connect accounts (e.g., one domain for Vendors and Distributors), it is required to add two DNS records for each domain instance on the Connect platform.

Enterprise Application

In case your Active Directory is successfully configured and your domain is successfully on the Connect platform , it is necessary to define your single sign-on system via the *Enterprise applications* section on the Microsoft Azure portal and upload your Connect *Service Provider* metadata and certificate files to the Azure portal. The following instructions showcase how to perform the aforementioned operations:



Enterprise applications | All applications

Front Street Inc - Azure Active Directory

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application type: Enterprise Applications

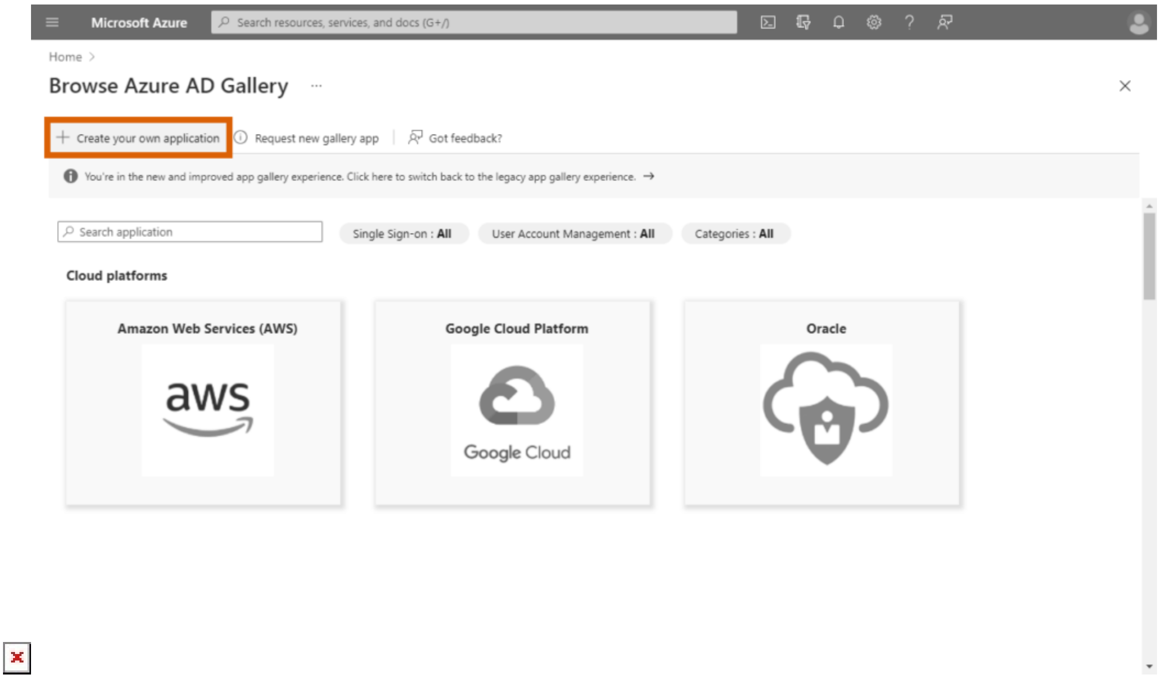
Applications status: Any

Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

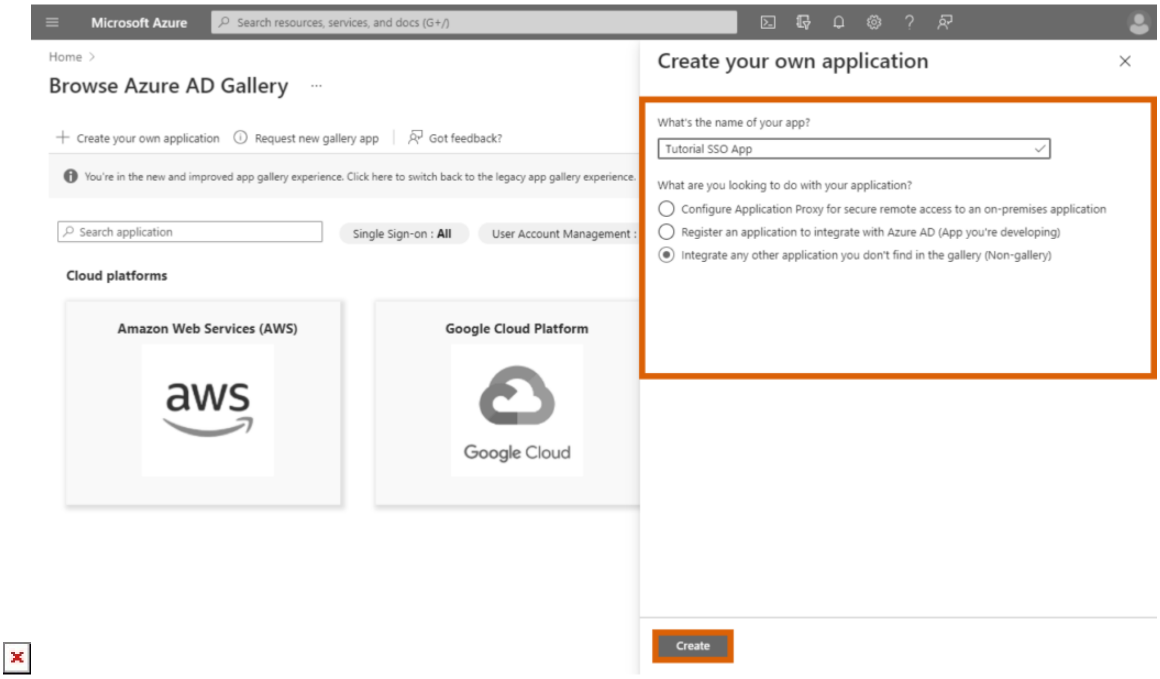
Name	Homepage URL	Object ID	Application ID
Didn't find what you're looking for? Click 'Add' above to add a new application.			

Step 1



You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

Step 2



You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience.

Create your own application

What's the name of your app?

Tutorial SSO App

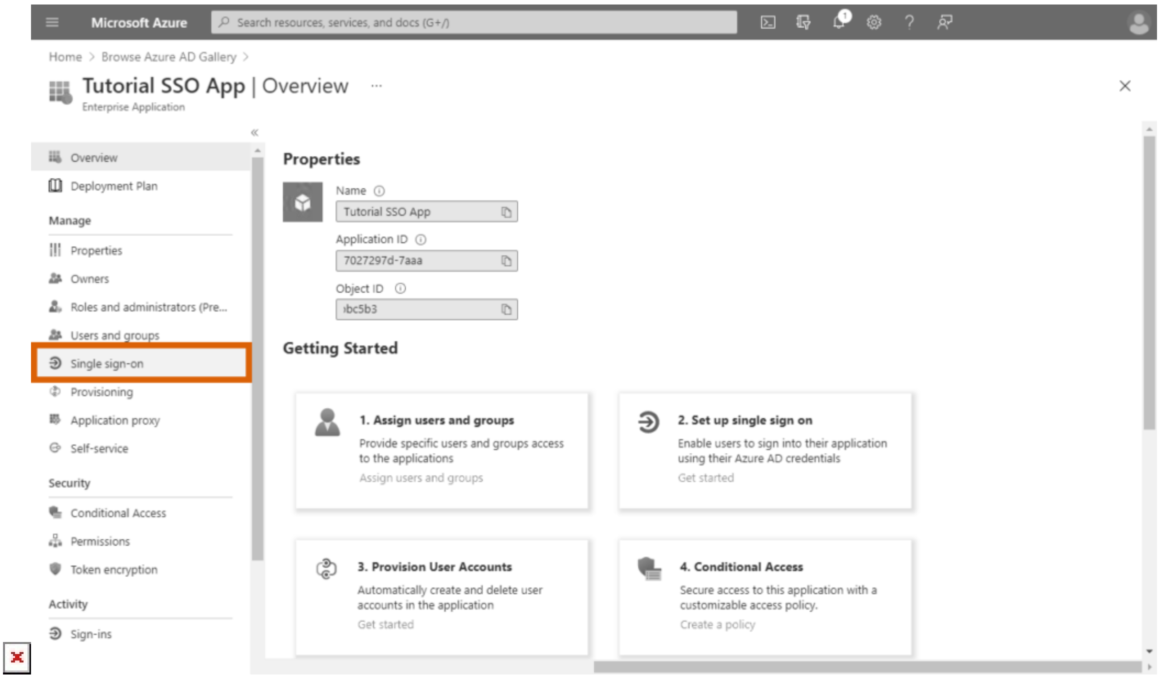
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

Step 3



Name: Tutorial SSO App

Application ID: 7027297d-7aaa

Object ID: ›bc5b3

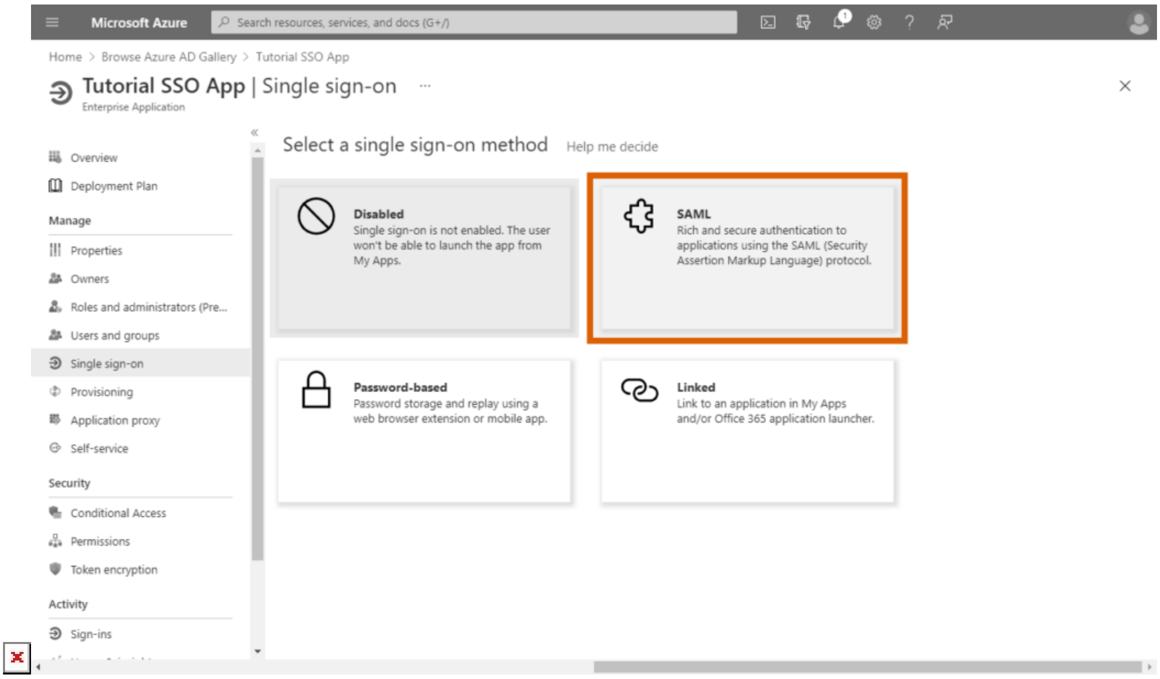
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

Step 4



Select a single sign-on method

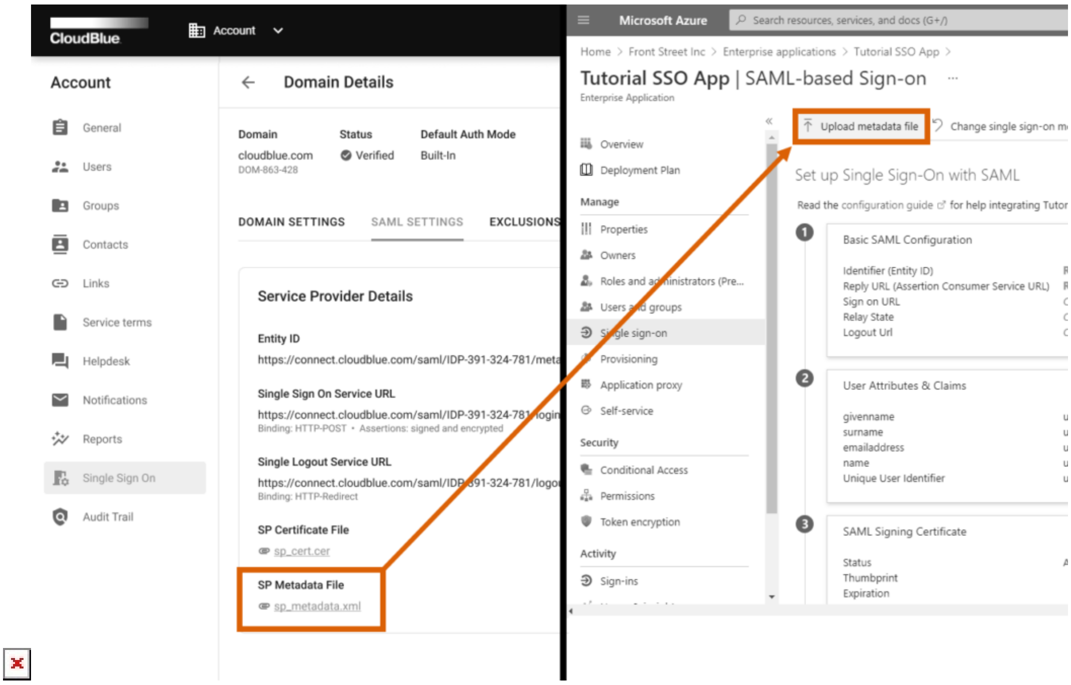
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

Step 5



Domain: cloudblue.com
DOM-863-428

Status: Verified

Default Auth Mode: Built-In

Service Provider Details

Entity ID
https://connect.cloudblue.com/saml/IDP-391-324-781/meta

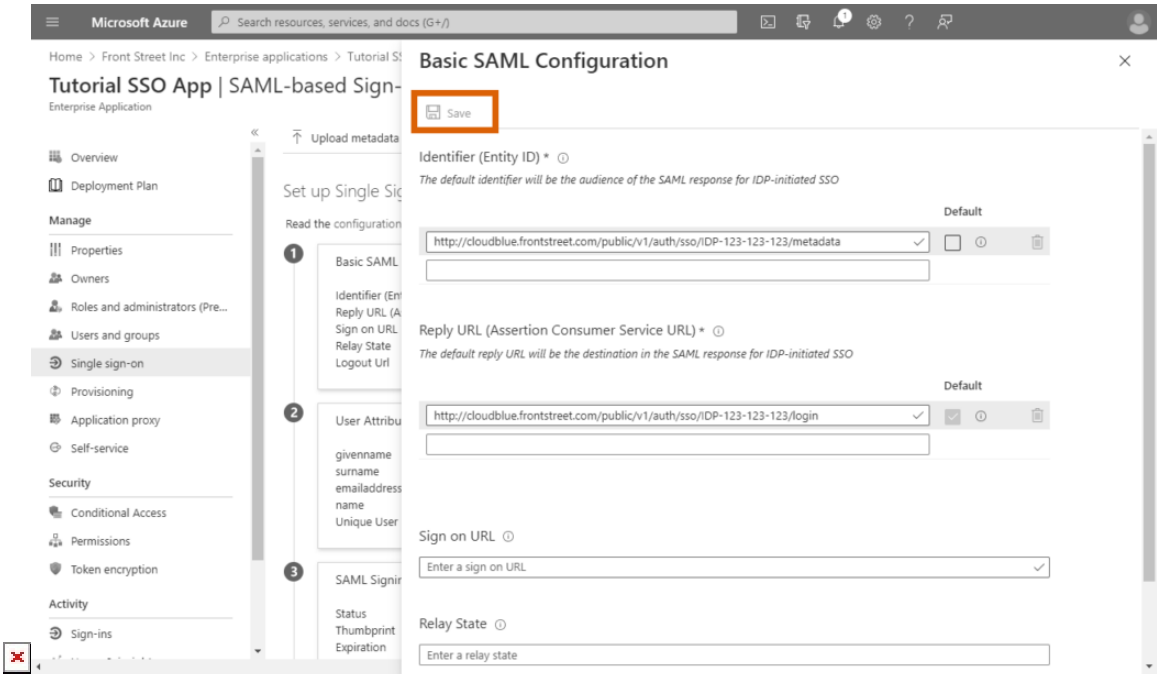
Single Sign On Service URL
https://connect.cloudblue.com/saml/IDP-391-324-781/login
Binding: HTTP-POST • Assertions: signed and encrypted

Single Logout Service URL
https://connect.cloudblue.com/saml/IDP-391-324-781/logo
Binding: HTTP-Redirect

SP Certificate File
sp_cert.cer

SP Metadata File
sp_metadata.xml

Step 6



Basic SAML Configuration

Identifier (Entity ID) *
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default
http://cloudblue.frontstreet.com/public/v1/auth/sso/IDP-123-123-123/metadata ☐

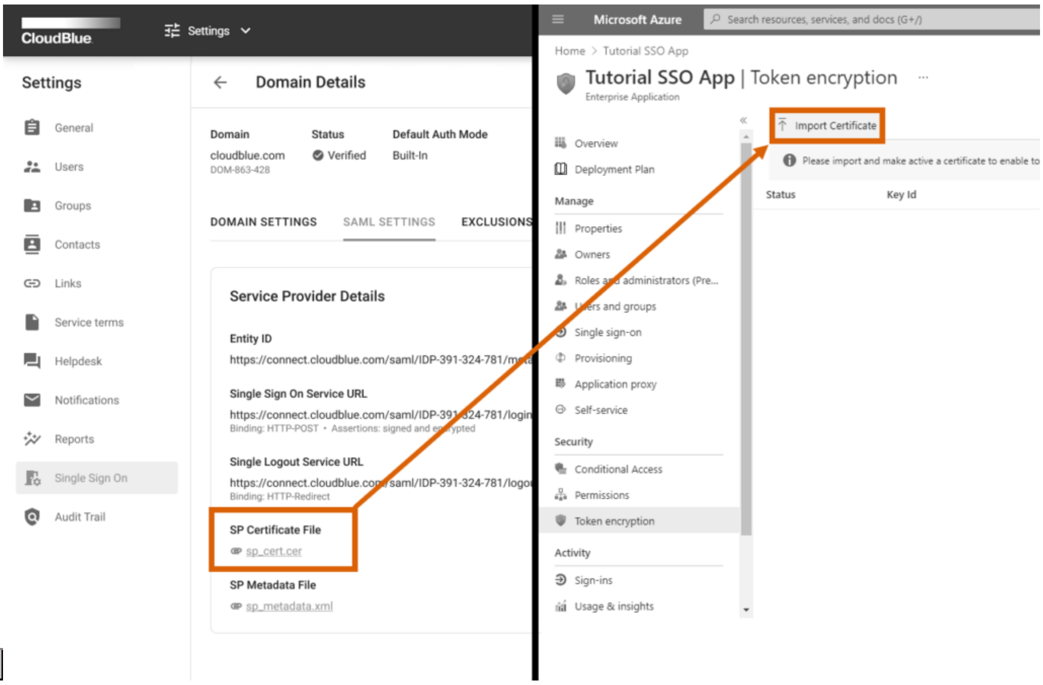
Reply URL (Assertion Consumer Service URL) *
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default
http://cloudblue.frontstreet.com/public/v1/auth/sso/IDP-123-123-123/login ☑

Sign on URL
Enter a sign on URL

Relay State
Enter a relay state

Step 7



Domain: cloudblue.com, DOM-863-428
Status: Verified
Default Auth Mode: Built-In

Service Provider Details

Entity ID
https://connect.cloudblue.com/saml/IDP-391-324-781/meta

Single Sign On Service URL
https://connect.cloudblue.com/saml/IDP-391-324-781/login
Binding: HTTP-POST • Assertions: signed and encrypted

Single Logout Service URL
https://connect.cloudblue.com/saml/IDP-391-324-781/logo
Binding: HTTP-Redirect

SP Certificate File
sp_cert.cer

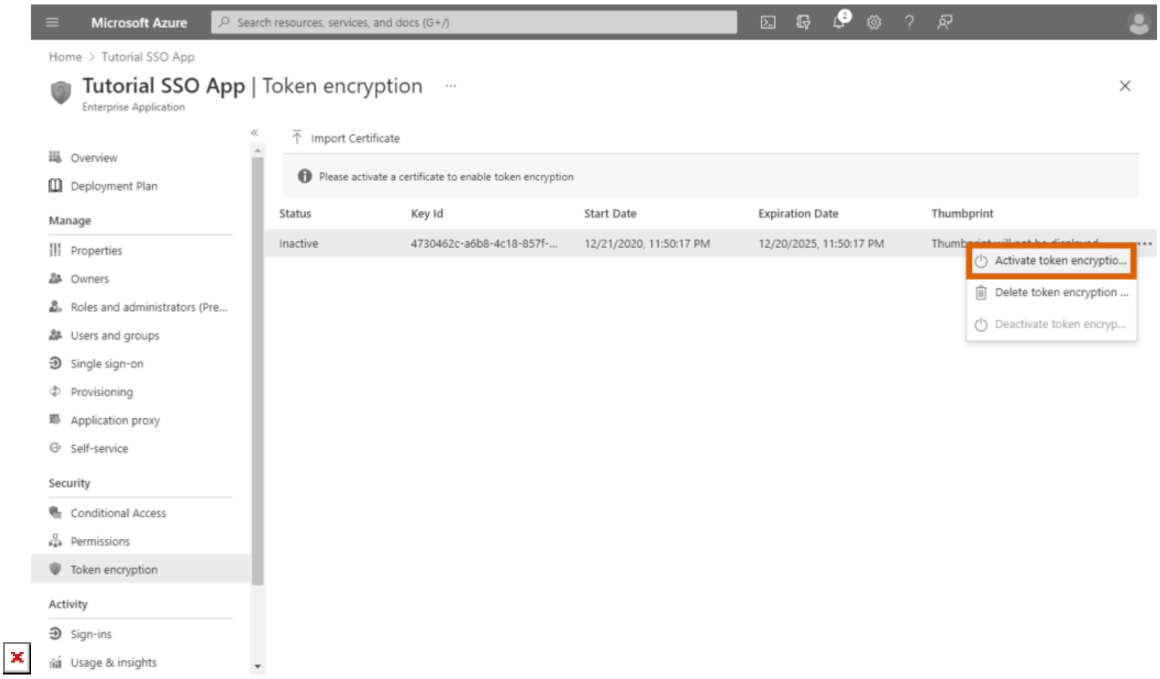
SP Metadata File
sp_metadata.xml

Tutorial SSO App | Token encryption
Enterprise Application

Please import and make active a certificate to enable to

Status	Key Id

Step 8



Tutorial SSO App | Token encryption
Enterprise Application

Please activate a certificate to enable token encryption

Status	Key Id	Start Date	Expiration Date	Thumbprint
Inactive	4730462c-a6b8-4c18-857f-...	12/21/2020, 11:50:17 PM	12/20/2025, 11:50:17 PM	Thumbprint will not be displayed

Step 9

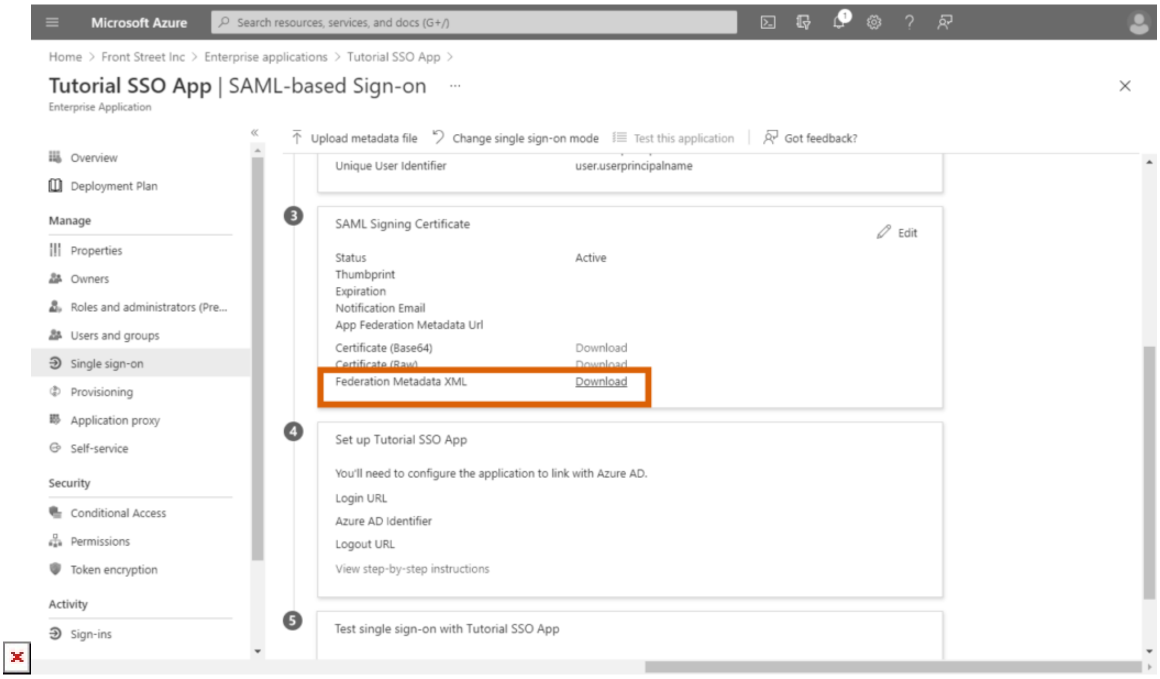
1. Access the **Enterprise applications** section from your created Azure Active Directory.
2. Click the **Create your own application** button under *Browse Azure AD Gallery*.

3. Enter your application name and select the **Integrate any other application you don't find in the gallery (Non-gallery)** radio option. Thereafter, click **Create** to create your enterprise application.
4. Access the **Single Sign-on** section of your created enterprise application once the system successfully processes your app.
5. Select the **SAML** option as your *Single Sign-On method*.
6. Click the **Upload metadata file** button to upload your Service Provider metadata file. Access the SP metadata file via the SAML settings tab from your verified domain on the Connect platform.
7. Once your metadata file is uploaded to the Microsoft Azure portal, click the **Save** button to save your provided metadata.
8. Access the **Token Encryption** section and click **Import Certificate** to upload your Connect certificate. Download this certificate via the SAML settings tab from your verified domain on the Connect platform. Note that Microsoft Azure requires you to get a Azure AD Premium P2 license in order to access this section.
9. Once your certificate is uploaded, activate this certificate by accessing the ellipsis (···) menu and clicking **Activate token encryption** within the Token Encryption section.

Therefore, your SSO system and the assertion encryption will be successfully configured on the Microsoft Azure portal. Note, however, that Azure's token encryption usually takes from 5 to 10 minutes to start working. Don't close your created Azure application just yet. It is required for the Connect SAML configuration as described below.

Connect SAML Configuration

If your created application and the assertion encryption is successfully configured on the Azure portal, it is necessary to configure *Identity Provider Details* and *User Management* attributes within your verified domain on the CloudBlue Connect platform. In addition, you can switch the SAML authentication mode of your domain to test out your configured single sign-on system. Note that in order to enable this mode at least one user should be added to the *Exclusions* list. The following steps showcase how to successfully perform all of the aforementioned operations:



Tutorial SSO App | SAML-based Sign-on

Enterprise Application

Unique User Identifier user.userprincipalname

SAML Signing Certificate

Status Active
Thumbprint
Expiration
Notification Email
App Federation Metadata Url
Certificate (Base64) Download
Certificate (Raw) Download
Federation Metadata XML Download

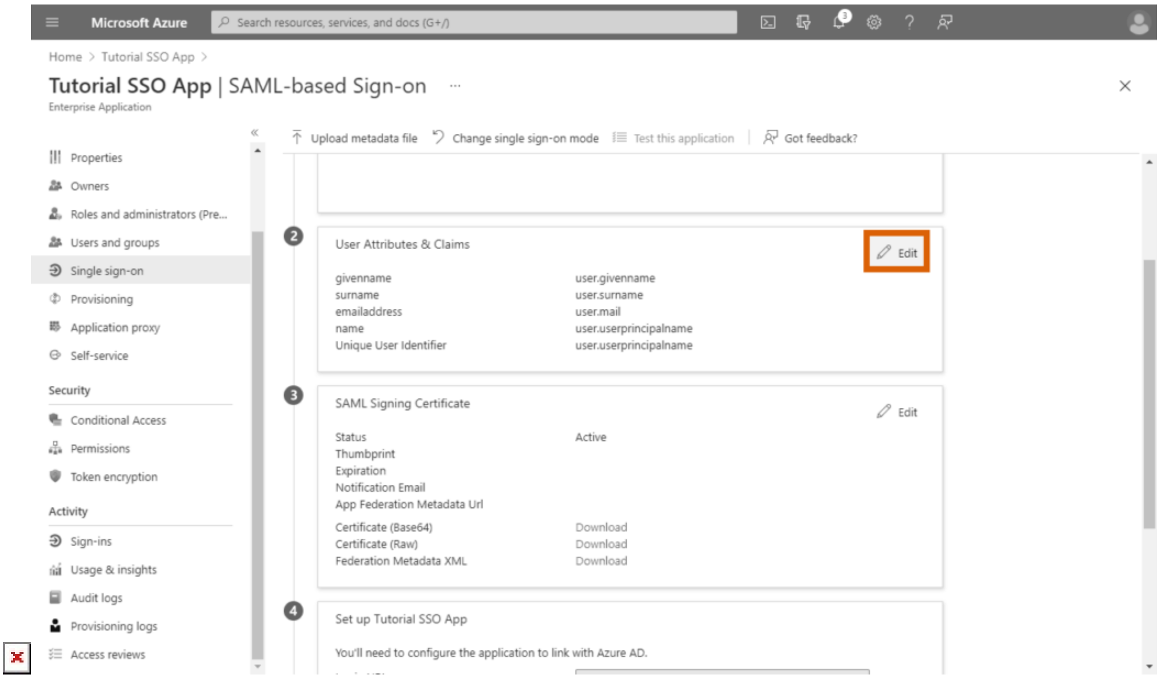
Set up Tutorial SSO App

You'll need to configure the application to link with Azure AD.

Login URL
Azure AD Identifier
Logout URL
View step-by-step instructions

Test single sign-on with Tutorial SSO App

Step 1



Tutorial SSO App | SAML-based Sign-on

Enterprise Application

2 User Attributes & Claims

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

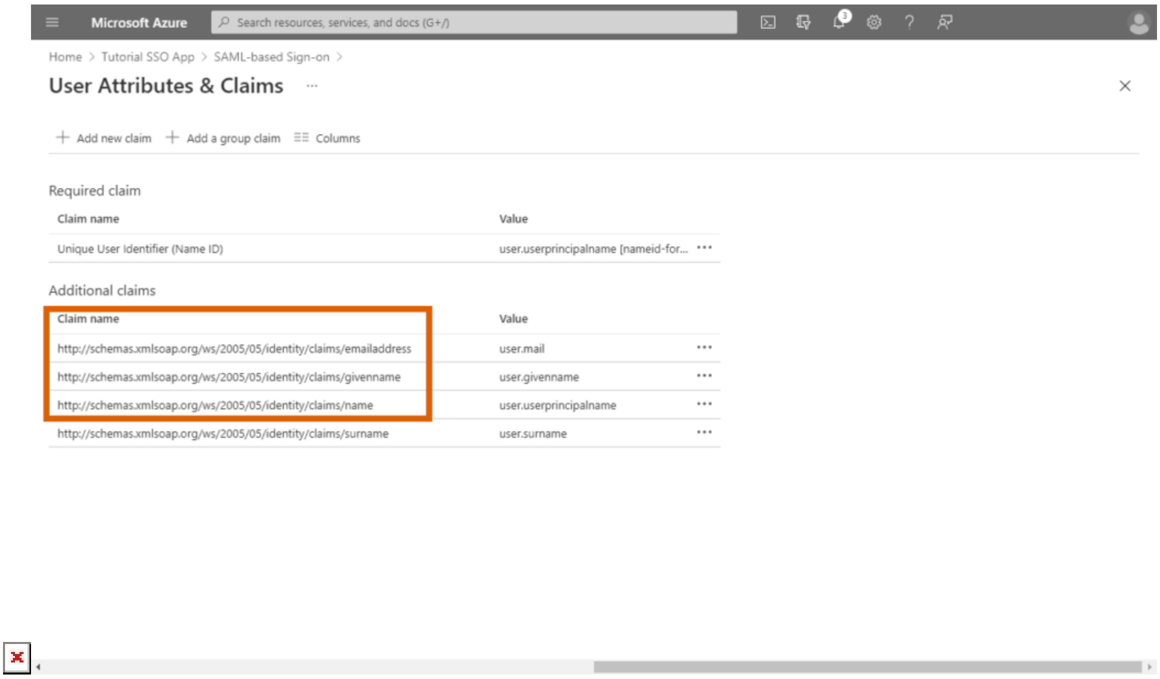
3 SAML Signing Certificate

Status	Active
Thumbprint	
Expiration	
Notification Email	
App Federation Metadata Url	
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Tutorial SSO App

You'll need to configure the application to link with Azure AD.

Step 2


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Tutorial SSO App > SAML-based Sign-on >
Add new claim
Add a group claim
Columns

User Attributes & Claims

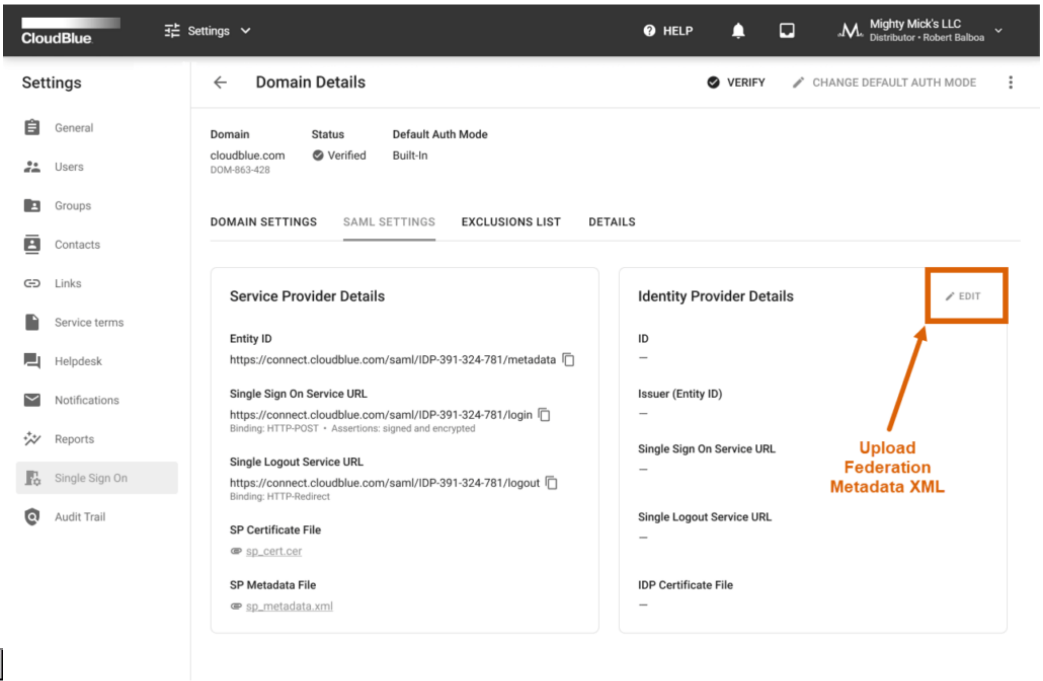
Required claim

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

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Step 3



Domain Details

Domain	Status	Default Auth Mode
cloudblue.com DOM-863-428	Verified	Built-In

Service Provider Details

Entity ID
https://connect.cloudblue.com/saml/IDP-391-324-781/metadata

Single Sign On Service URL
https://connect.cloudblue.com/saml/IDP-391-324-781/login
Binding: HTTP-POST • Assertions: signed and encrypted

Single Logout Service URL
https://connect.cloudblue.com/saml/IDP-391-324-781/logout
Binding: HTTP-Redirect

SP Certificate File
sp_cert.cer

SP Metadata File
sp_metadata.xml

Identity Provider Details

ID
–

Issuer (Entity ID)
–

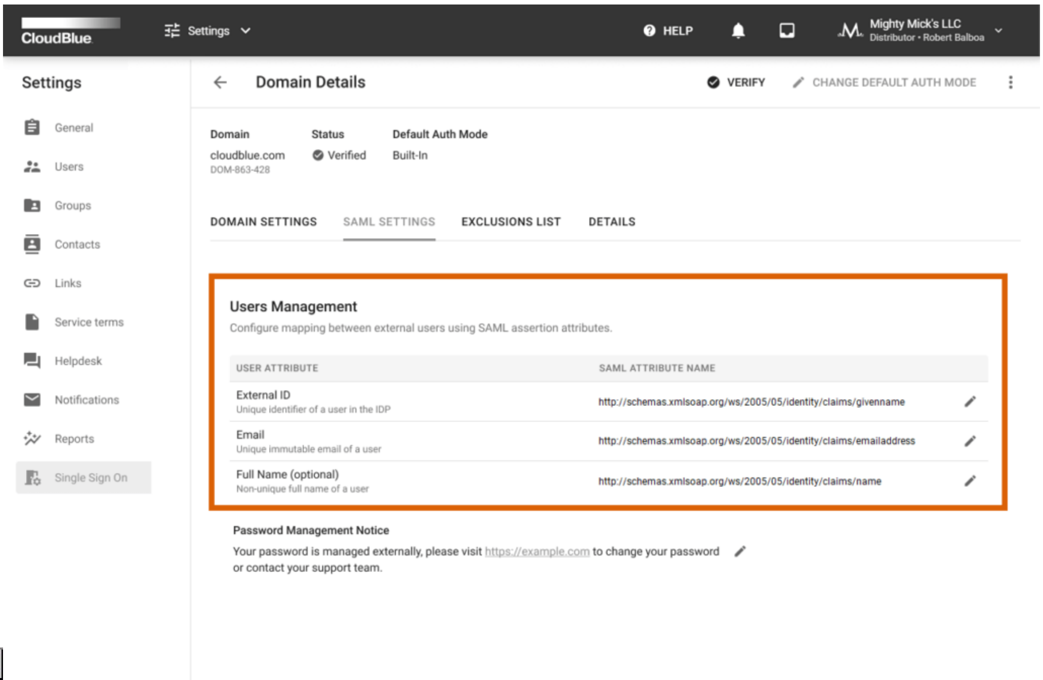
Single Sign On Service URL
–

Single Logout Service URL
–

IDP Certificate File
–

Upload Federation Metadata XML

Step 4



Domain Details

Domain	Status	Default Auth Mode
cloudblue.com DOM-863-428	Verified	Built-In

Users Management

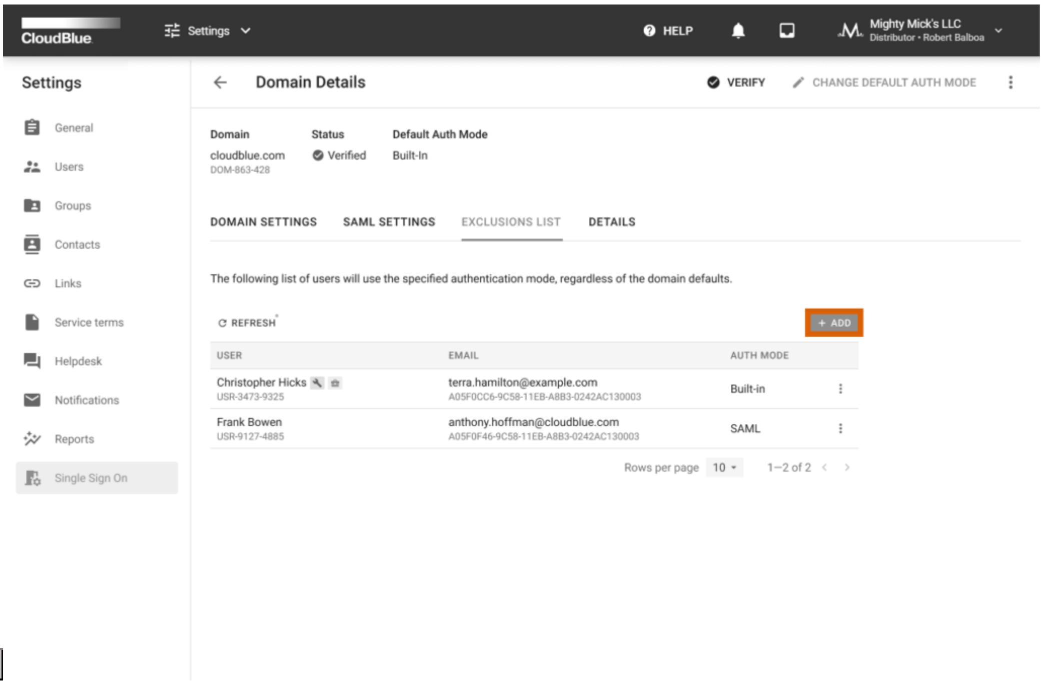
Configure mapping between external users using SAML assertion attributes.

USER ATTRIBUTE	SAML ATTRIBUTE NAME
External ID Unique identifier of a user in the IDP	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Email Unique immutable email of a user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Full Name (optional) Non-unique full name of a user	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

Password Management Notice

Your password is managed externally, please visit https://example.com to change your password or contact your support team.

Step 5



Domain Details

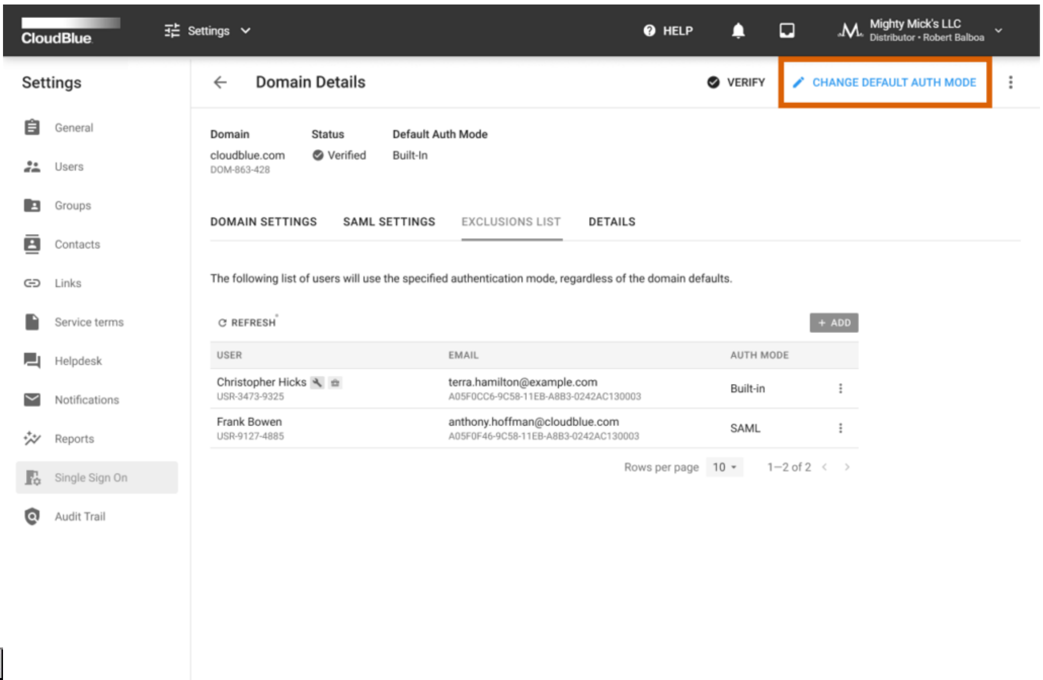
Domain	Status	Default Auth Mode
cloudblue.com DOM-863-428	Verified	Built-In

The following list of users will use the specified authentication mode, regardless of the domain defaults.

USER	EMAIL	AUTH MODE
Christopher Hicks USR-3473-9325	terra.hamilton@example.com A05F0CC6-9C58-11EB-A8B3-0242AC130003	Built-in
Frank Bowen USR-9127-4885	anthony.hoffman@cloudblue.com A05F0F46-9C58-11EB-A8B3-0242AC130003	SAML

Rows per page 10 1–2 of 2

Step 6



Domain Details

Domain	Status	Default Auth Mode
cloudblue.com DOM-863-428	Verified	Built-In

The following list of users will use the specified authentication mode, regardless of the domain defaults.

USER	EMAIL	AUTH MODE
Christopher Hicks USR-3473-9325	terra.hamilton@example.com A05F0CC6-9C58-11EB-A8B3-0242AC130003	Built-in
Frank Bowen USR-9127-4885	anthony.hoffman@cloudblue.com A05F0F46-9C58-11EB-A8B3-0242AC130003	SAML

Rows per page 10 1–2 of 2

Step 7

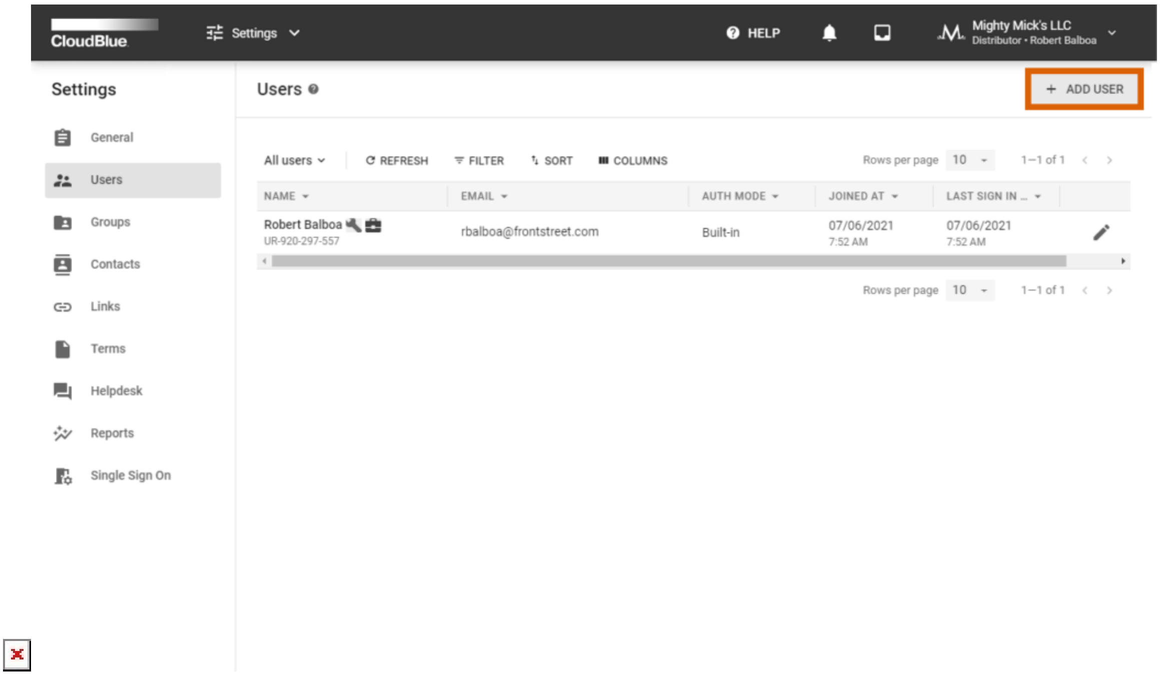
1. Access the **Single Sign-on** section from your configured Azure application. Thereafter, download the **Federation Metadata XML** under *SAML Signing Certificate*.

2. Scroll up to the *User Attributes & Claims* section and click the **Edit** button to access required user management attributes.
3. Copy the Azure claim names under *Additional Claims*. Namely, it is required to copy the following claim names:
   Email: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`
   External ID: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`
   Full Name: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`
4. Access the SALM Settings tab from your verified domain on Connect. Click the **Edit** button next to *Identity Provider Details* and upload your exported **Federation Metadata XML** to the corresponding form.
5. Locate the *User Management* section of the SAML Settings tab and provide the copied claim names as **SAML Attribute Names**.
6. Access the **Exclusions List** tab of your Connect domain. Click the **Add** button to specify at least one user with the *built-in* authentication mode.
7. Click **Change Default Auth Mode** at the top-right corner of your domain details screen. The appeared wizard will help you switch the default mode to the *SAML* authorization mode.

By completing the provided instruction, your Connect domain will be successfully configured for single sign-on authorization via the Azure Active Directory. Therefore, you can add users to your authorization system and test out as described below.

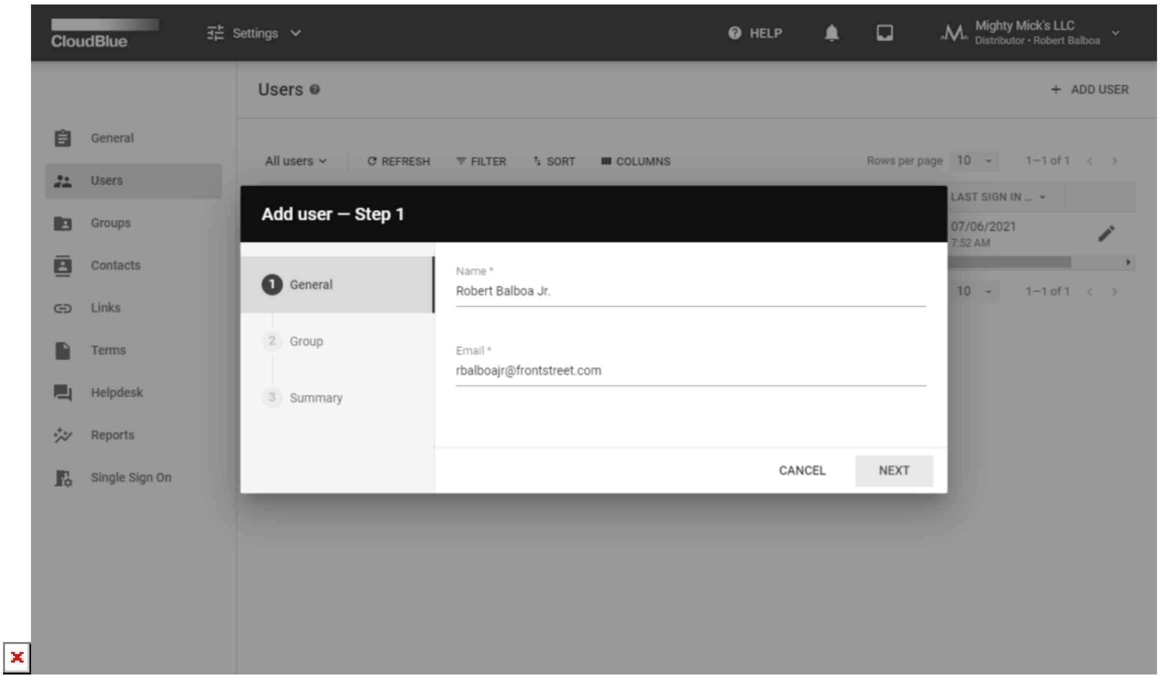
Adding Users and Test Authorization

Once your single sign-on system will be successfully configured, you can create a new user on Connect and add this user to your Azure Active Directory as well as your to your configured application. Therefore, you can test out your configured SAML authorization. Follow the steps below to add a new user and test your single sign-on system:



NAME	EMAIL	AUTH MODE	JOINED AT	LAST SIGN IN ...
Robert Balboa UR-920-297-557	rbalboa@frontstreet.com	Built-in	07/06/2021 7:52 AM	07/06/2021 7:52 AM

Step 1

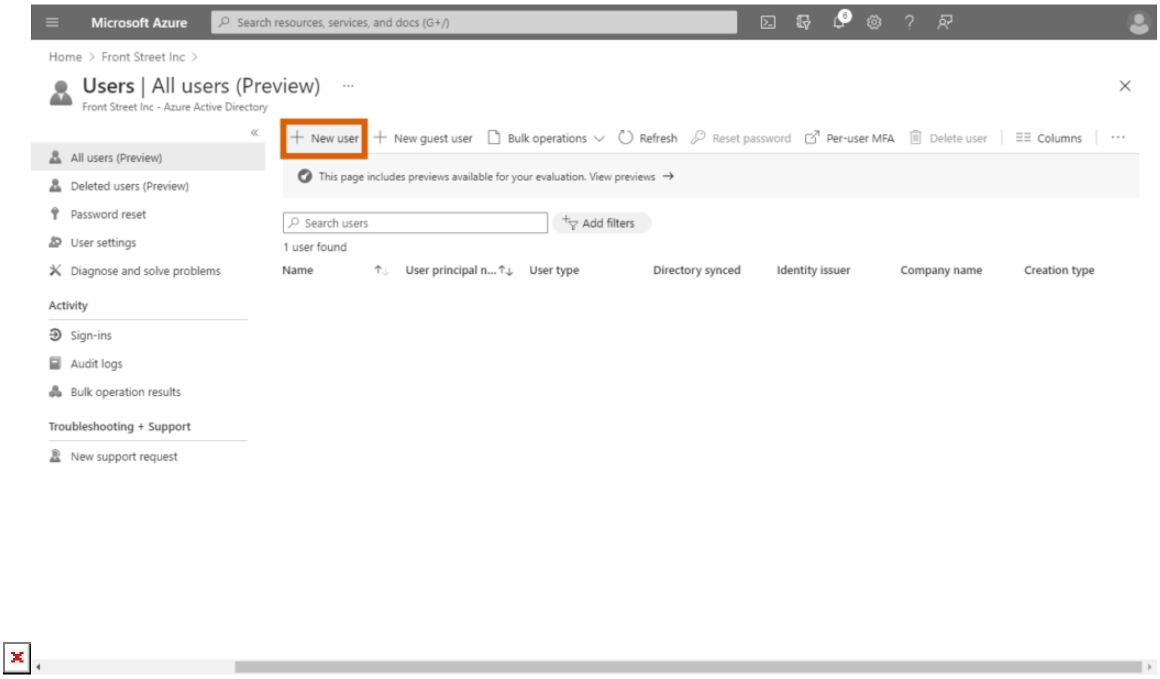


Add user — Step 1

Name * Robert Balboa Jr.

Email * rbalboajr@frontstreet.com

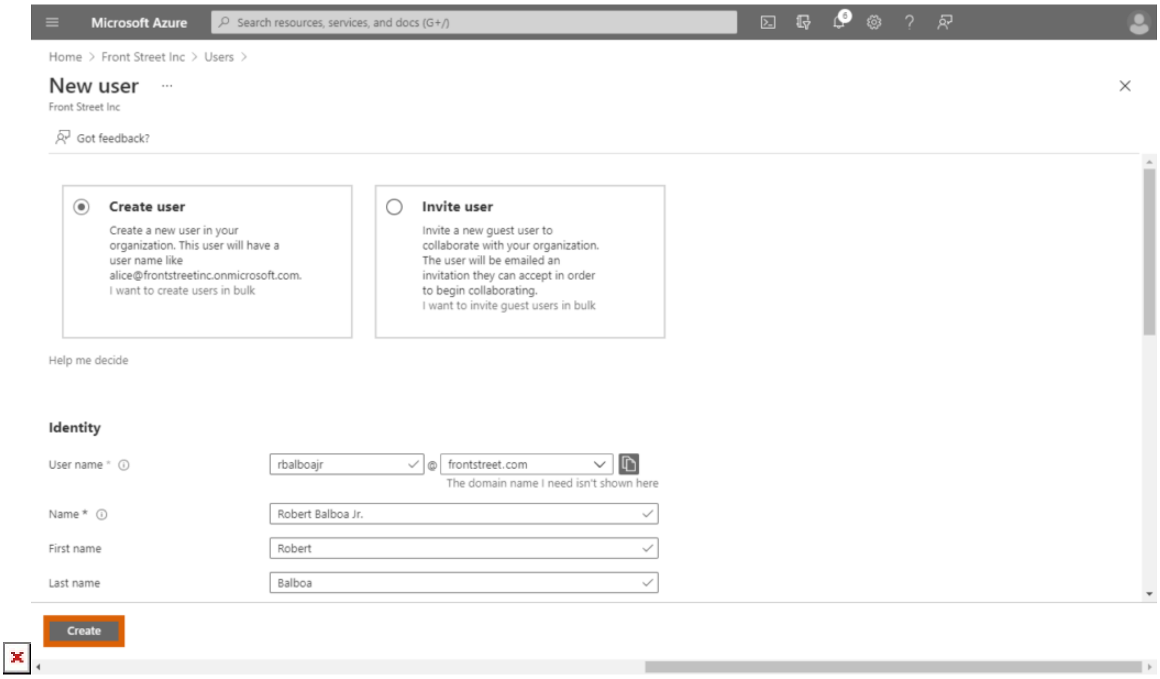
Step 1



This page includes previews available for your evaluation. View previews →

1 user found

Step 2



Home > Front Street Inc > Users >

New user ...

Front Street Inc

Got feedback?

● **Create user**

Create a new user in your organization. This user will have a user name like alice@frontstreetinc.onmicrosoft.com.

I want to create users in bulk

○ **Invite user**

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

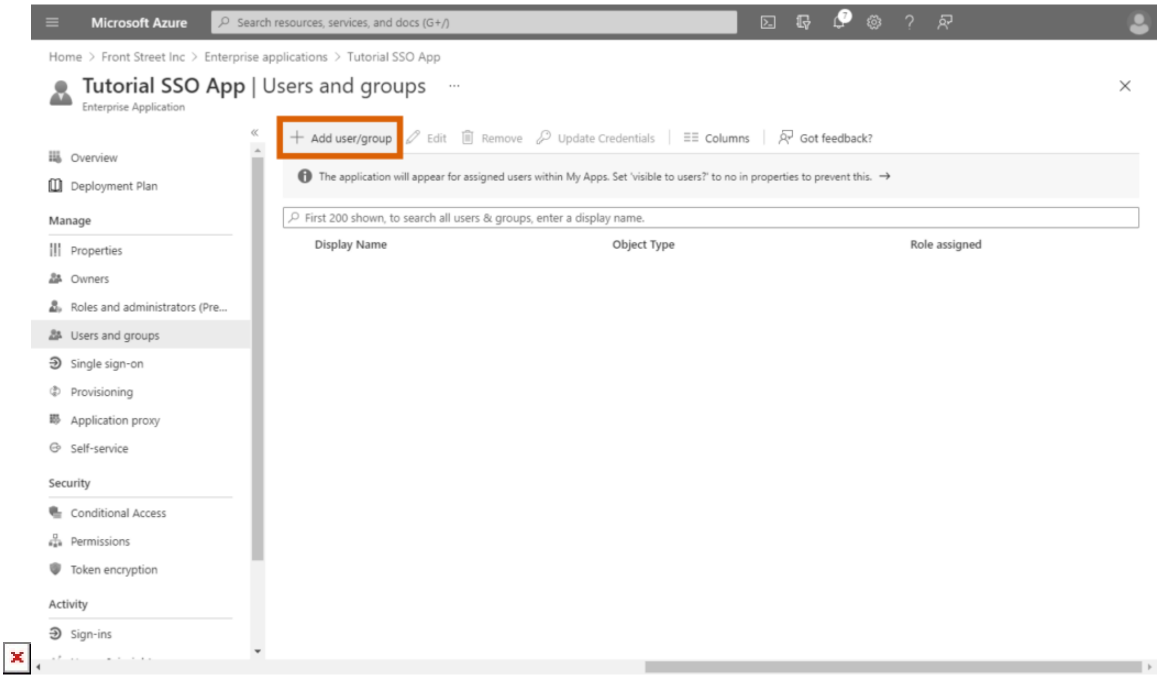
I want to invite guest users in bulk

Help me decide

Identity

User name *	rbalboajr @ frontstreet.com The domain name I need isn't shown here
Name *	Robert Balboa Jr.
First name	Robert
Last name	Balboa

Step 2



Home > Front Street Inc > Enterprise applications > Tutorial SSO App

Tutorial SSO App | Users and groups ...

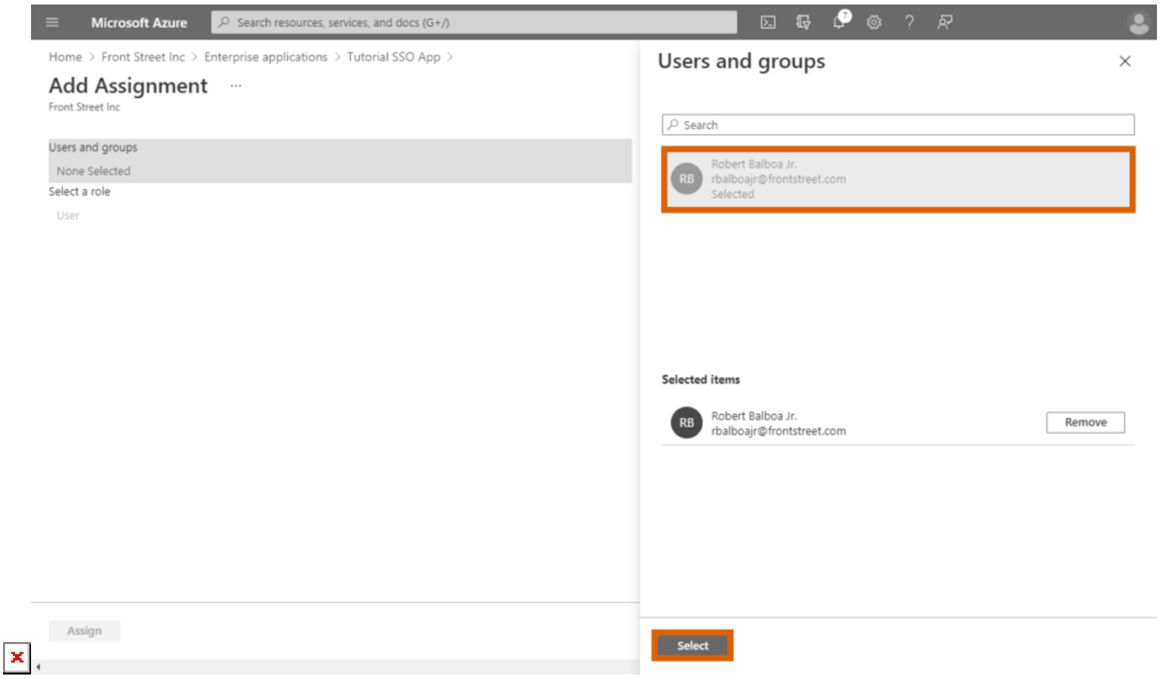
Enterprise Application

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned

Step 3



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Front Street Inc > Enterprise applications > Tutorial SSO App >
Select
Remove
Assign

Add Assignment

Front Street Inc

Users and groups

None Selected

Select a role

User

Users and groups

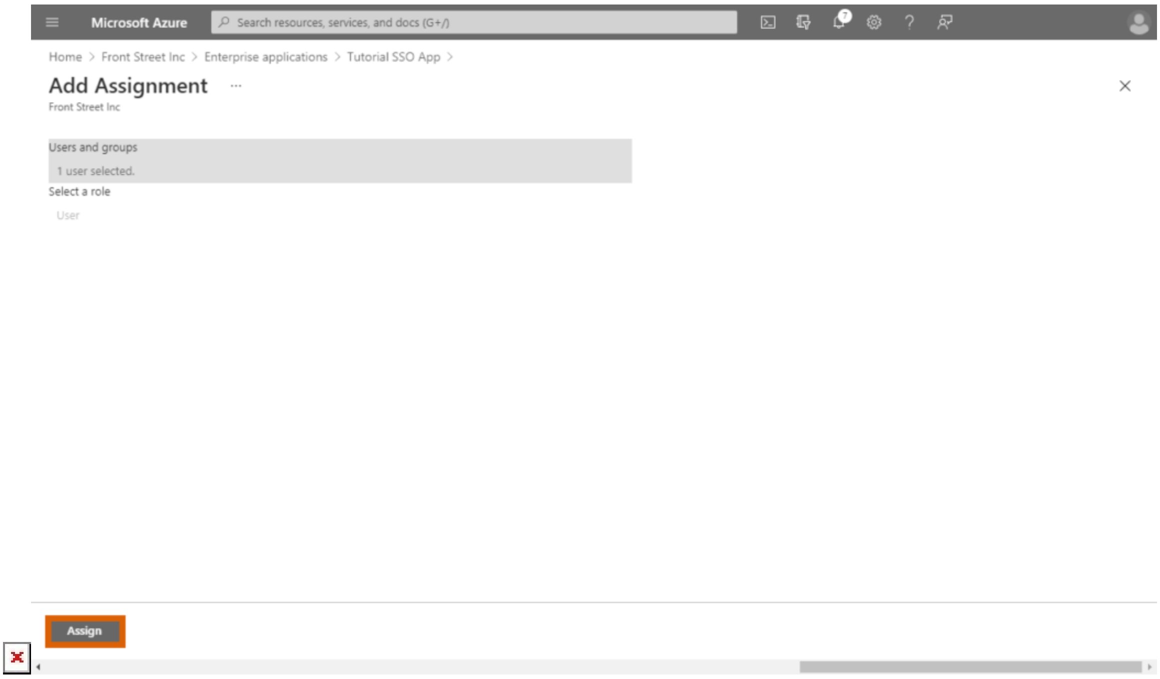
Search

Robert Balboa Jr.
rbalboajr@frontstreet.com
Selected

Selected items

Robert Balboa Jr.
rbalboajr@frontstreet.com

Step 4



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Front Street Inc > Enterprise applications > Tutorial SSO App >
Assign

Add Assignment

Front Street Inc

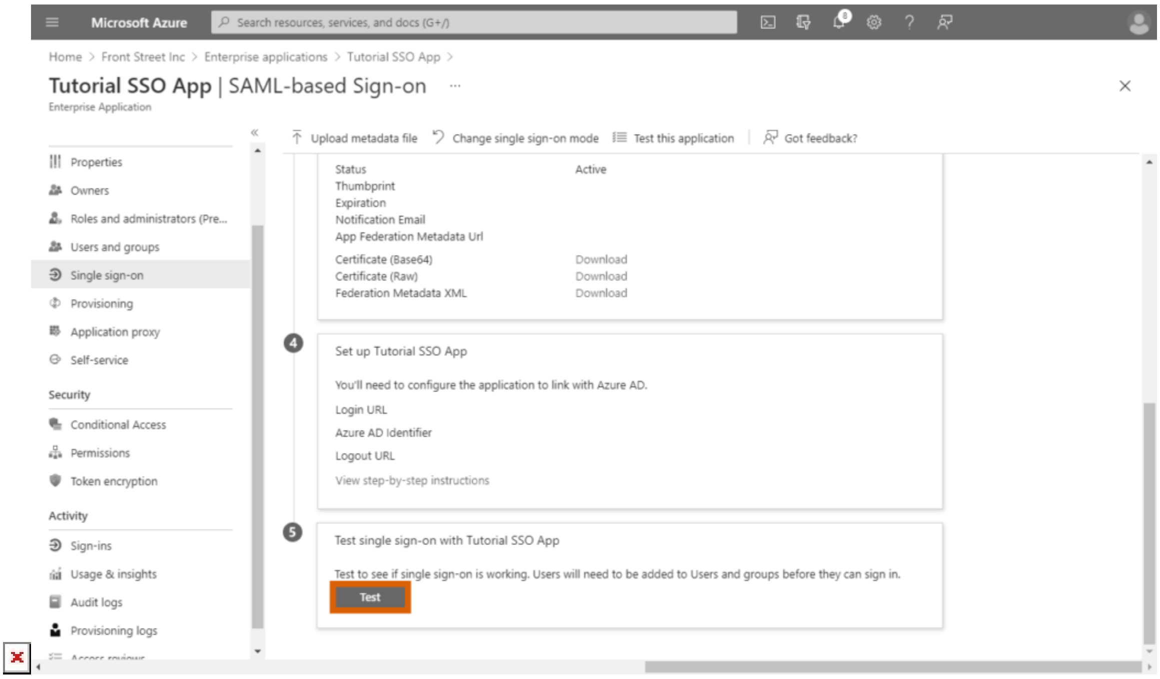
Users and groups

1 user selected.

Select a role

User

Step 5



Microsoft Azure

Home > Front Street Inc > Enterprise applications > Tutorial SSO App >

Tutorial SSO App | SAML-based Sign-on

Enterprise Application

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

Status: Active
Thumbprint
Expiration
Notification Email
App Federation Metadata Url
Certificate (Base64): Download
Certificate (Raw): Download
Federation Metadata XML: Download

4 Set up Tutorial SSO App

You'll need to configure the application to link with Azure AD.

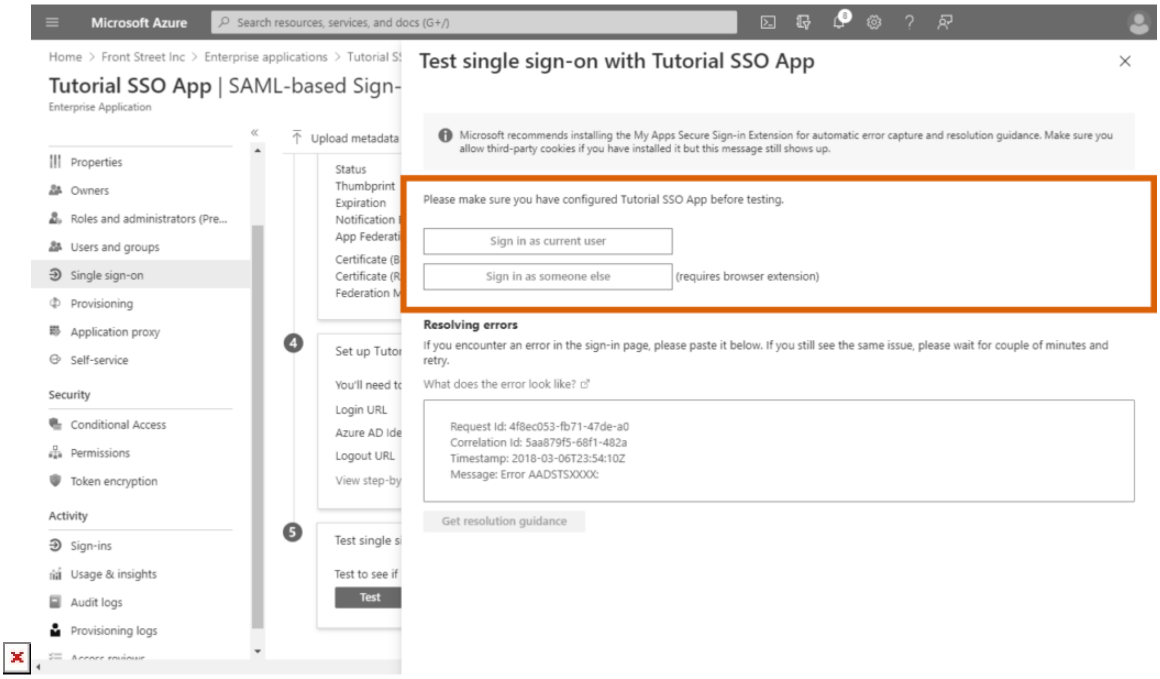
Login URL
Azure AD Identifier
Logout URL
View step-by-step instructions

5 Test single sign-on with Tutorial SSO App

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Test

Step 6



Test single sign-on with Tutorial SSO App

Microsoft recommends installing the My Apps Secure Sign-in Extension for automatic error capture and resolution guidance. Make sure you allow third-party cookies if you have installed it but this message still shows up.

Please make sure you have configured Tutorial SSO App before testing.

Sign in as current user

Sign in as someone else (requires browser extension)

Resolving errors

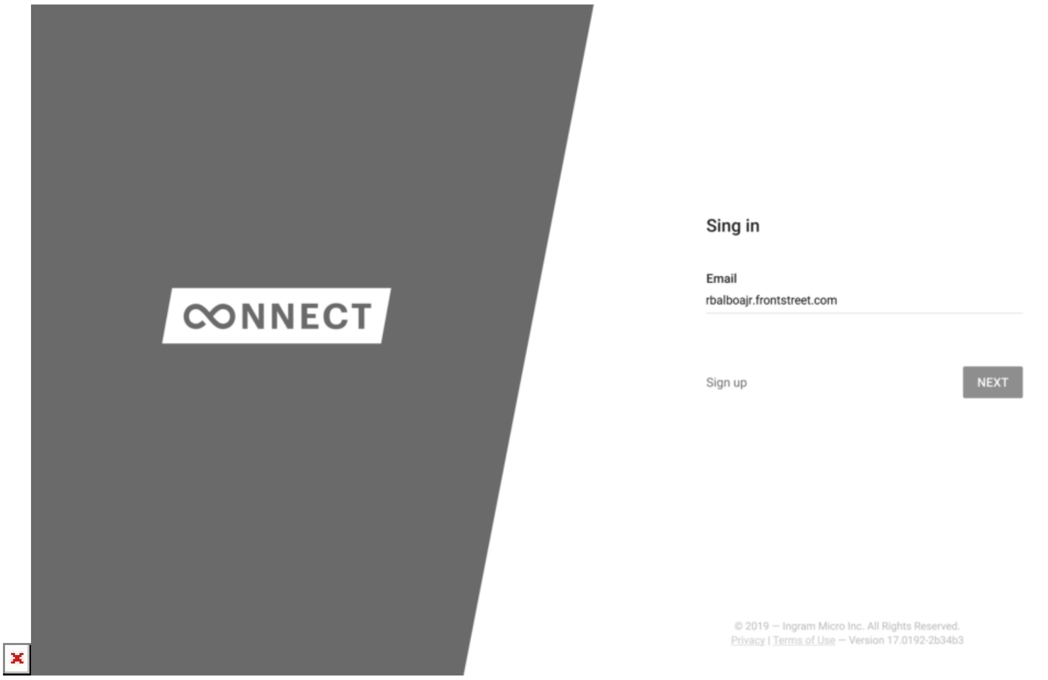
If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.

What does the error look like?

```
Request Id: 4f8ec053-fb71-47de-a0
Correlation Id: 5aa879f5-68f1-482a
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXX:
```

Get resolution guidance

Step 6

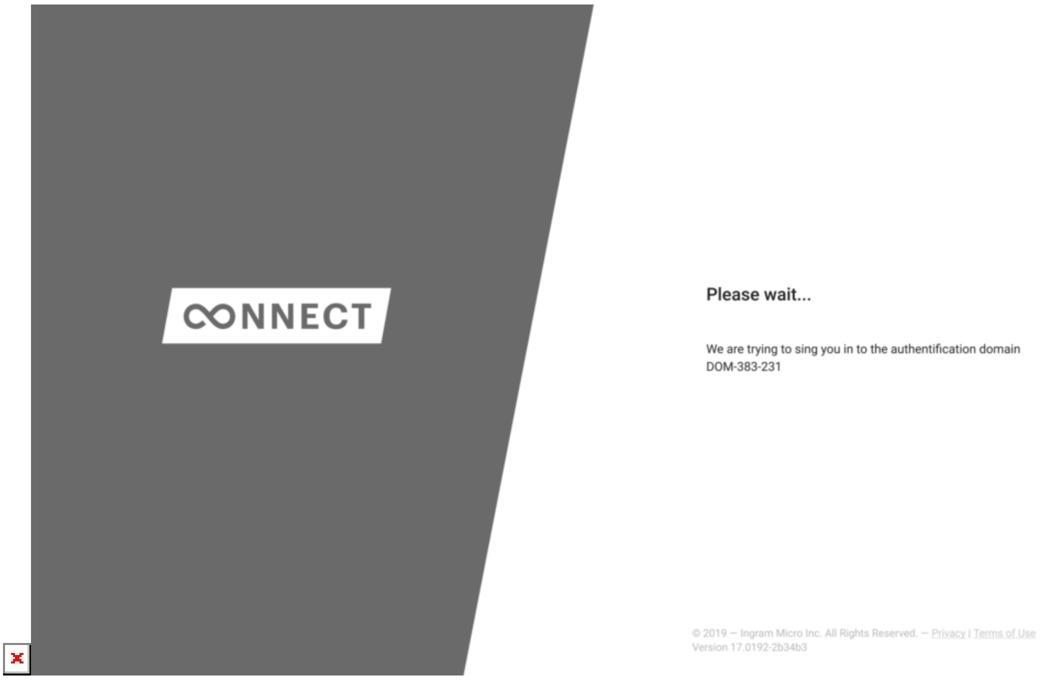


Sing in

Email
rbalboajr.frontstreet.com

© 2019 — Ingram Micro Inc. All Rights Reserved.
Privacy | Terms of Use — Version 17.0192-2b34b3

Step 7



Please wait...

We are trying to sing you in to the authentification domain DOM-383-231

© 2019 — Ingram Micro Inc. All Rights Reserved. — Privacy | Terms of Use
Version 17.0192-2b34b3

Step 7

1. Access the **Users** section of the Account module on the Connect platform. Click **Add User** to launch the wizard and create your test user on Connect.

2. Proceed to the **Users** section from your configured **Azure Active Directory.** Click the **New User** button to add your test user with same credentials.
3. Navigate to the **Users and Groups** section from your configured *Enterprise Application*. Click the **Add user/group** to add your configured user.
4. Click on *Users and Groups* from the provided form. Thereafter, choose your user from the list and click the **Select** button.
5. Click **Assign** to successfully assign your selected user to your application.
6. Access the **Single Sign-on** section and click the Test button in case you want to test your SAML configuration. Sign in as your current user or test your application as someone else.
7. Finally, use your created user's credentials to sign into your Connect domain.

In case your single-sign on authorization system is configured correctly, the Connect platform will allow you to sign into your domain by using your specified credentials.