×

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This article has been generated from the online version of the documentation and might be out of date.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 July 3, 2025

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.
- 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.



- 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:

	Clou	idBlue. 랴 :	ettings V 😯 HELP 🌲 🗔 Mighty Mick's LLC Substributor - Robert Balboa V
	Sett	ings	← Domain details ●
	Ê	General	Domain Status Default auth mode frontstreetinc.onmicrosoft.com
	**	Users Groups	DOM-438-327
	8	Contacts	
	69 •	Links Helpdesk	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.
	**	Reports	NAME         TYPE         VALUE           cloudblue.frontstreetinc.onmicrosoft.com         TXT         connect=a670a22b10401752bb63ad1bc7dc502b3         []]
	Б	Single Sign On	
×			© 2021 – Ingram Micro Inc. All Rights Reserved. – <u>Privacy   Terms of Use</u> – Version 23.0.1299-g75017e3 [Staging]

Step 1

Home > Microsoft.DnsZone-202107	712 >					
frontstreetinc.cor	n ጵ…					
	« + Record set +	Child zone $ ightarrow$ Move $ ightarrow$ $\widehat{\blacksquare}$	Delete zone 💍 Refr	esh		
Overview	∧ Essentials					JSON Vie
Activity log						
PR Access control (IAM)						
Tags						
Diagnose and solve problems						
Settings						
III Properties	Tags (change)					
A Locks	Click here to add tags					
Monitoring		cord sets that have been loaded	on this page. If you don'	t see what you're looking fo	r, you can try scrolling to allow	more record sets to load
Alerts						
má Metrics	Name	Туре	TTL	Value	Alias resource type	Alias target
Automation	0	NS				
Tasks (preview)						
Export template						
Support + troubleshooting	۵	SOA				

Step 2

	rade 🖉 P Search resources, services,	and docs (G+/)		Þ.	I 🕼 🗘 🍩 ? 🔊	8
Home > Microsoft.DnsZone-20210712					Add record set	×
DNS zone     Search (Ctrl+/) «     Overview     Activity log     Access control (IAM)     Tags     Diagnose and solve problems     Settings     III Properties     Locks	+ Record set + Child zon	e → Move ∨ 🗐	] Delete zone 🖒 Refresh		Name Cloudblue.frontstreetinc.onmicrosoft.com Type TxT – Text record type TTL * TTL unit 1 ✓ Hours Value connect=a670a22b10401752bb63ad1bc The quick brown fox jumps over the lazy	
Monitoring	You can search for record sets t           P Search record sets	hat have been loaded	on this page. If you don't see	e what you're		
III Alerts 論 Metrics	Name	Туре	TTL	Value		
Automation	۵	NS	172800			
Tasks (preview)     Export template Support + troubleshooting     New support request	٥	SOA	3600			
, ,			_	_	ок	

Step 3 & 4

Seneral Domain Status Default auth mode   Ivers Users frontstreet.onmicrosoft.com Iverifying -   Sroups DOMAIN SETTINGS SAML SETTINGS EXCLUSIONS LIST DETAILS   Contacts 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.   Image: Single Sign On NAME TYPE VALUE	Sett	ings	← Domain details
DOMAIN SETTINGS       SAML SETTINGS       EXCLUSIONS LIST       DETAILS         Demain Verification Record       In order to validate ownership of frontstreet.com/crosoft.com, you must create the following records in the DNS settings for the domain with the following values.         Helpdesk       NAME       TYPE       VALUE         Couldblue.frontstreet.onmicrosoft.com       TXT       connect=2888cc52b7b1af5e67705b7feb42988a611d92da	_		frontstreet.onmicrosoft.com
CD Links CD Omain 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.  Helpdesk NAME TYPE VALUE Cloudblue.frontstreet.onmicrosoft.com TXT connect=2888cc52b7b1af5e67705b7feb42988a611d92da	_		DOMAIN SETTINGS SAML SETTINGS EXCLUSIONS LIST DETAILS
Reports     cloudblue.frontstreet.onmicrosoft.com     TXT     connect=2888cc52b7b1af5e67705b7feb42988a611d92da	_		
	4	Helpdesk	NAME TYPE VALUE
💦 Single Sign On	**	Reports	cloudblue.frontstreet.onmicrosoft.com TXT connect=2888cc52b7b1af5e67705b7feb42988a611d92da
	6	Single Sign On	
			© 2021 – Ingram Micro Inc. All Rights Reserved. – Privacy   Terms of Use – Version 23.0.1299-075017e3 [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

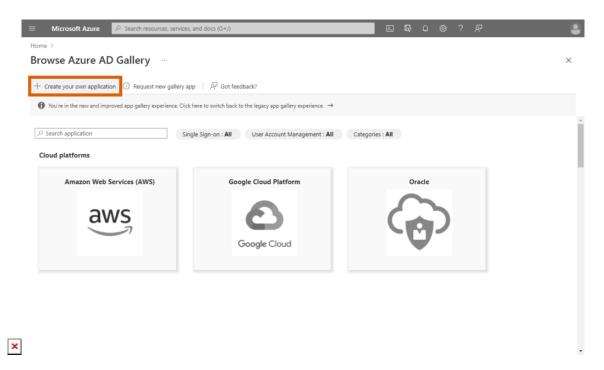
In case you have the same domain for two different Connect accounts (e.g., one domain for Vendors and Distributors), it is required to add two DNS records for each domain instance on the Connect platform.

#### **Enterprise Application**

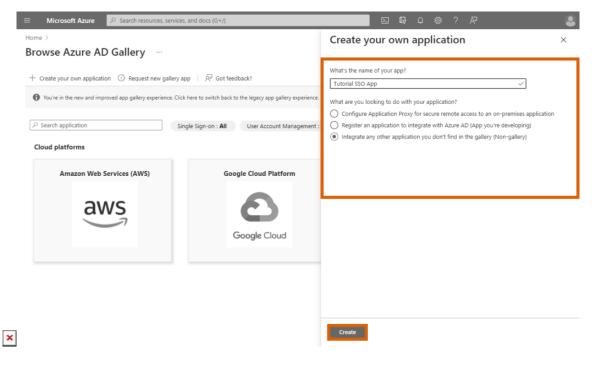
In case your Active Directory is successfully configured and your domain is successfully on the Connect platform, it is necessary to define your single sign-on system via the *Enterprise applications* section on the Microsoft Azure portal and upload your Connect *Service Provider* metadata and certificate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

🗏 Microsoft Azure 🔎 Se	earch resources, services, and docs (G+/)			R (°	🕲 ? ନି		
Home > Front Street Inc > Enterpris	se applications						
	ations   All applications						>
Front Street Inc - Azure Active Direc Overview	≪ + New application == Co	lumns 🔄 Preview features 🛛					
Overview	Try out the new Enterprise Application	ps search preview! Click to enable the prev	riew. →				
imes Diagnose and solve problems	Application type	Applications status	Application visibility				
Manage	Enterprise Applications 🗸 🗸	Any 🗸	Any	$\sim$	Apply	Reset	
All applications		your applications, enter a display nam	e or the application ID.				
聯 Application proxy	Name	Homepage URL		Object ID		Application ID	
🕲 User settings	Didn't find what you're looking fo	or? Click 'Add' above to add a new app	lication.				
Security							
Conditional Access							
Consent and permissions							
Activity							
Sign-ins							
ள் Usage & insights							
Audit logs							
Provisioning logs							
i≡ Access reviews							
Admin consent requests							

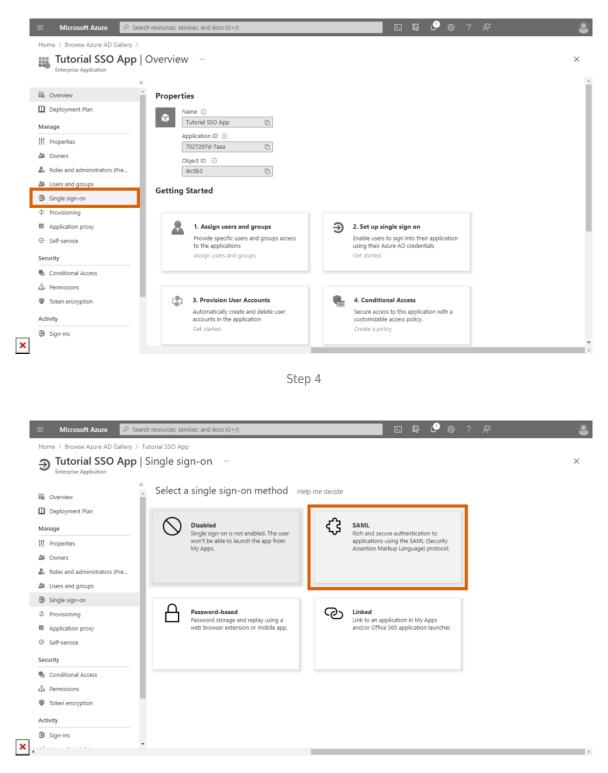
Step 1



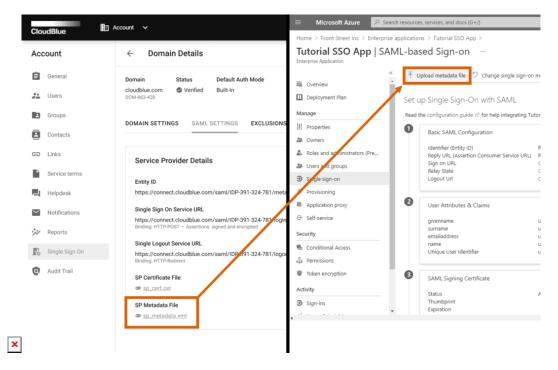
Step 2

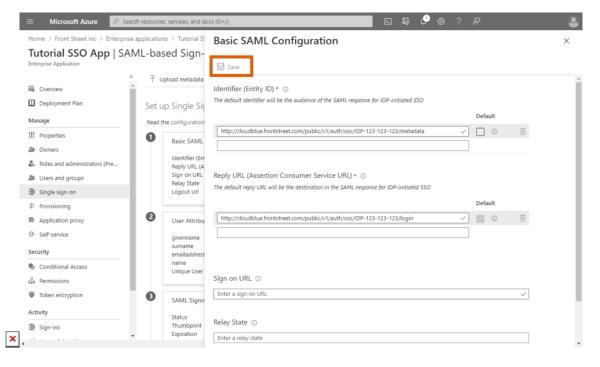


Step 3

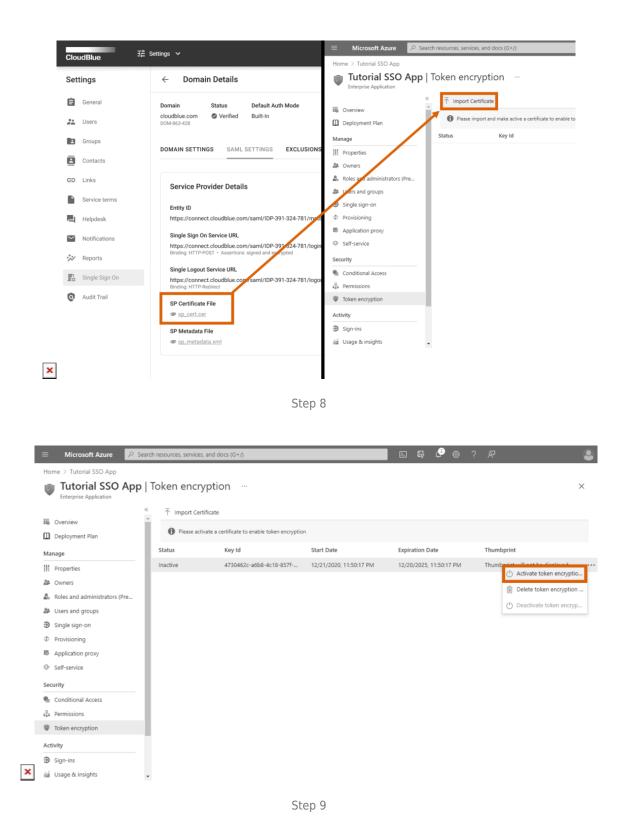


Step 5





Step 7



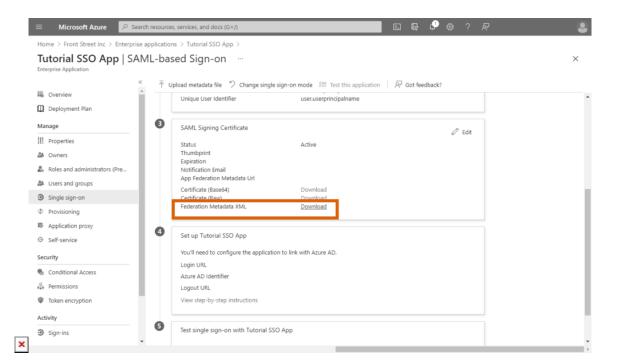
- 1. Access the **Enterprise applications** section from your created Azure Active Directory.
- 2. Click the **Create your own application** button under *Browse Azure AD Gallery*.

- 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:

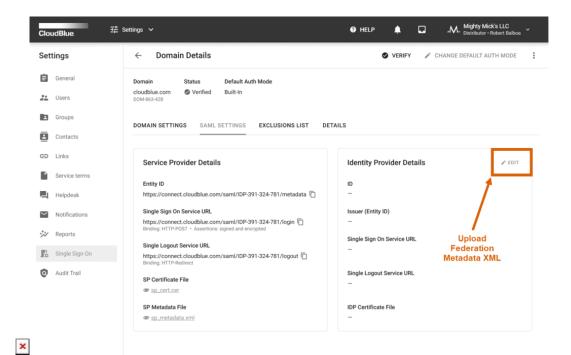


Step 1

Tutorial SSO App   SA Enterprise Application	ML-ba	ised Sign-on			×
Properties Owners Roles and administrators (Pre Users and groups Single sign-on Provisioning Application proxy	<ul> <li>▲     <li>↑     <li>▲     <li>↓     </li> <li>↓      </li> <li>↓     </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li> <li>↓      </li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></ul>	Upload metadata file "> Change single User Attributes & Claims givenname surname emailaddress name	sign-on mode III Test this application User.givenname user.sumame user.mail user.mail	₽ Got feedback?	
Security Conditional Access Permissions Token encryption	0	SAML Signing Certificate Status Thumbprint Expiration Notification Email App Federation Metadata Url	Active	🖉 Edit	
Activity           ③ Sign-ins           mi         Usage & insights           Image: Audit logs         Image: Audit logs           Image: Access reviews         Image: Access reviews	0	Certificate (Base64) Certificate (Raw) Federation Metadata XML Set up Tutorial SSO App You'll need to configure the applicatio	Download Download Download		

Microsoft Azure $P$ Search resources, services, and docs (G	+/)		D 🖓	P 🕸		
Home > Tutorial SSO App > SAML-based Sign-on >						
User Attributes & Claims						×
$+$ Add new claim $+$ Add a group claim $\equiv$ Columns						
Required claim						
Claim name	Value					
Unique User Identifier (Name ID)	user.userprincipalname [nameid-fc	r •••				
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					





CloudBlue. 芊	Settings 🗸	HELP     ▲     □     Mighty Mick's LLC     Substitutor - Robert Balboa     ×
Settings	← Domain Details	VERIFY / CHANGE DEFAULT AUTH MODE
😫 General	Domain Status Default Auth Mode cloudblue.com 🕲 Verified Built-In	
Jusers Users	DOM-863-428	
Groups	DOMAIN SETTINGS SAML SETTINGS EXCLUSIONS LIST DET	TAILS
Contacts		
GD Links		
Service terms	Users Management Configure mapping between external users using SAML assertion attributes	a.
Helpdesk	USER ATTRIBUTE SA	AML ATTRIBUTE NAME
Notifications	External ID ht Unique identifier of a user in the IDP	tp://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Reports	Email ht Unique immutable email of a user	tp://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Single Sign On	Full Name (optional) ht Non-unique full name of a user	tp://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
	Password Management Notice Your password is managed externally, please visit <a href="https://example.com">https://example.com</a> to or or contact your support team.	change your password 🕜

×

Step 5

Settings <ul> <li>Domain</li> <li>Status</li> <li>Domain</li> <li>Status</li> <li>Default Auth Mode</li> <li>cloudblue.com</li> <li>Verified</li> <li>Built-In</li> </ul> DomAin     Status     Default Auth Mode             cloudblue.com           Verified           Built-In             DomAin           Status           Default Auth Mode             cloudblue.com           Verified           Built-In             DomAin SETTINGS           SAML SETTINGS           EXCLUSIONS LIST             Default Auth Mode             contacts             Contacts             Service terms             C REFRESH             Notifications             VERFR             Notifications             Reports             Brack Signon                         State Signon	i General   Domain Status   Domain Status   i Conducts   i Groups   DomAIN SETTINGS SAML SETTINGS   E Contacts   i Contacts   i The following list of users will use the specified authentication mode, regardless of the domain defaults.   i Service terms   i Certified   i Helpdeak   VISER Itera Mail   Mutifications USER   I Notifications   VISH-9127-4885 ADSF01-46-9C58-11EB-AB83-9242AC130003   SAML i:	Clou	idBlue. 랴 :	Settings 🗸	Ø H	ELP 🌲		Mighty Mick's LLC Distributor - Robert Balboa	~
Domain     Status     Default Auth Mode       Lusers     DomAin     Status     Default Auth Mode       Lusers     DomAin     Status     Default Auth Mode       DomAin     DomAins     Wrified     Built-in       DomAin     Service terms     DomAins service terms     The following list of users will use the specified authentication mode, regardless of the domain defaults.       Service terms     Or REFRESH <sup>1</sup> + ADD       Helpdesk     USER     EMAIL     AUTH MODE       Notifications     USER     Lerra hamilton@example.com     Built-in       WISH:347279225     ADSFORCe9/05SHITEBABB3/0242/AC130003     Built-in     I       Motifications     USER     ADSFORCe9/05SHITEBABB3/0242/AC130003     SAML     I       Wishing 127/4885     ADSFORCe9/05SHITEBABB3/0242/AC130003     SAML     I	Image: Status       Demail Autor Mode         Image: Status       Downess-428         Image: Status       Downess-428<	Sett	ings	← Domain Details		VERIFY	🖌 🧨 СНА	ANGE DEFAULT AUTH MODE	
Users DOMAR983-428      DOMAIN SETTINGS SAML SETTINGS EXCLUSIONS LIST DETAILS      DOMAIN SETTINGS SAML SETTINGS EXCLUSIONS LIST DETAILS      DOMAIN SETTINGS EXCLUSIONS LIST EXCLUSIONS LIST EXCLUSIONS EXCLUSIO	Users DOMAIN SETTINGS SAML SETTINGS EXCLUSIONS LIST DETAILS  DOMAIN SETTINGS DOMAIN SETTINGS EXCLUSIONS LIST DETAILS  DOMAIN SETTINGS SAML SETTINGS EXCLUSIONS LIST DETAILS  DOMAIN SETTINGS SAML SETTINGS EXCLUSIONS LIST DETAILS  Contacts  Contacts Co	Ê	General	Domain Status Default	Auth Mode				
DOMAIN SETTINGS       SAML SETTINGS       EXCLUSIONS LIST       DETAILS         Image: Detail of the contracts       Image: Detail of the contract of the contrac	DOMAIN SETTINGS       SAML SETTINGS       EXCLUSIONS LIST       DETAILS         Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts         Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts         Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts         Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts       Image: Contacts <td< td=""><td>**</td><td>Users</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	**	Users						
Image: Contacts       The following list of users will use the specified authentication mode, regardless of the domain defaults.         Image: Service terms       C REFRESH <sup>1</sup> Image: ADD Contacts         Image: Service terms       C REFRESH <sup>1</sup> Image: Contacts         Image: Service terms       Contacts       Emage: Contacts         Image: Service terms       Contacts       Emage: Contacts         Image: Service terms       Contacts       Contacts       Contacts         Image: Service terms       Contacts       Conta	Image: Contacts       The following list of users will use the specified authentication mode, regardless of the domain defaults.         Image: Service terms       C REFRESH*       Image: Authentication mode, regardless of the domain defaults.         Image: Service terms       C REFRESH*       Image: Authentication mode, regardless of the domain defaults.         Image: Service terms       C REFRESH*       Image: Authentication mode, regardless of the domain defaults.         Image: Service terms       C REFRESH*       Image: Authentication mode, regardless of the domain defaults.         Image: Service terms       C REFRESH*       Image: Authentication mode, regardless of the domain defaults.         Image: Service terms       C REFRESH*       Image: Service terms       Authentication mode, regardless of the domain defaults.         Image: Service terms       C REFRESH*       Image: Service terms       Built*in       Image: Service terms         Image: Service terms       C Reports       C Reports       C Reports       Service terms       Service terms       Service terms       Service terms		Groups	DOMAIN SETTINGS SAMI SETTING	S EXCLUSIONS LIST DETAILS				
Image: Service terms       O REFRESH       Image: ADD         Image: Service terms       O REFRESH       Image: ADD         Image: Service terms       USER       EMAIL       AUTH MODE         Image: Service terms       O REFRESH       Image: Service terms       Built-in         Image: Service terms       O REFRESH       Image: Service terms       Built-in         Image: Service terms       O REFRESH       Image: Service terms       Built-in         Image: Service terms       O REFRESH       Image: Service terms       SAML       Image: Service terms         Image: Service terms       Image: Service terms       Image: Service terms       Image: Service terms       Image: Service terms	Image: Service terms       O REFRESH       Image: ADD         Image: Service terms       O REFRESH       Image: ADD         Image: Service terms       USER       EMAIL       AUTH MODE         Image: Service terms       O REFRESH       Image: Service terms       Built-in         Image: Service terms       O REFRESH       Image: Service terms       Built-in         Image: Service terms       O REFRESH       Image: Service terms       Built-in         Image: Service terms       O REFRESH       Image: Service terms       SAML       Image: Service terms         Image: Service terms       Image: Service terms       Image: Service terms       Image: Service terms       Image: Service terms	2	Contacts						
USER       EMAIL       AUTH MODE         Christopher Hicks	USER       EMAIL       AUTH MODE         Christopher Hicks	Θ	Links	The following list of users will use the speci	fied authentication mode, regardless of the doma	ain defaults.			
Image: Prepares in the prepares	Image: Prepares in the prepares		Service terms	C REFRESH			+ .	ADD	
Notifications         USR-3473-9325         A05FOCC6-9CS8-11EB-A883-0242AC130003         Duitrim         I           Notifications         Frank Bowen USR-9127-4885         anthony.hoffman@cloudblue.com A05F0F4-9CS8-11EB-A883-0242AC130003         SAML         I	Notifications         USR-3473-9325         A05FOCC6-9CS8-11EB-A883-0242AC130003         Duitrim         I           Notifications         Frank Bowen USR-9127-4885         anthony.hoffman@cloudblue.com A05F0F4-9CS8-11EB-A883-0242AC130003         SAML         I		Helpdesk	USER	EMAIL	AUTH	NODE		
Reports         USR-9127-4885         A05F0F46-9058-11EB-A883-0242AC130003         SAML         :           Brows per page         10 + 11-2 of 2 < >         >         >         >	Reports         USR-9127-4885         A05F0F46-9058-11EB-A883-0242AC130003         SAML         :           Brows per page         10 + 11-2 of 2 < >         >         >         >	$\mathbf{>}$	Notifications			Built-in	I	:	
Rows per page 10 • 1-2 of 2 < >	Rows per page     10 ⋅     1−2 of 2 <	**	Reports			SAML		:	
		12	Single Sign On		Rows per	page 10 -	1-2 of 2 <	>	

Step 6

Clou	udBlue. 랴 s	ettings 🗸	HELP	۸. 🖬 🖡	Mighty Mick's LLC Distributor • Robert Balboa
Set	tings	← Domain Details		S VERIFY 🖍 CHANG	E DEFAULT AUTH MODE
Ê	General		Auth Mode		
**	Users	cloudblue.com Verified Built-In DOM-863-428			
1	Groups	DOMAIN SETTINGS SAML SETTINGS	EXCLUSIONS LIST DETAILS		
	Contacts				
Ð	Links		ied authentication mode, regardless of the domain def		
	Service terms	C REFRESH	EMAIL	+ ADD	
L V	Helpdesk	Christopher Hicks 🔌 🚖 USR-3473-9325	terra.hamilton@example.com A05F0CC6-9C58-11EB-A8B3-0242AC130003	Built-in E	
**	Reports	Frank Bowen USR-9127-4885	anthony.hoffman@cloudblue.com A05F0F46-9C58-11EB-A8B3-0242AC130003	SAML :	
Б.	Single Sign On		Rows per page	10 ▼ 1-2 of 2 < >	
0	Audit Trail				
1					
			Step 7		

 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
- 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 *builtin* 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:

Sett	tings	Users @				+ ,	ADD USE
Ê	General	All users 🗸 🗸 C REFRESH	≂ FILTER <sup>1</sup> 4 SORT III COLUMNS		Rows per page	e 10 - 1-1 of 1	
**	Users	NAME -	EMAIL -	AUTH MODE 👻	JOINED AT 👻	LAST SIGN IN *	
2	Groups	Robert Balboa 🔧 💼 UR-920-297-557	rbalboa@frontstreet.com	Built-in	07/06/2021 7:52 AM	07/06/2021 7:52 AM	1
1	Contacts	<					
Ð	Links				Rows per page	e 10 ∓ 1−1 of 1	< >
	Terms						
	Helpdesk						
***	Reports						
12	Single Sign On						

CloudBlue	፰는 Settings ∨		🕜 HELP	۰		Mighty Mick's LLC Distributor - Robert Balboa
	Users @					+ ADD USER
🛱 General	All users 🗸 🕐 RE	FRESH 🗢 FILTER 14 SORT 🗰 COLUMNS			Rows per pa	ige 10 - 1−1 of 1 < →
Croups	Add user – Step	1			_	LAST SIGN IN
Contacts	1 General	Name *				07/06/2021 7:52 AM
GD Links	General	Robert Balboa Jr.				10 ~ 1-1 of 1 < >
Terms	2 Group	Email * rbalboajr@frontstreet.com				
Helpdesk	3 Summary					
*** Reports						
Single Sign O	n		CANCE	L	NEXT	

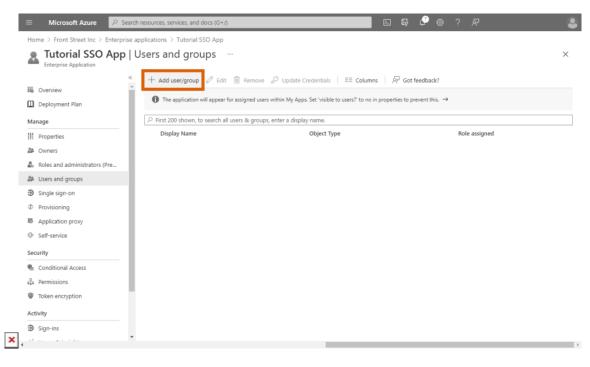
Step 1

fome > Front Street Inc >		
Series All users (Pl Front Street Inc - Azure Active Director	ary	2
All users (Preview)	+ New user + New guest user 🗅 Bulk operations 🗸 🖒 Refresh 🖉 Reset password 🖾 Per-user MFA 🗎 Delete user   🎫 Colu	umns
Deleted users (Preview)	$\circlearrowright$ This page includes previews available for your evaluation. View previews $\rightarrow$	
Password reset		
User settings	1 user found	
K Diagnose and solve problems	Name $\uparrow_{\downarrow}$ User principal n $\uparrow_{\downarrow}$ User type Directory synced Identity issuer Company name Creation	on type
Activity		
Sign-ins		
Audit logs		
Bulk operation results		
roubleshooting + Support		
New support request		

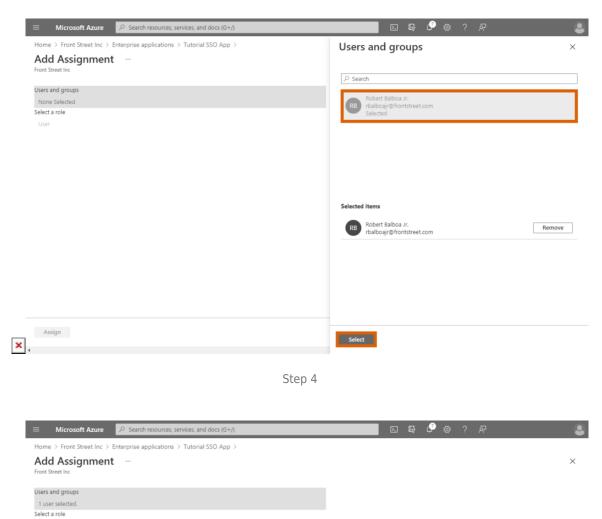
×

Step 2

	Front Street Inc > Users >					
New						
₽ Got	feedback?					
۲	Create user Create a new user in your organization. This user will hav user name like alice@frontstreetinc.onmicross I want to create users in bulk		Invite user Invite a new guest user to collaborate with your organi The user will be emailed an invitation they can accept in to begin collaborating.			
	I want to create users in bulk		I want to invite guest users i	in bulk		
Help me d			i vant to invite guest users i	in bulk		
Help me d	lecide		i vant to invite guest users i	in bulk		
	iecide	rbalboajr	vant to invite guest users i vant to invite guest users i v @ frontstreet.com The domain name I nee	~ 1		
Identity	lecide , 2 ° ⊙	rbalboajr Robert Balboa J	I want to invite guest users i	~ 1		
<b>Identity</b> User name	ecide , e * © D		I want to invite guest users i	ed isn't shown here		

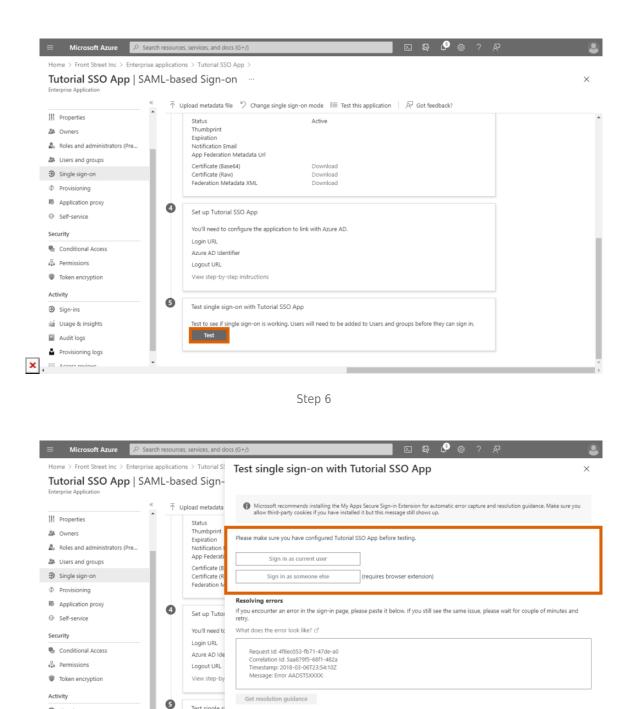


Step 3



Select a role

Assign , Step 5



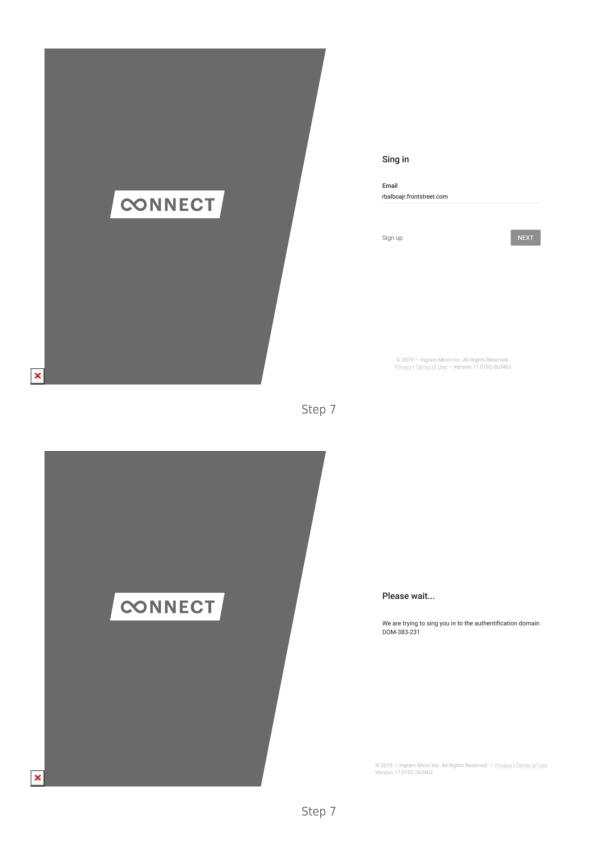
Test single si

Test to see if Test

ியி் Usage & insights

Audit logs Provisioning logs

S= Accore rouid



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.

- 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.