# Trusted Connection Guide

**Identity Management Systems (IdM) integration documentation**

verizon business

# Contents

# Directions for integrating IDM applications

Trusted Connection requires integration with an Identity Management System to identify users in your organization and to apply security policies at organization, group or individual user basis. This document explains the steps and information needed to integrate Trusted Connection with some popular IDM applications. Instructions include IDMs that support both the Security Assertion Markup Language (SAML) and Lightweight directory access Protocol (LDAP) autentication protocols. Click on the link to the IDM in the table to jump to the appropriate section with details on how to integrate Trusted Connection for each of these IDMs. Note that for the most part Trusted Connection will need to be manually integrated with the IDM.

| IDM product | Supported protocol | Group creation (Manual / Automated) |
|---|---|---|
| **Microsoft EntraID** | SAML | Manual |
| **Okta** | SAML | Manual |
| **Okta** | SAML + LDAP | Automated |
| **Ping Identity** | SAML | Manual |
| **Windows AD/OpenLDAP** | LDAP | Automated |
| **Other*** | LDAP or SAML | Manual or Automated |

*Other Identity Providers may be applicable if SAML or LDAP are supported

**Key point:** Trusted Connection requires integration with an Identity Management system in order to recognize the users in your organization and to assign Trusted Connection security policies to those users in your organization.

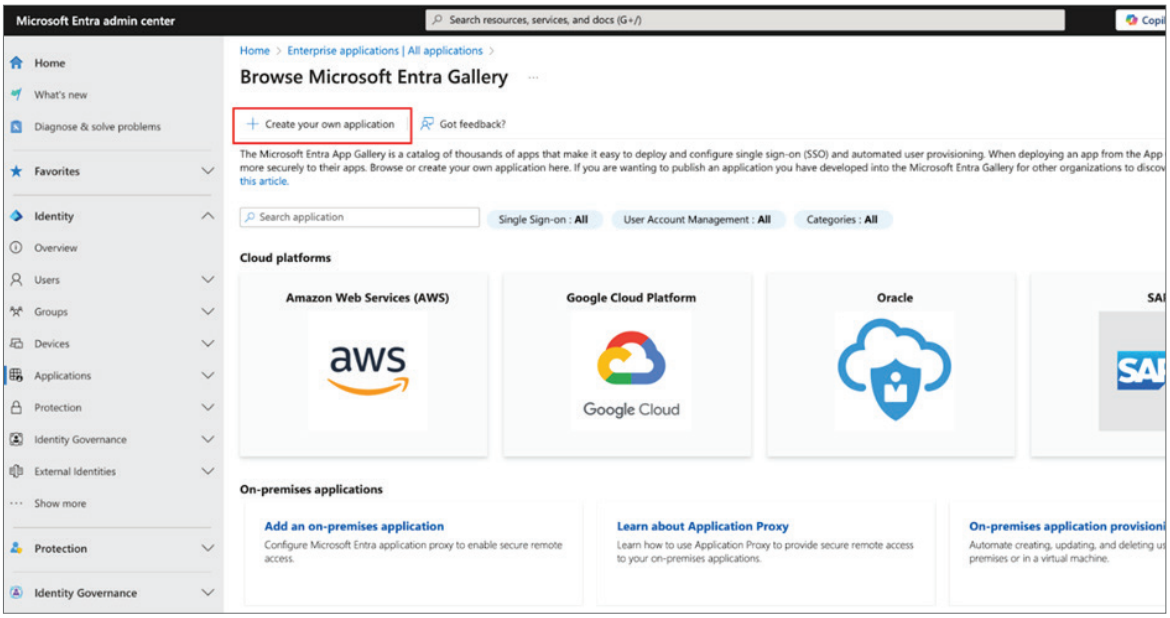
- **Trusted Connection with SAML-only:** Allows creation of Trusted Connection policies that apply to the organization as a whole and policies that target specific User Groups that have been assigned to Trusted Connection in your IDM. User Groups must be manually created within Trusted Connection to match the same User Groups in your IDM.
- **Trusted Connection with LDAP:** Allows creation of Trusted Connection policies that apply to the organization as a whole and policies that target specific User Groups, as well as, specific individuals that have been assigned to Trusted Connection in your IDM. Users Groups and Individuals are automatically synchronized between Trusted Connection and your IDM.

## Microsoft EntraID integration for SAML authentication

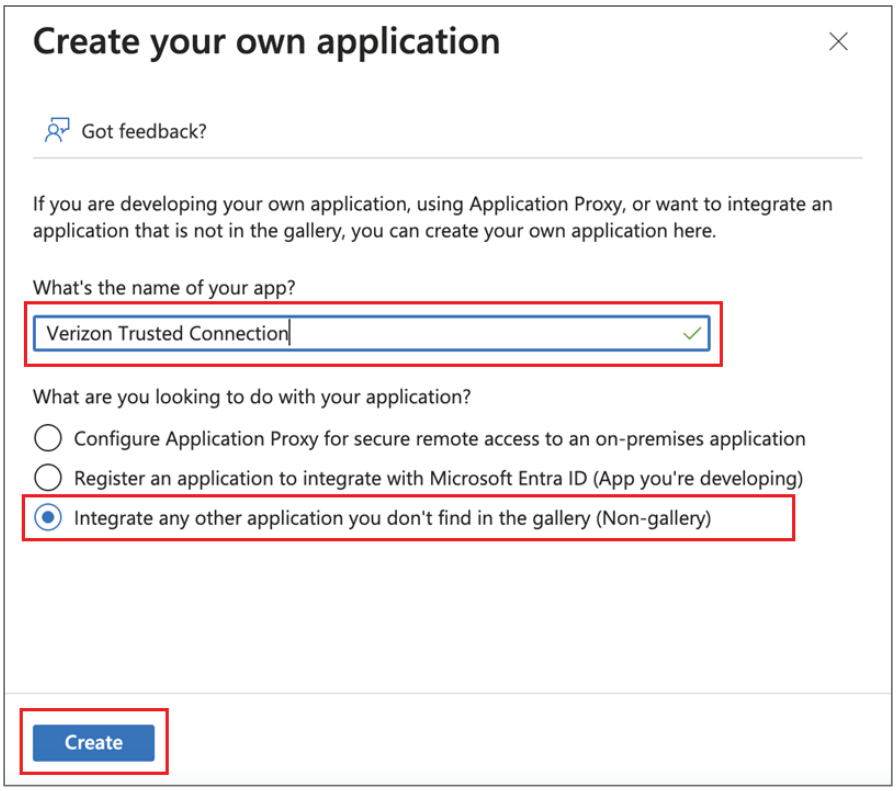
The following screens go through the steps required to allow Trusted Connection to sync with Microsoft EntraID.

You will need to set up two browser windows. One into your **Microsoft Admin admin center** and the second into the Verizon Trusted Connection portal. Perform the following steps from within the Microsoft Entra admin center

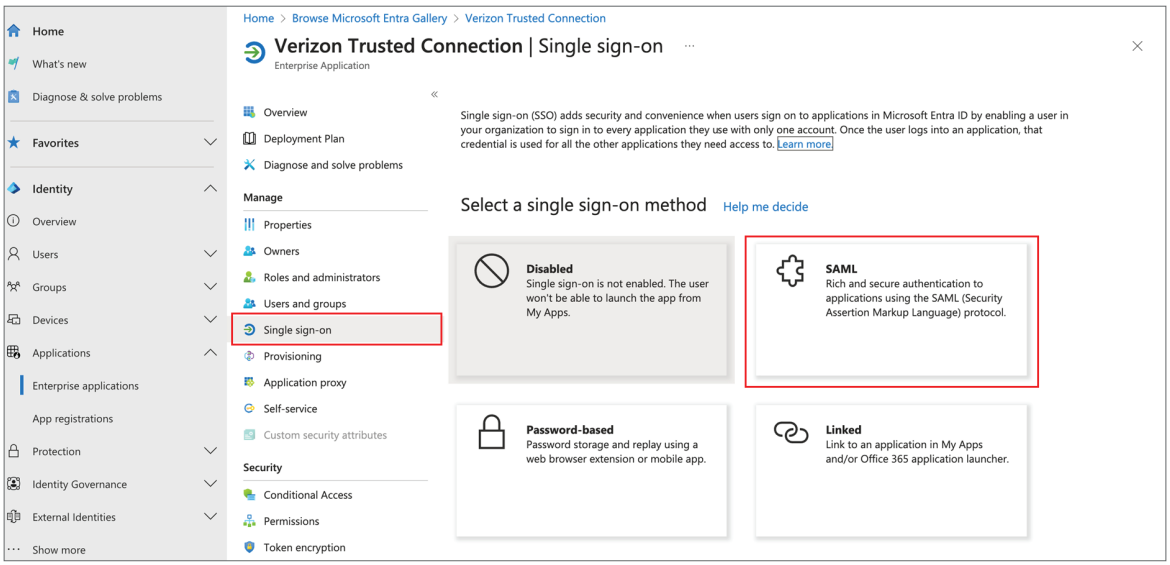
**Step 1:** Go to **Enterprise applications** in the Microsoft Entra admin center, then click on "**Create your own application**".



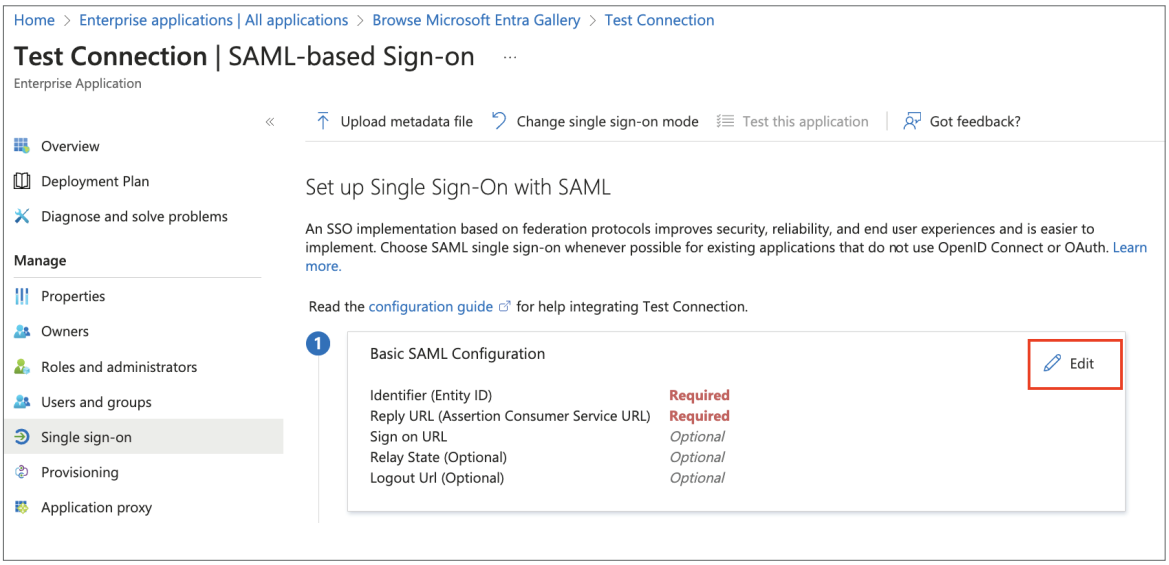
**Step 2:** Name your **new application** as **Verizon Trusted Connection**. The application is not in the Entra ID gallery at this time. Click the radio button for Integrate any other application you don't find in the gallery and select **"Create"**.




**Step 3:** Then choose **"Single sign-on"** from the left side of the Application dashboard and select the **SAML** tile.



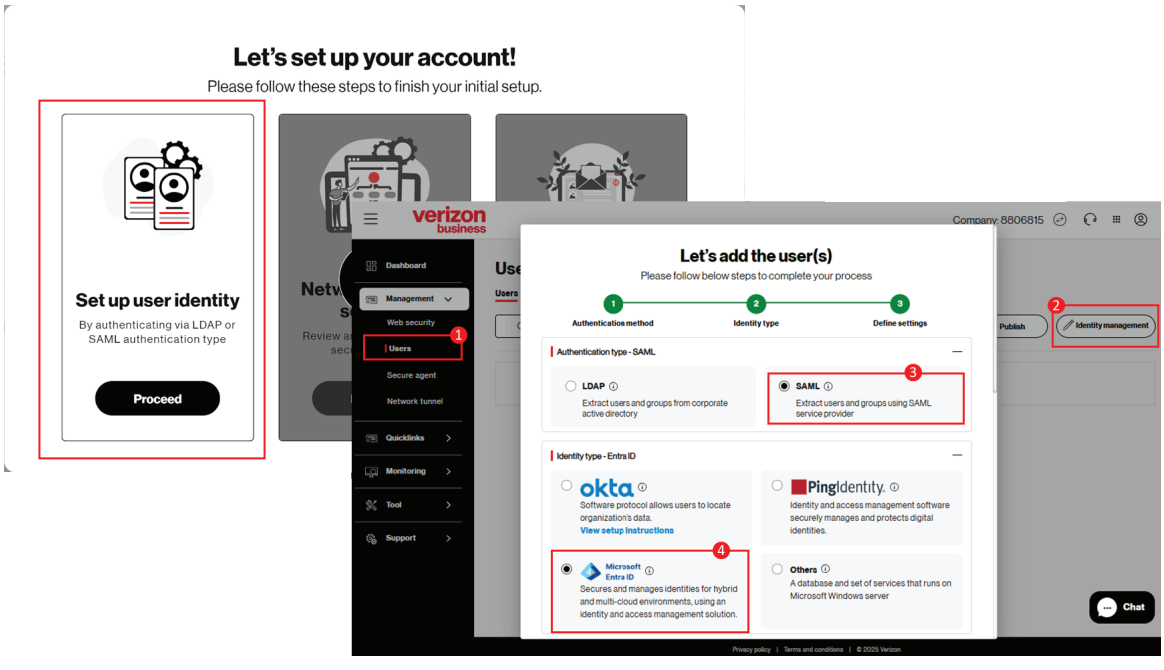
**Step 4:** Click on **“Edit”** within the **Basic SAML Configuration** section.




For the next step, you will need to open a browser for **Trusted Connection** at trustedconnection.verizon.com.

**Step 5:** Navigated to Set up user identity from the setup wizard or the **Trusted Connection** menu system as shown below:

Accessing user identity via the set up wizard

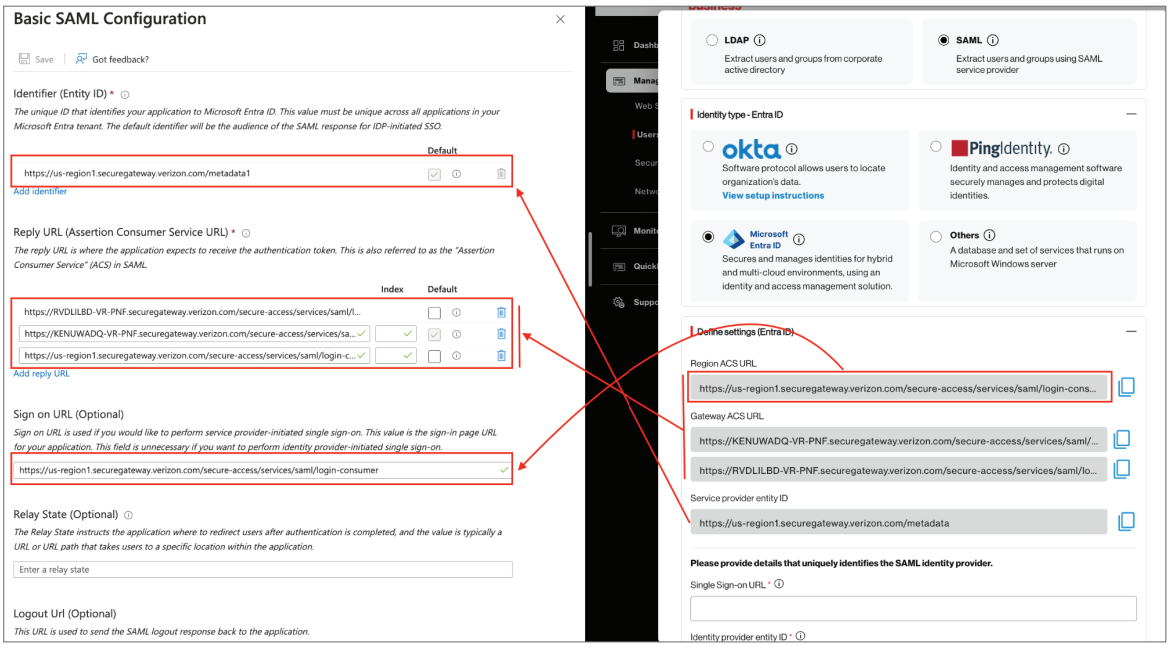



Accessing user identity via the main menu

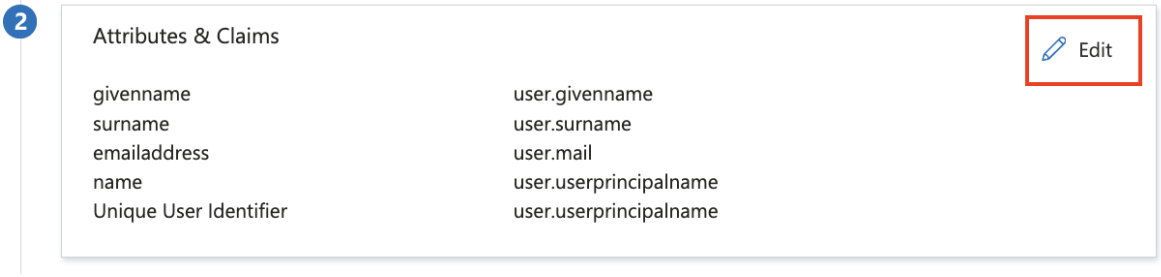
**Step 6:** You will now copy information from the Trusted Connection browser into your Entra ID application setup. Keep the Entra Basic SAML Configuration tab open. Perform the following steps:

1. Use the **“Add Identifier”** link to create a blank Identifier (Entity ID) field. Copy the Trusted Connection Service Provider Entity ID field to the Entra Identifier (Entity ID) field .
2. Use the **“Add reply URL”** link to create three blank Reply URL fields. Copy the Trusted Connection Regional ACS URL and paste into two places, the Entra Sign-on URL and the first Reply URL (Assertion Consumer Service URL) field.
3. Copy the two Trusted Connection Gateway ACS URLs and paste into the second and third Reply URL (Assertion Consumer Service URL) fields

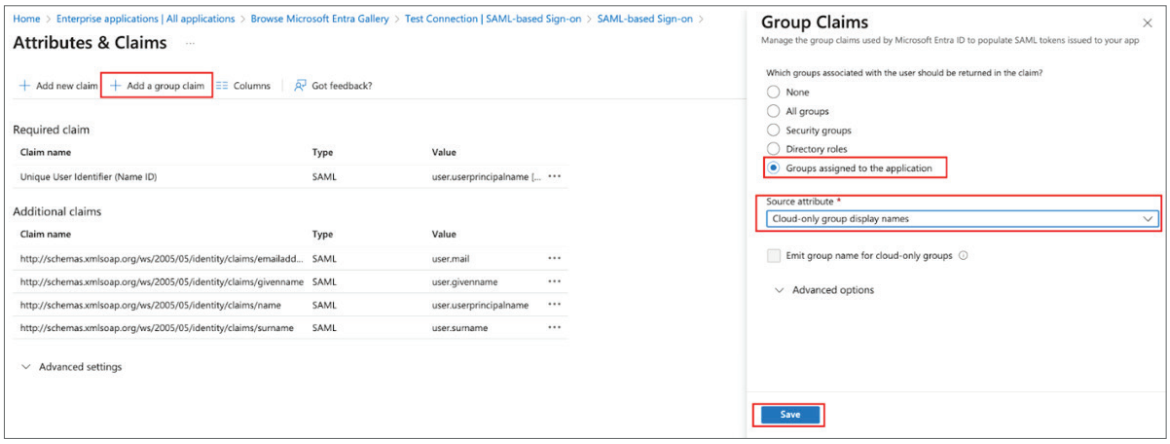
Then click **“Save”** in Entry ID.




**Step 7:** Once the previous step is saved, you’ll be back to the Set-up Single sign-on with SAML screen in the Entra portal. Click “**Edit**” on **Attributes & Claims** to add group claim.

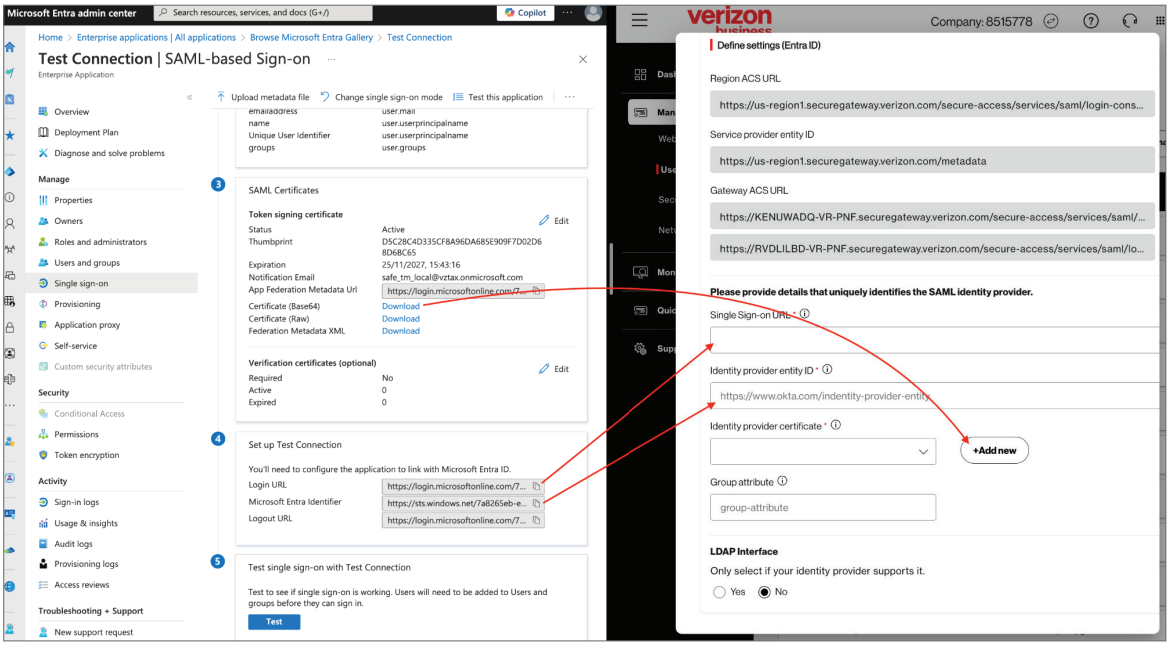


**Step 8:** Add a group claim as shown in the configuration below and then click **“Save”**.



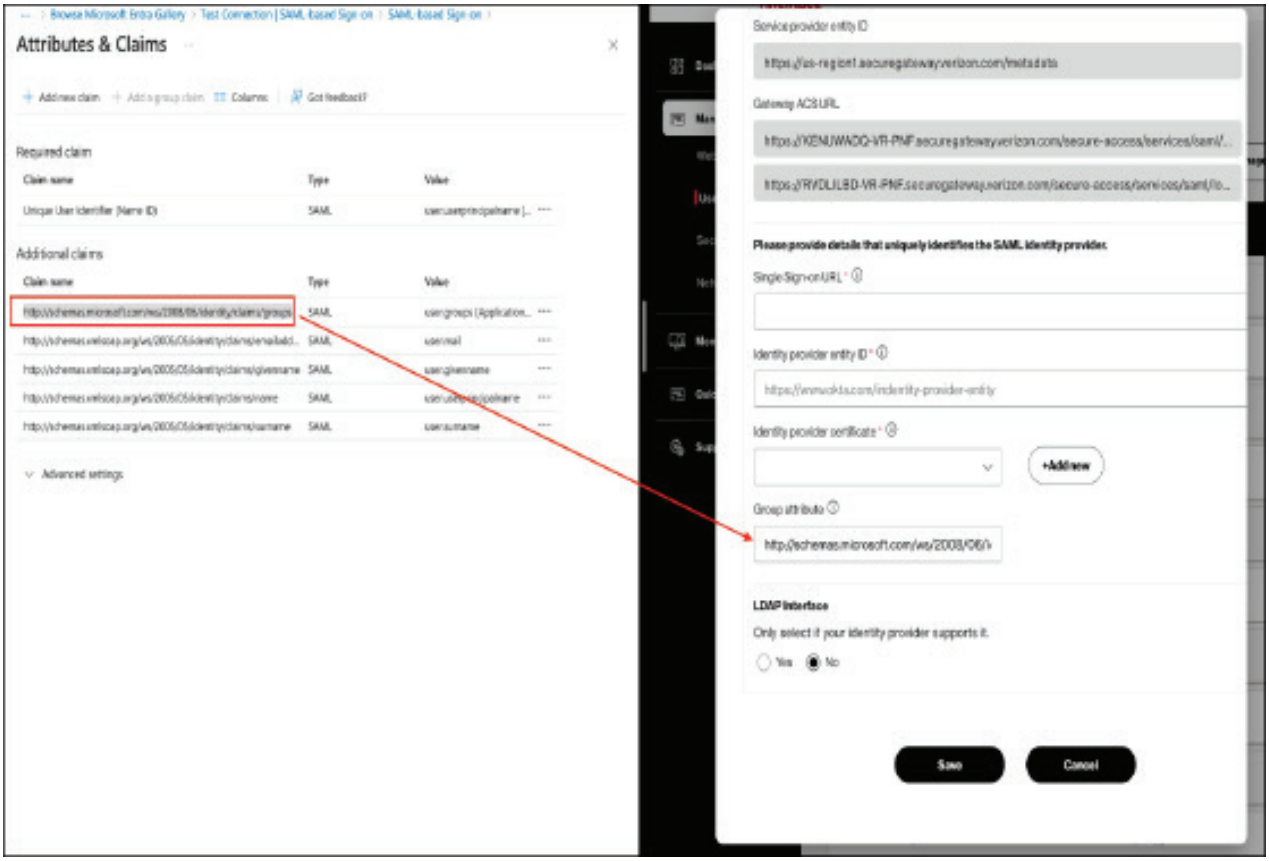

**Step 9:** From your Entra tab, navigate to the SAML Certificate section. Download the Certificate (Base64) and upload it to the Identity Provider certificate field in the Trusted Connection Portal by clicking **“+Add new”**. From the Set up Verizon Trusted Connection section (the name is based on what you entered) copy the Login URL and Microsoft Entity Identifier URLs to the Trusted Connection Single Sign-on URL and Identity provider entity ID fields as shown.

**Important note**
Remove the last “/” when pasting the Microsoft Entra Identifier onto the “Identity Provider EntityID” section of the portal.



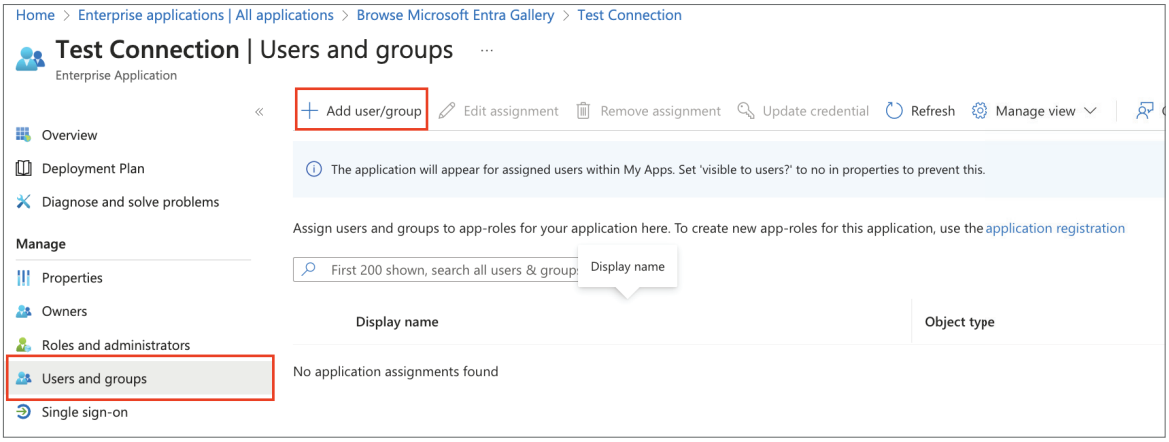
**Step 10:** Go back to the Attributes and Claims section from Step 7. Copy the user.groups claim name and paste it in the Trusted Connection portal's Group attribute field as shown below.

You can now click **"Save"** on the Trusted Connection Identity Provider tab.

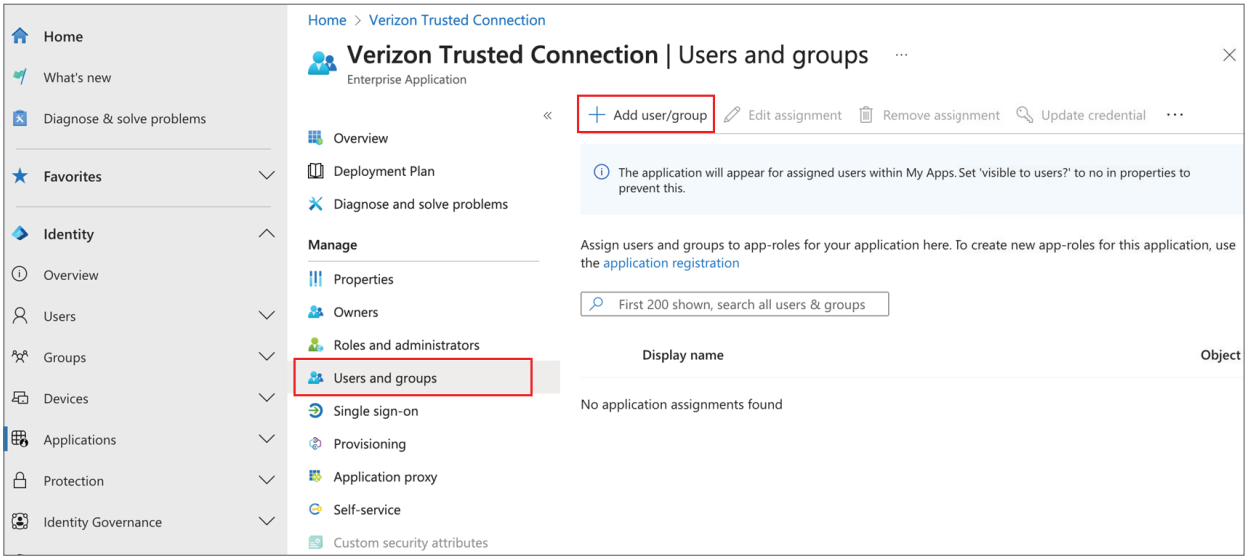



**Step 11:** Now, Add your user groups to the newly created Verizon Trusted Connection application

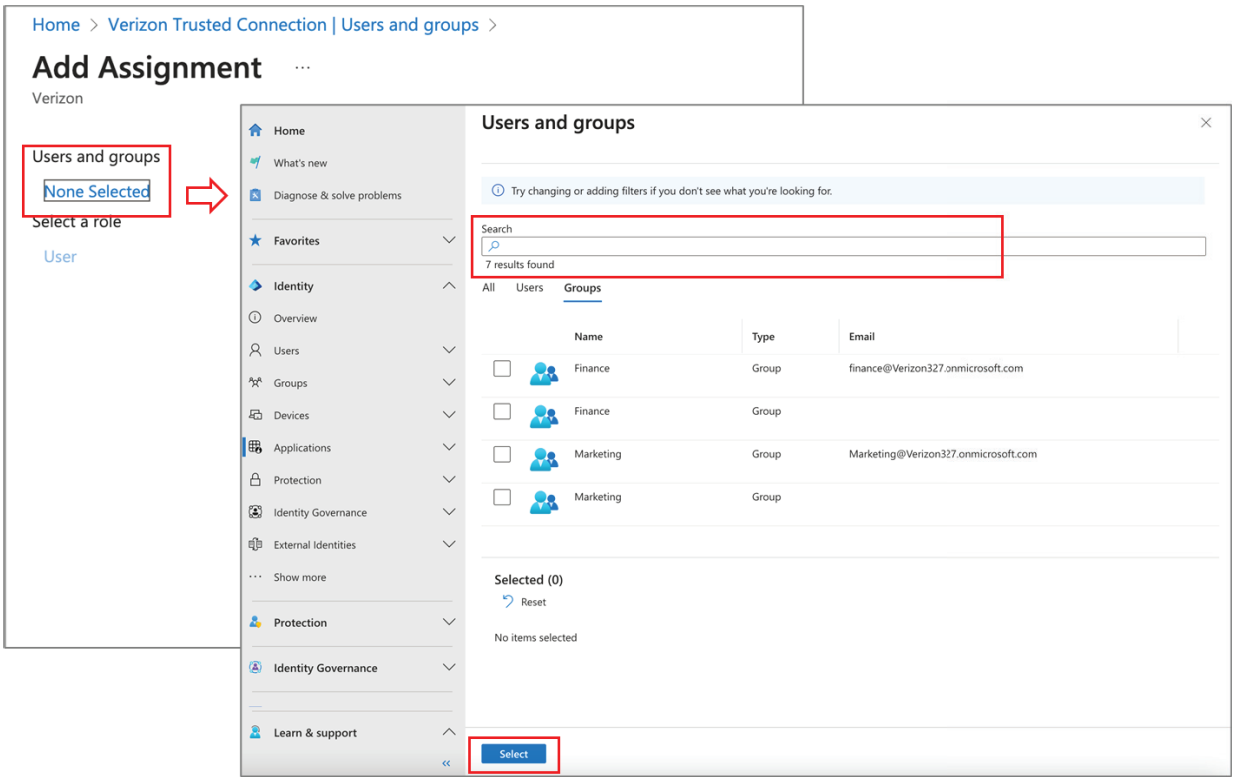
**Step 11a:** Go to Users and groups in the app dashboard and click on **"+ Add user/group"**



**Step 11b:** Click on **“None Selected”**, **Search** for the desired group and then click on **“Select”**.

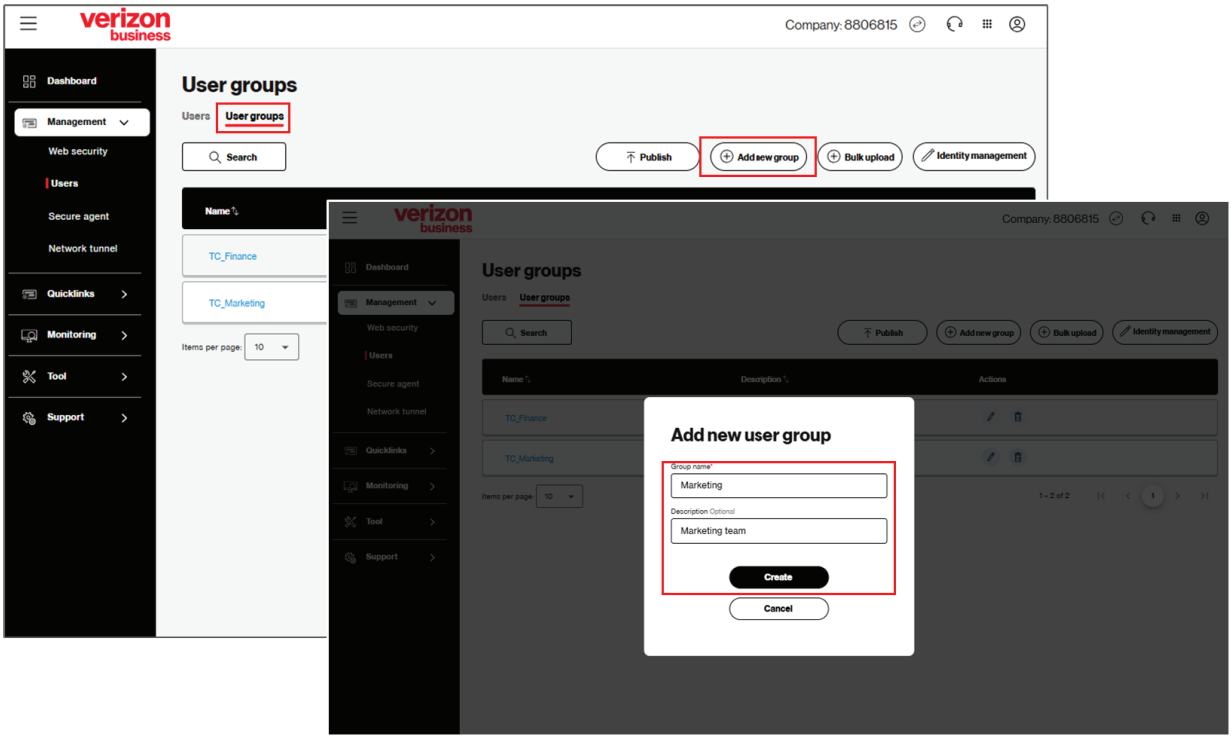



**Step 11b:** Click on **“None Selected”**, **Search** for the desired group and then click on **“Select”**.



**Step 12:** Once all the above steps have been completed, go back to the Trusted Connection Setup Wizard to complete the onboarding process.

Finally, you must create User Groups in Trusted Connection that match the identical User Groups in Entra ID. Navigate the Management > Users on the left side of the screen. Select **“User Groups”** and press the **“(+) Add new group”** button to add your groups, one at a time.

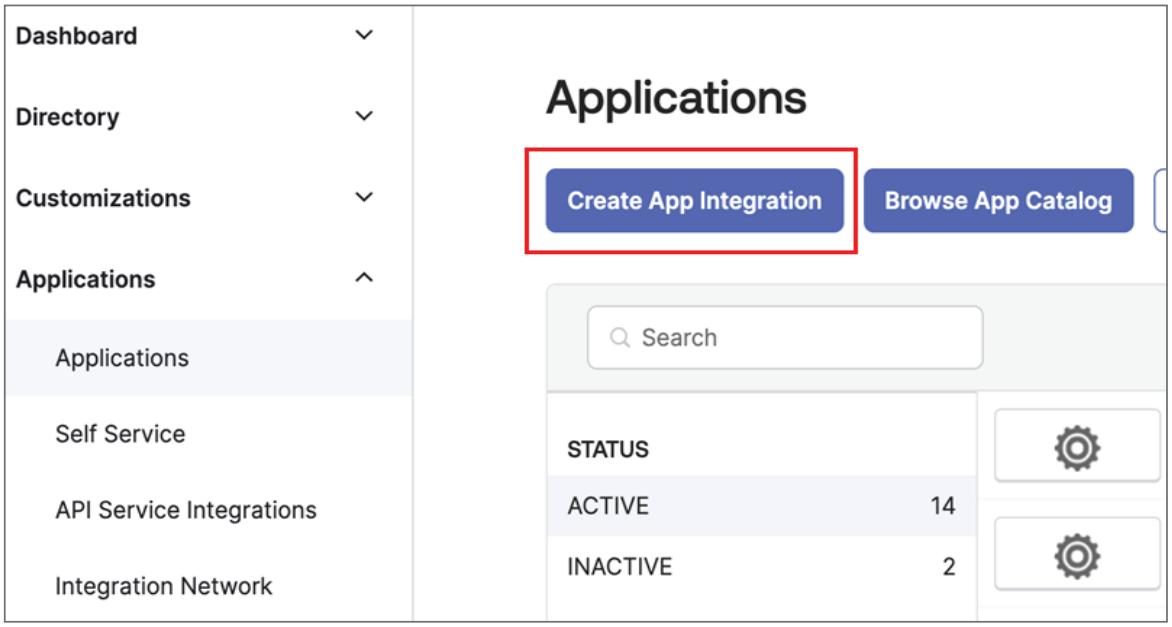


## Okta Integration for SAML Authentication

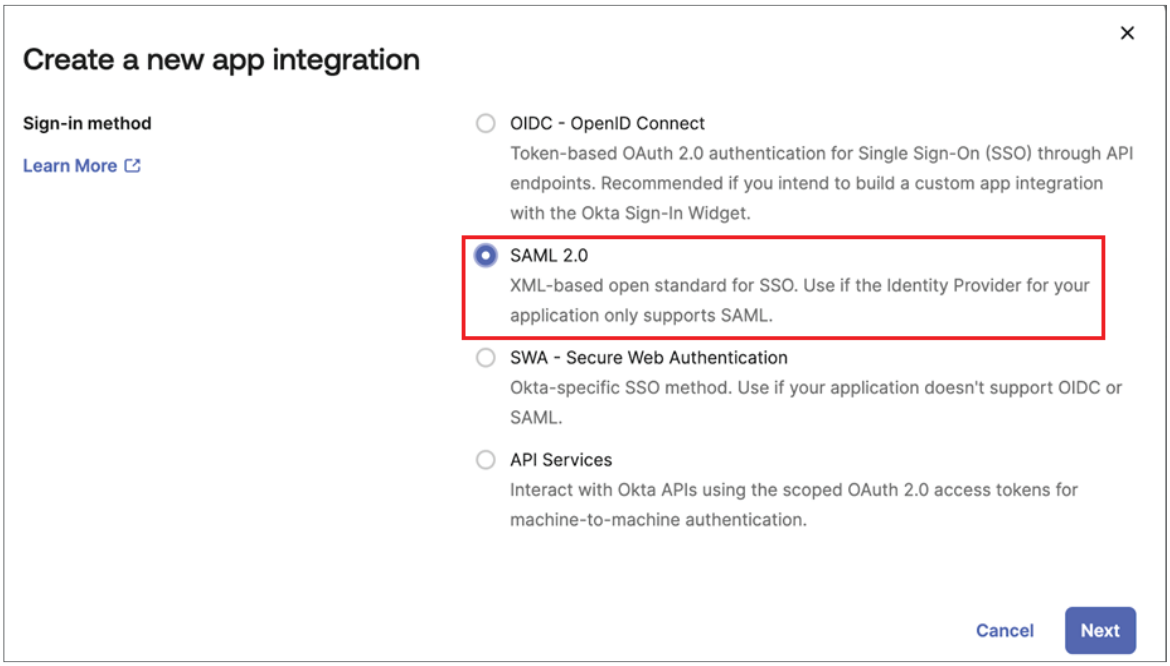
The following steps demonstrate how to integrateTrusted Connection with Okta, for SAML authentication. Instructions on how to integrate with the OKTA LDAP interface are located in the next section.

You will need to set up two browser windows. One into your Okta Single Sign-On Dashboard and the second into the Verizon Trusted Connection portal. Perform the following steps from within the Okta Dashboard.

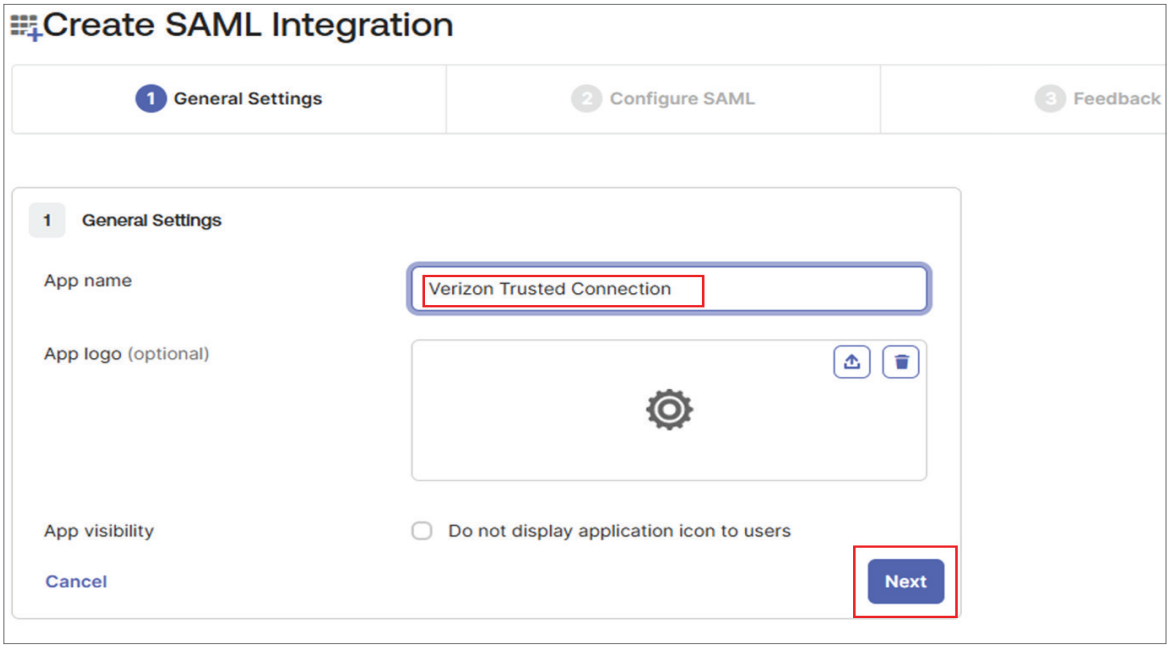
**Step 1:** Login to the Okta Dashboard, then click on the **Applications** menu on the left side of the page, select "**Create App Integration"**.



**Step 2:** On the **Create a new app integration** screen, select **SAML 2.0** and then click **“Next”**.



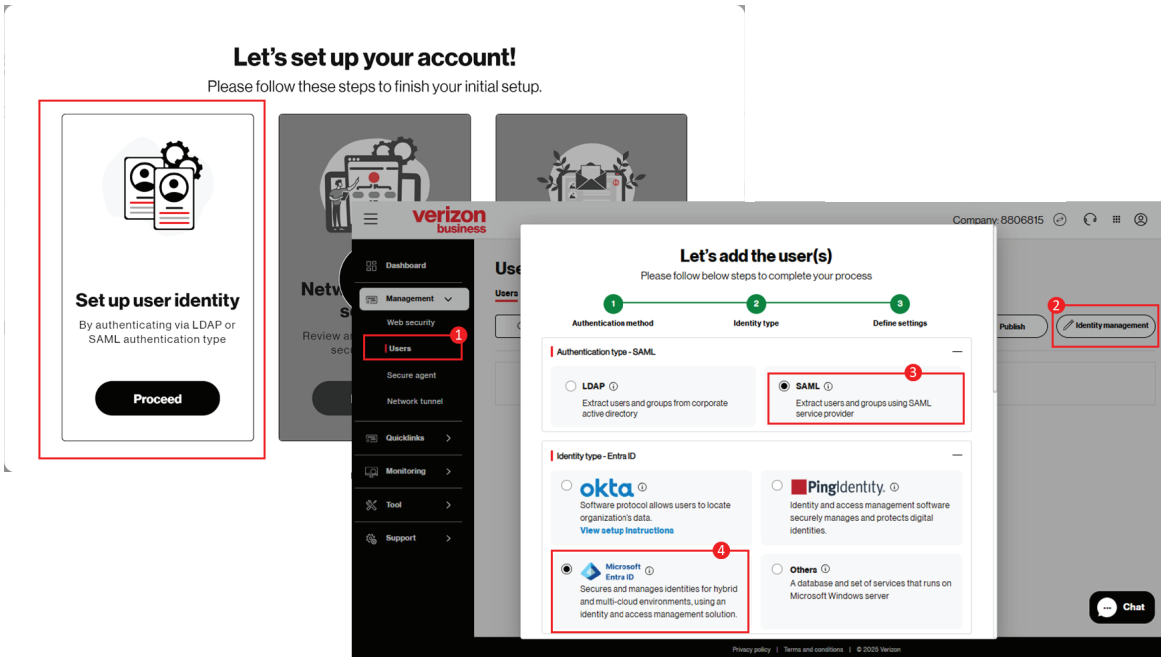

**Step 3:** In the box next to App name, enter the **App name** (as Verizon Trusted Connection) and then click **“Next”**.



For the next step, you will need to open a browser for Trusted Connection at trustedconnection.verizon.com.

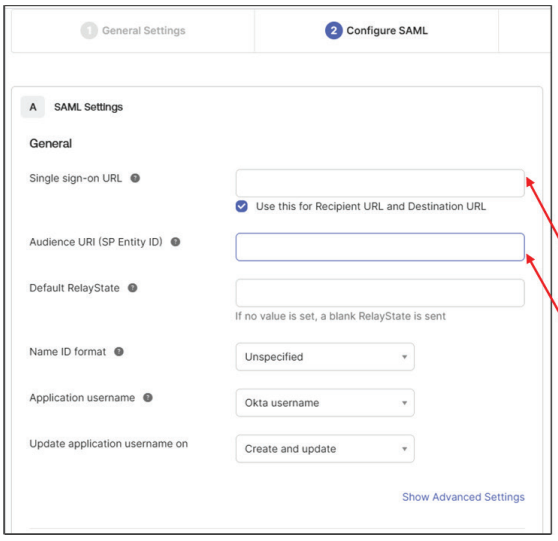
**Step 4:** Navigated to Set up user identity from the setup wizard or the Trusted Connection menu system as shown below:

Accessing user identity via the set up wizard

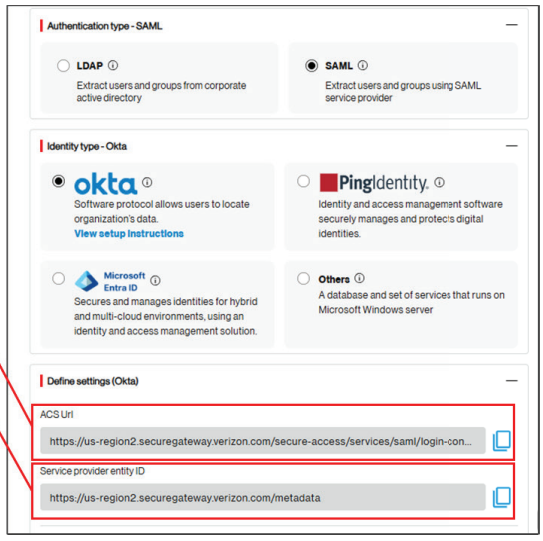



Accessing user identity via the main menu

**Step 5:** Copy the SSO URL and Entity ID from the Trusted Connection browser tab into the Okta browser tab as shown below.




Entry ID browser tab




Trusted Connection browser tab

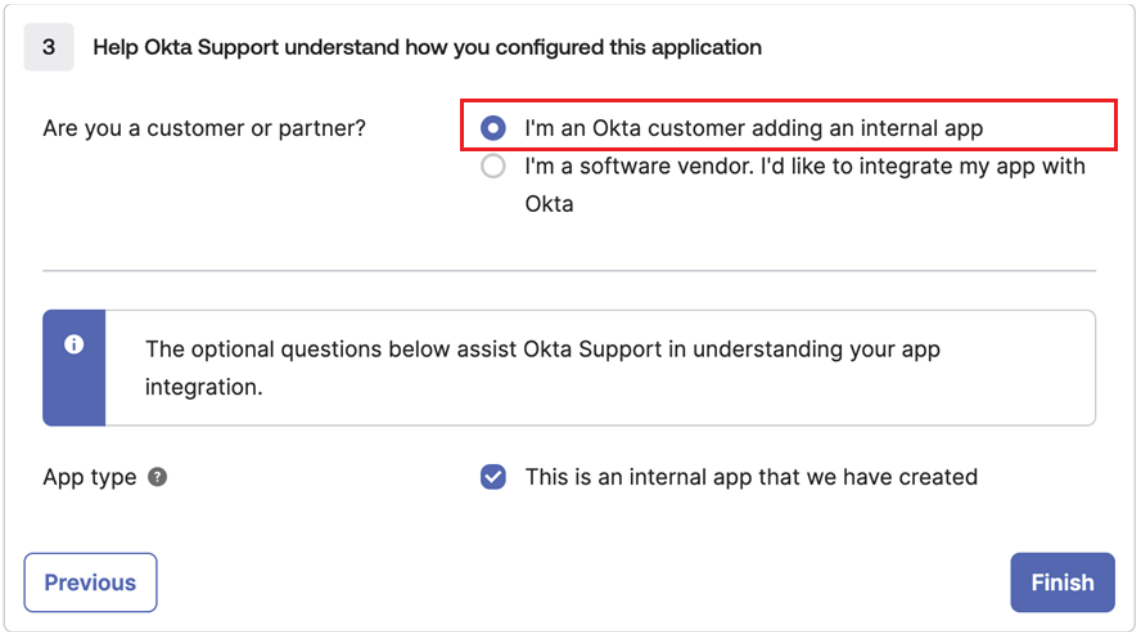
After adding the urls in Okta, keep everything else as default.

**Step 6:** In order to release the group names in the Okta SAML assertion to Trusted Connection, you will need to create a group attribute statement in Okta and assign that same attribute in Trusted Connection. Scroll down within the open Okta screen and Trusted Connection screen to assign the groupname attribute to both.

Optionally, Okta gives you the ability to filter which groups are shared with Trusted Connection. For example you could create unique security user groups that only contain the string “TrustedConnection”

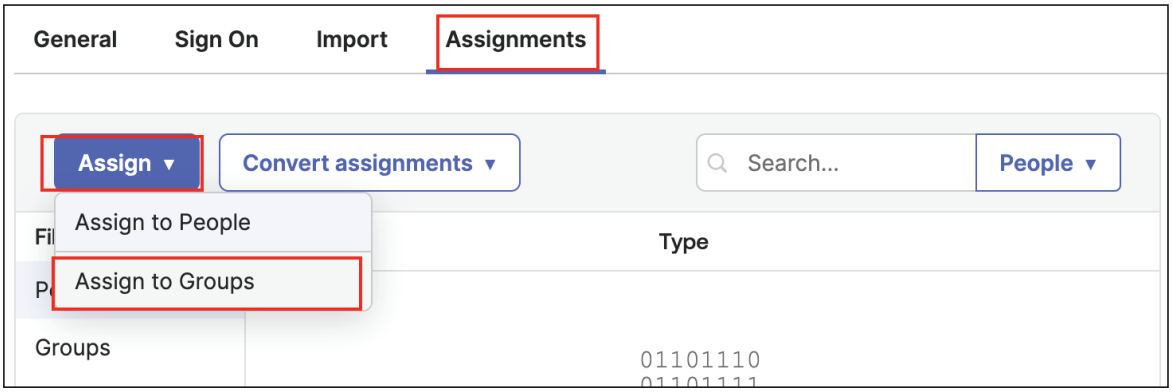
**Note** - Skip this step if you are using Okta LDAP.


**Step 7:** Set the following items to their default values and click on finish.
This creates an app integration in Okta

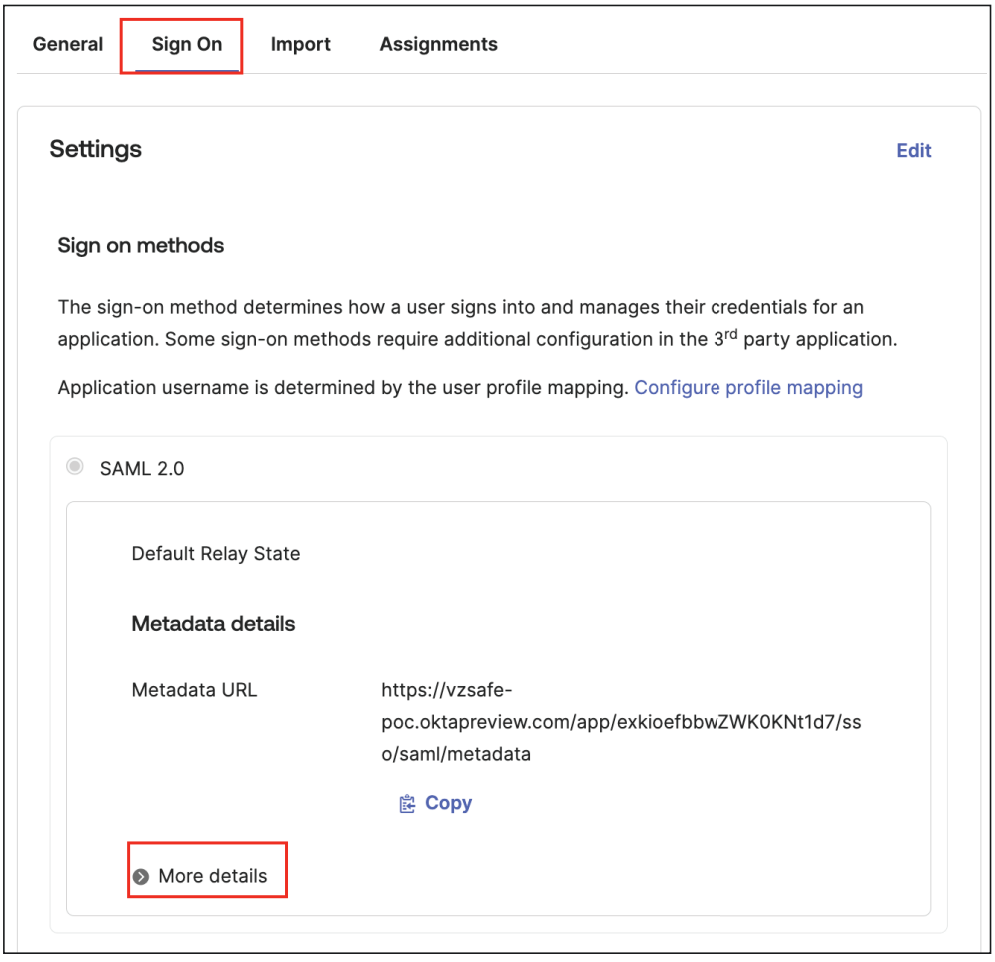


**Step 8:** From within Okta, assign the user groups that require Trusted Connection support to be assigned to the new application.

Go to **Assignments** > **Assign** > **Assign to Groups** and select the desired group.



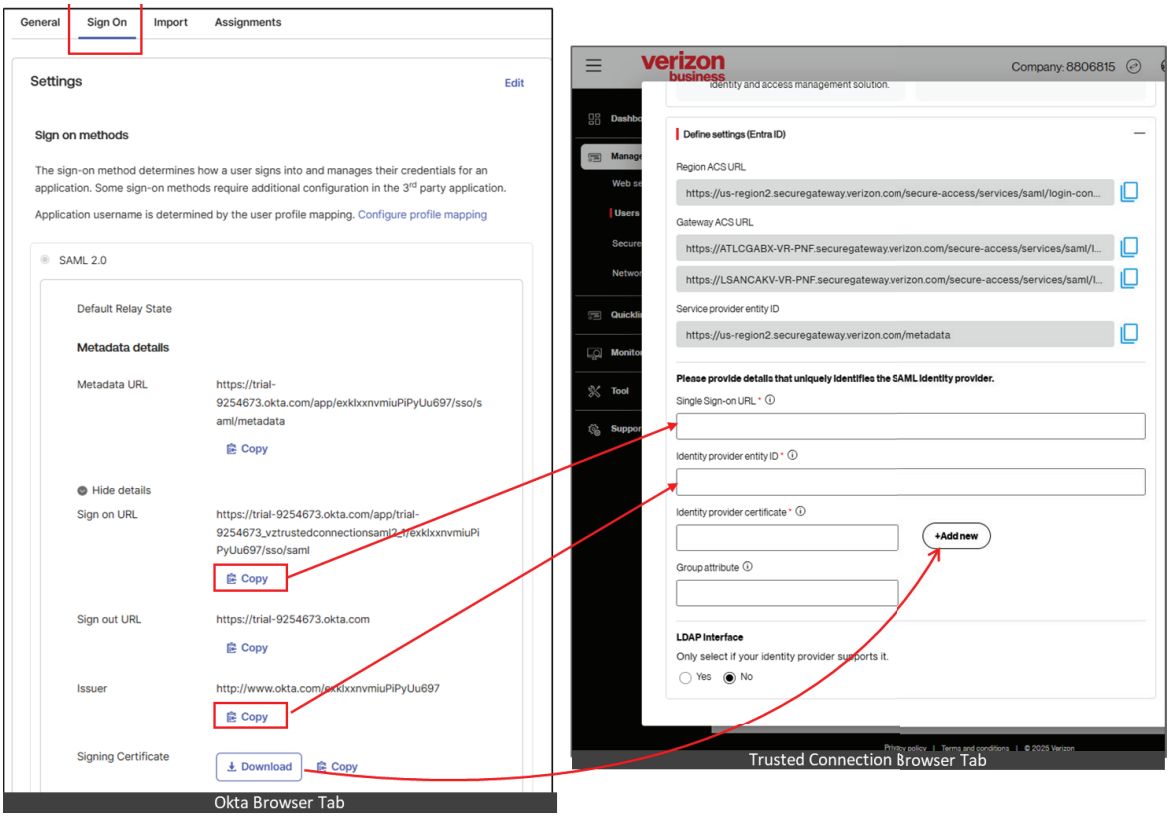

**Step 9:** Go to **“Sign On”** and click on ”**More details**”.



**Step 8a:** Copy and paste the **“Sign On URL”** and **“Issuer”** URL from Okta to the corresponding Trusted Connection fields, as shown.

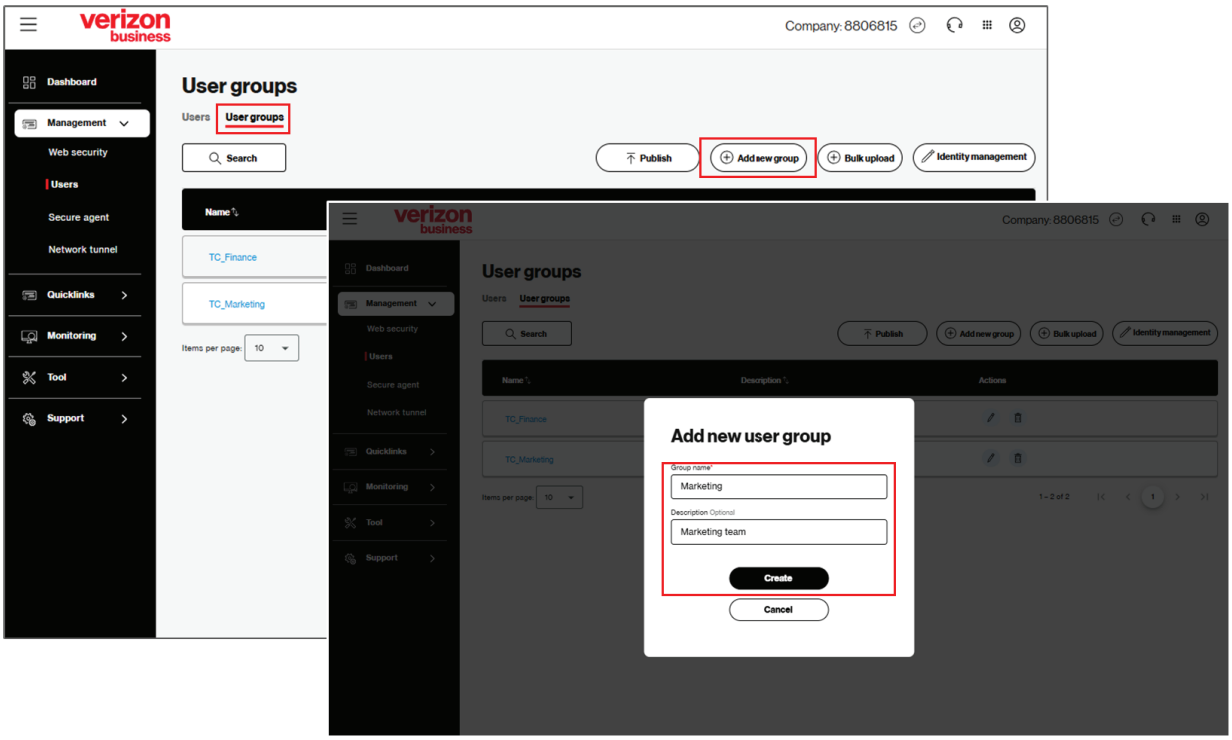
**Step 8b:** Download the certificate by pressing the Okta **“Download”** button as shown. When saving the certificate, change the file extension format from .cert to .cer (as .cert is not acceptable in Trusted Connection). From within the Trusted Connection tab upload the certificate and add it to in the “Identity provider certificate” field by clicking on **“+Add new”**.

Then **“Save”** the configuration in the Trusted Connection.



**Step 9:** Once all the above steps have been completed, go back to the Trusted connection portal to complete the onboarding process.

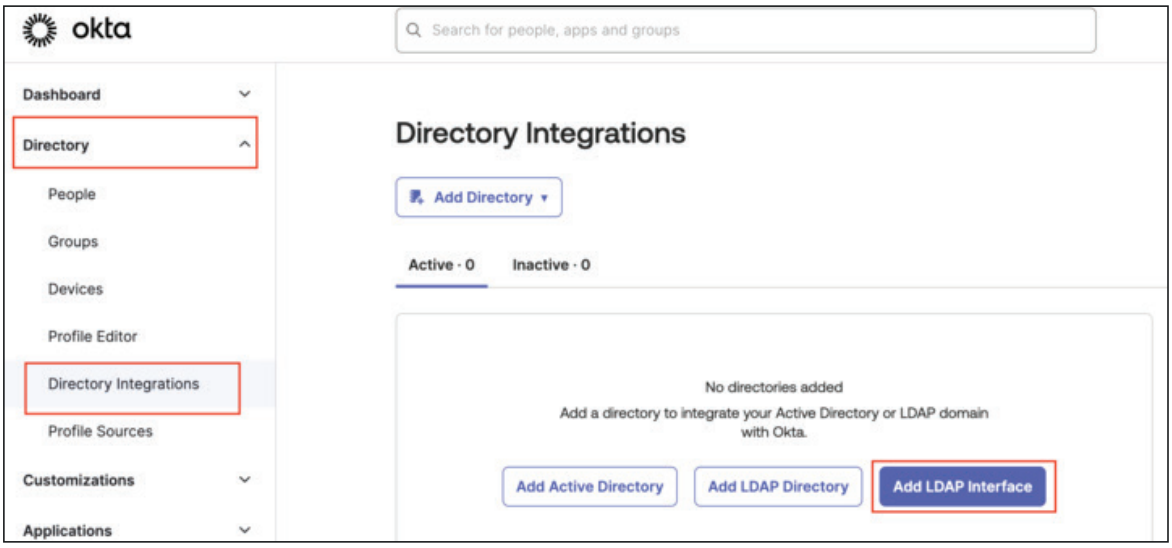
Finally, you must create User Groups in Trusted Connection that match the identical User Groups in Entra ID. Navigate the Management > Users on the left side of the screen. Select **“User Groups”** and press the **“(+) Add new group”** button to add your groups, one at a time.



## Okta LDAP interface configuration

The following screens go through the steps required to allow Trusted Connection to sync with Okta, specifically the LDAP Interface configuration. Instructions on how to integrate with OKTA SAML Authentication are outlined in the previous section.

**Step 1:** First log into the OTKA dashboard to enable the LDAP interface of your Okta tenant by choosing Directory in the Menu on the left side of the screen. Then click on **“Directory Integrations”**, then click on **“Add LDAP Interface”**.



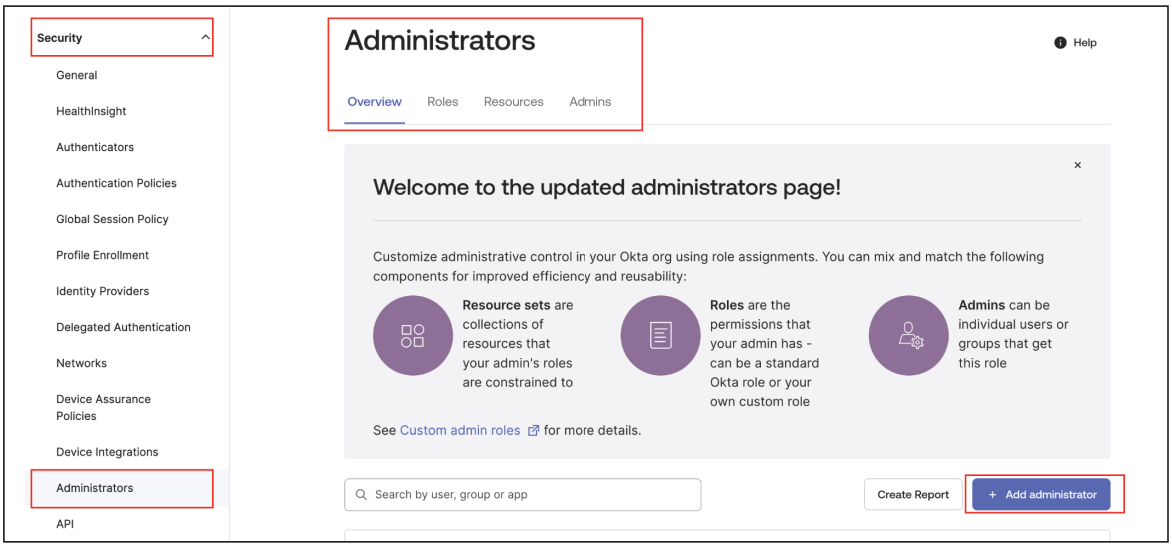

**Step 2:** The LDAP Interface is then enabled and will display the Host, Bind DN and Base DN values as shown below.

**Note**
The values shown below are samples only. The actual attributes values will be different for each Okta instance.

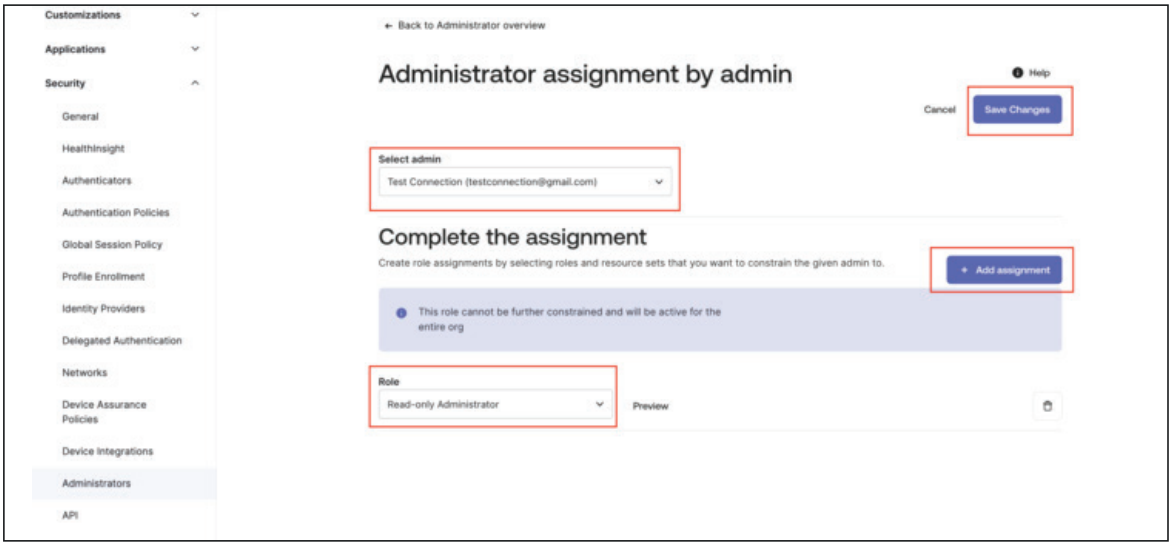
**Step 3:** Create a service account user for Bind authentication with minimum read-only administrator privileges.

**For example:** The user shown was created with the name “Testconnection” and assigned read-only admin privileges. Any name for this user is acceptable, but it is recommended that it be a name that will help the administrator remember what it is for in the future.

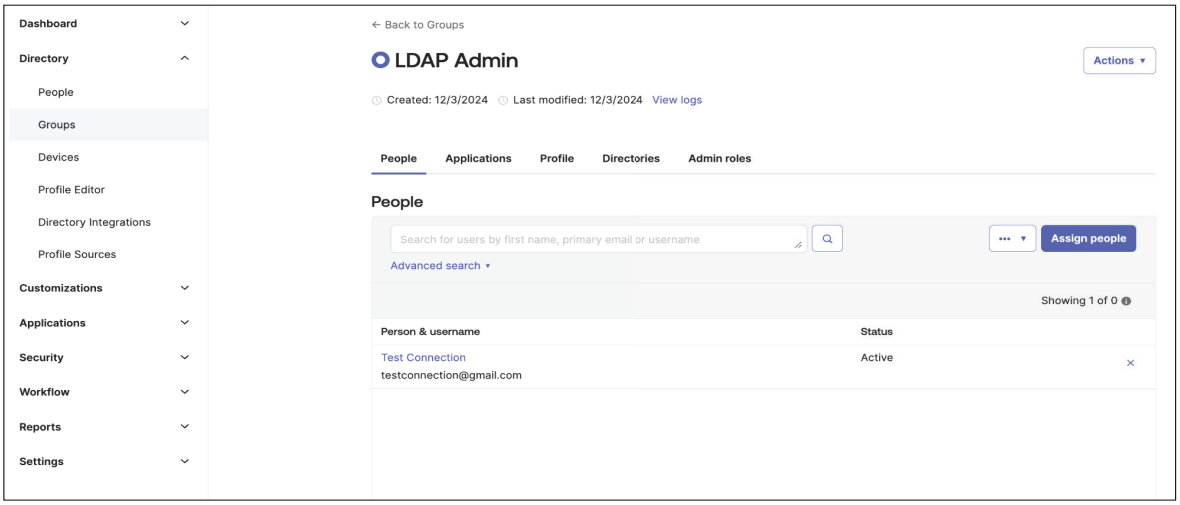
**Step 3a:** After the user has been created, the next step is to assign them the correct privileges to allow the proper authentication processes to work. Follow the Dropdown Menu on the left side of the screen and click on Security, then Administrators. Once in the Administrator Overview screen, Click on the **“Add administrator”** button.



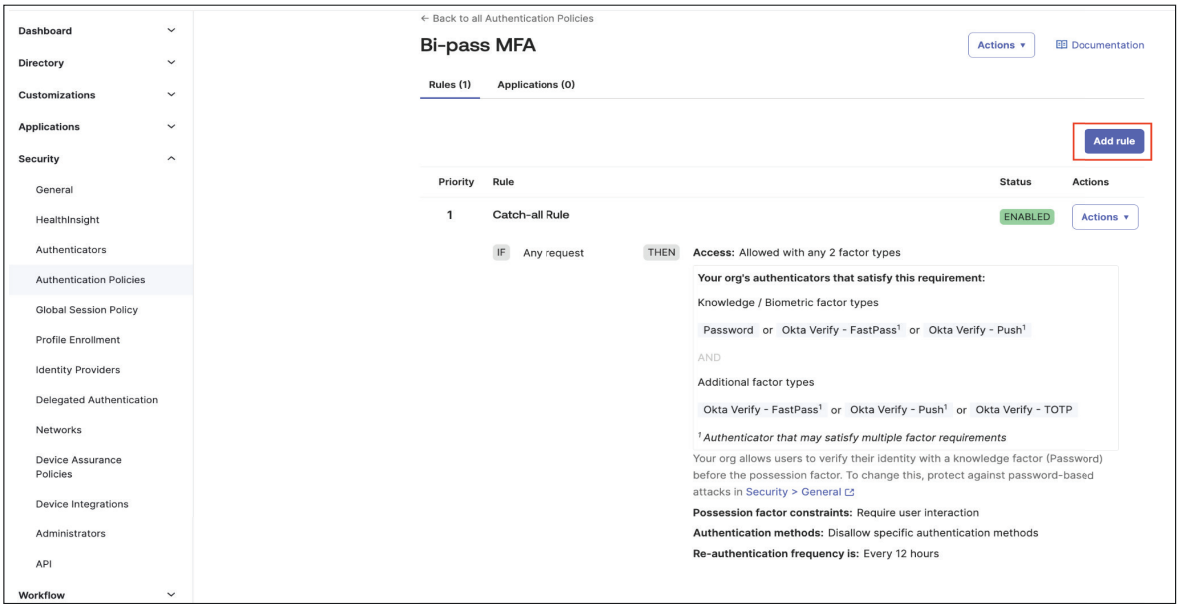

**Step 3b:** Select the user that was created in the previous steps as admin and assign read-only admin role and click on **“Save Changes”**.



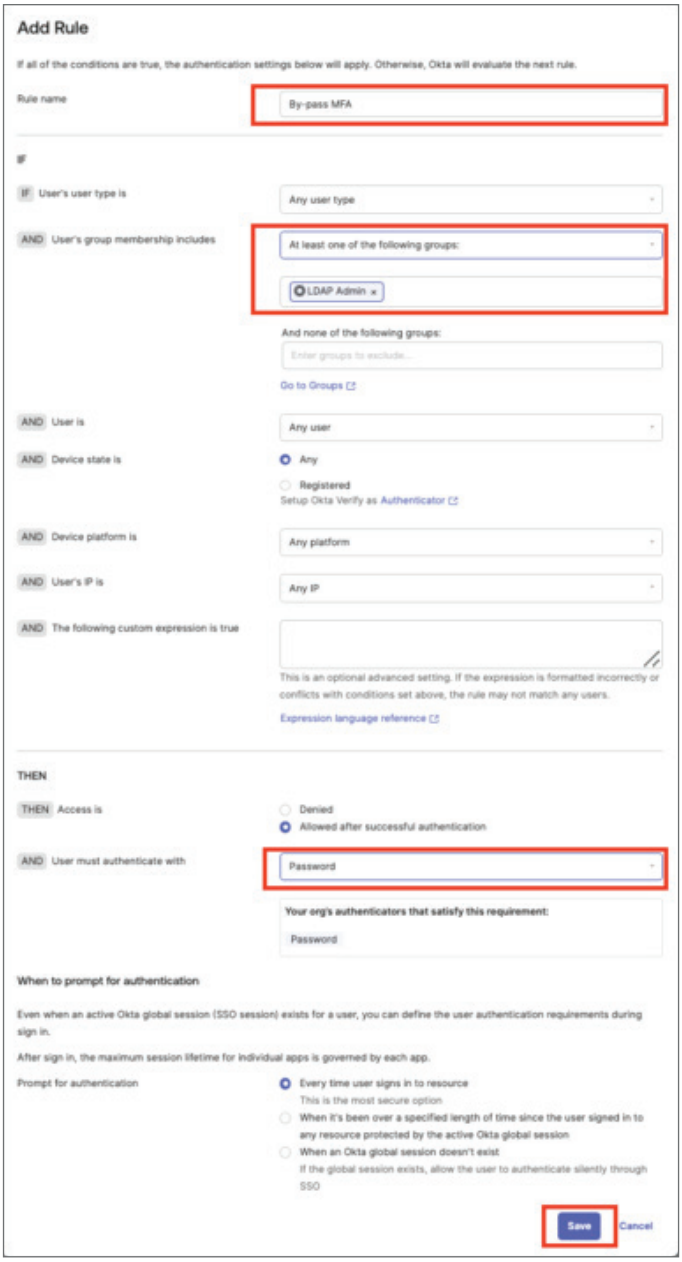
**Step 4:** Add the service admin account that was created in the previous steps to a specific group that will be used to set the policies to By-pass MFA and set authentication policies to authenticate using LDAP instead. This allows this special user to authenticate against the LDAP data. Once the group is created, it can be called anything memorable, the name below is LDAP Admin, it is time to add the user that was created in the above steps added to the just created group. Even though it says to Assign People to the group, in this case the “person” that will be assigned is the user that was created earlier. Choose the username you just created and add it to the group, then click on Assign people.



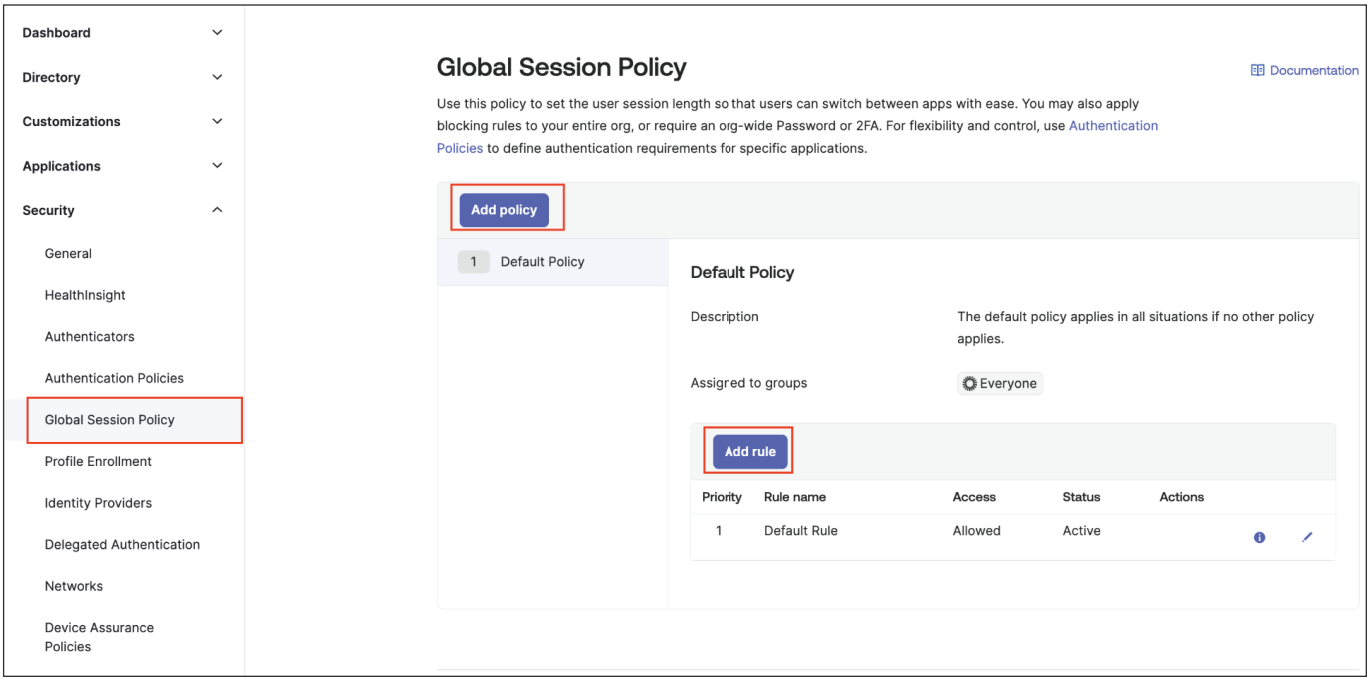

**Step 5:** Once the user has been assigned to the group, the next step is to create a rule in Authentication policies. Go to the Main Menu and choose **“Security”**, then **“Authentication Policies”**. Once in the Authentication Policies screen, click on **“Add rule”**.



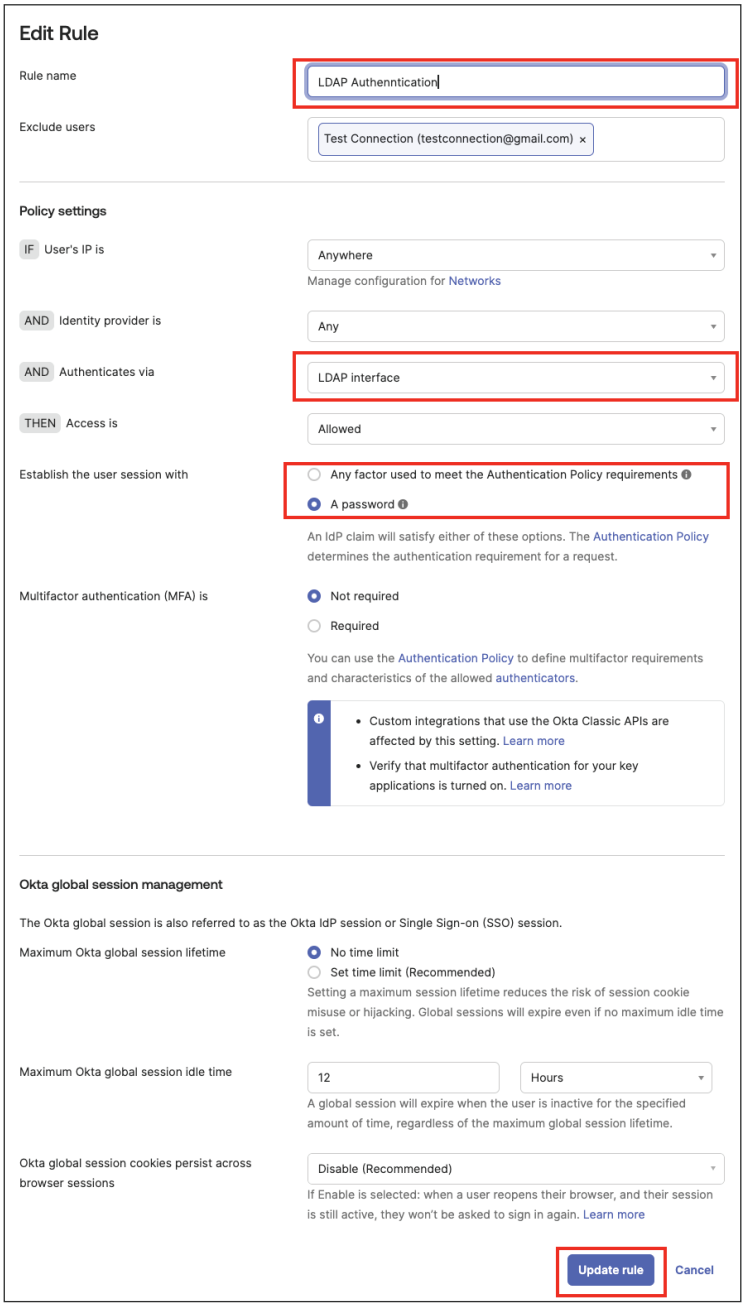
**Step 6:** In the Add rule screen, name the rule (suggestion: MFA By-Pass, but it can be anything that can help remember what it is for) then select and add the specific LDAP admin group created previously and select password so that the user must authenticate with a password and click on Save.



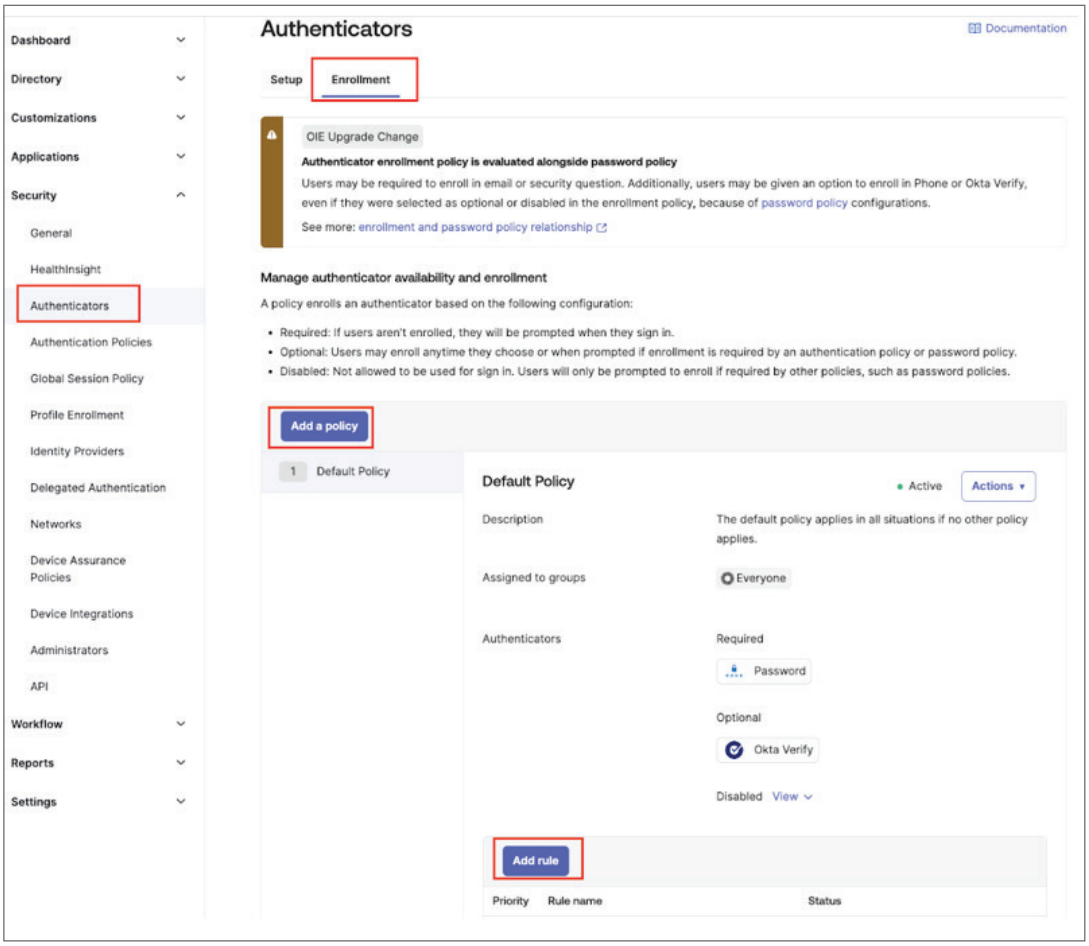
**Step 7:** Create a rule in Global Session Policy by choosing that dropdown in the Main Menu under Security. Once in that screen choose **“Add policy”**, then **“Add rule”**.



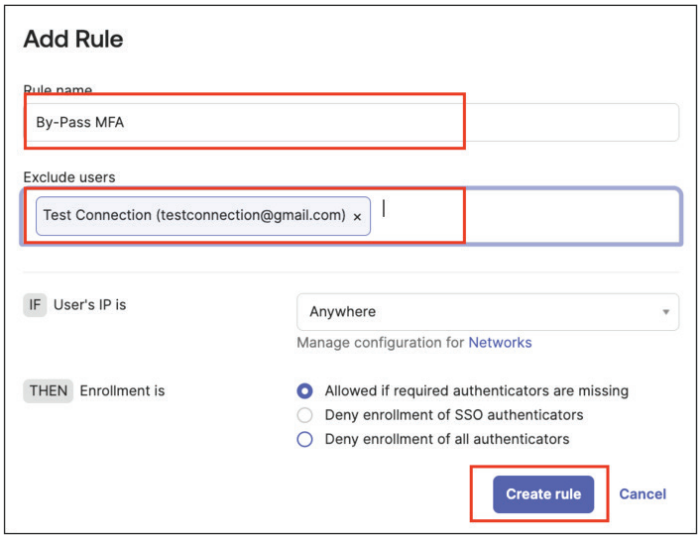
Follow the steps in the Edit Rule screen. Name the rule and add the admin service user to exclude users list and keep authenticate via LDAP interface and keep everything else as default. Once everything has been added as shown, click **“Update rule”**.



**Step 8:** Create a rule in Authenticators. Choose **“Authenticators”** under Security as shown. Under the Enrollment tab, choose **“Add a policy”**, then **“Add rule”**.




**Step 9:** Under Add a Rule, create a rule name (suggestion: MFA By-Pass, but it can be anything that can help remember what it is for) and exclude the users as shown. Follow what is shown in the screen shot, then click on **“Create rule”**.



**Step 10:** The final step is to test and verify the authentication for LDAP interface is working correctly by executing the following ldapsearch, which prompts for the user password of the service account and once authenticated will return the user and group details. More information on how to use the LDAP search function with OKTA can be found at Verify a Connection to the Okta LDAP Interface.

FQDN, Bind DN, Bind password, Base DN and Domain name are dependent on the LDAP tenant.

- Users in Okta instances must have a displayName attribute
- Username login attribute is set to email
- Allow up to 30 mins to sync

For more details and help with identifying the required attributes:

https://help.okta.com/en-us/content/topics/directory/ldap-interface-connection-settings.htm

Here is the general search command format for testing if the authentication rules work correctly:

ldapsearch -H ldaps://[subdomain].ldap.okta.com:636 -D “uid=[user@domain.com],ou=users,dc=[subdomain],dc=okta,dc=com” -W -b dc=[subdomain],dc=okta,dc=com

To test the function the command will need to replace the following variables with the real values.

uid=[user@domain.com] -- this would be the user id of the user that was created above in Step 3
dc=[subdomain] -- This would be the unique domain for the organization.

Below is an example of what the LDAP search command would look like for a UID of testconnection@gmail.com and a domain of trial-5115266.

ldapsearch -H ldaps://trial-5115266.ldap.okta.com:636 -D “uid=testconnection@gmail.com,ou=users,dc=trial-5115266,dc=okta,dc=com” -W -b dc=trial-5115266,dc=okta,dc=com

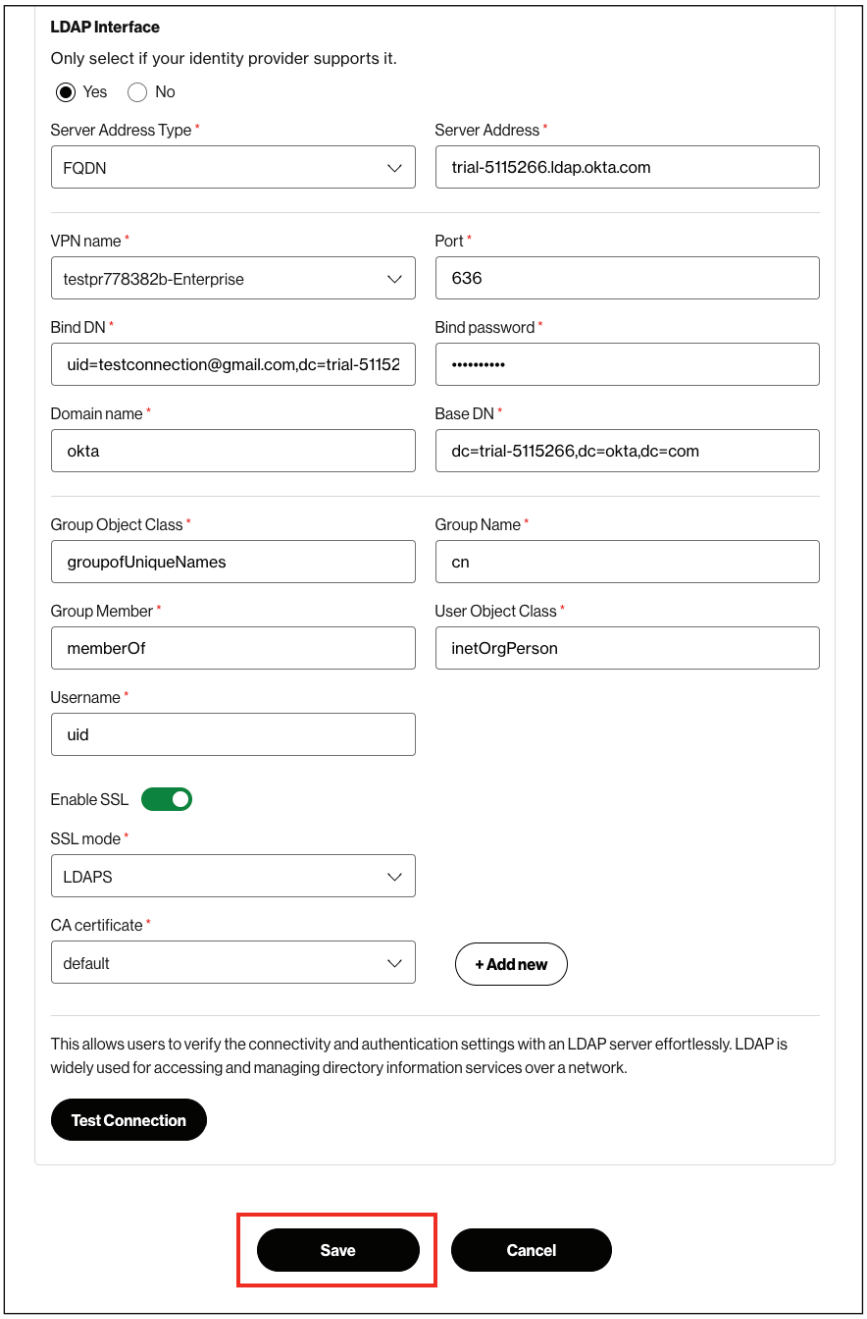
```
mohta3m@CQT9XWVVJW ~ % ldapsearch -H ldaps://trial-5115266.ldap.okta.com:636 -D "uid=testconnection@gmail.com,ou=users,dc=trial-5115266,dc=okta,dc=com" -W -b dc=trial-5115266,dc=okta,dc=com
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=trial-5115266,dc=okta,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# trial-5115266.okta.com
dn: dc=trial-5115266,dc=okta,dc=com
dc: trial-5115266
objectClass: top
objectClass: domain

# users, trial-5115266.okta.com
dn: ou=users,dc=trial-5115266,dc=okta,dc=com
ou: users
objectClass: top
objectClass: organizationalUnit

# groups, trial-5115266.okta.com
dn: ou=groups,dc=trial-5115266,dc=okta,dc=com
ou: groups
objectClass: top
objectClass: organizationalUnit
```

Once the LDAP interface has been verified with ldapsearch for Okta, the integration with Trusted Connection will work correctly. Group and user attributes are the same for any Okta LDAP interface shown below:

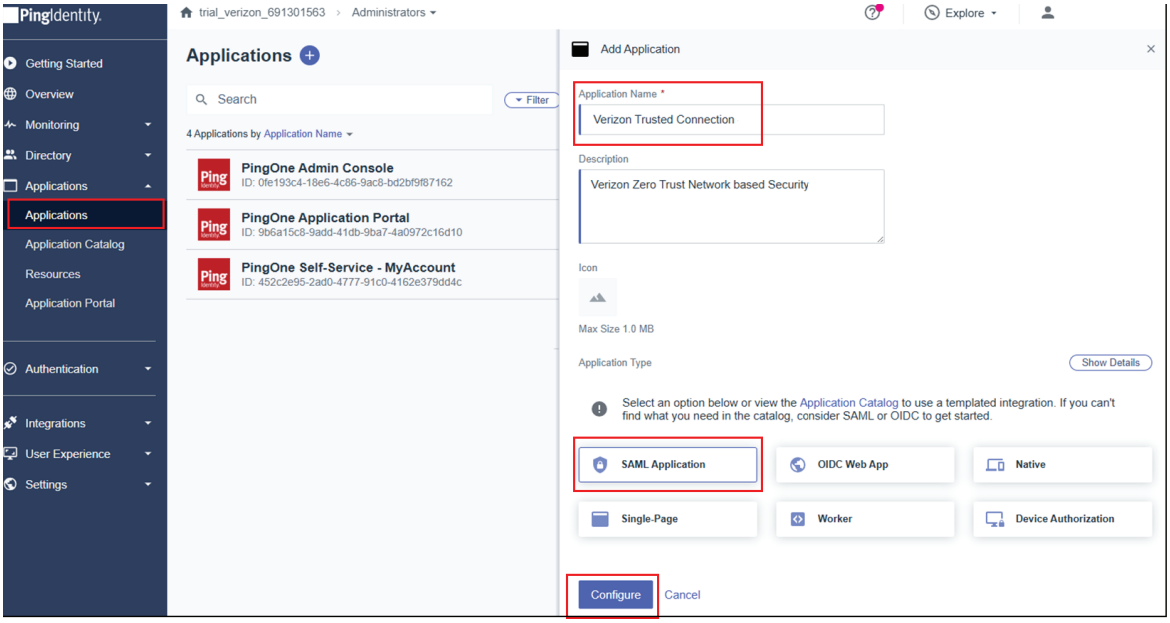


## Ping Identity Integration for SAML Authentication

The following steps demonstrate how to integrate Trusted Connection with the Ping Identity, for SAML Authentication.

You will need to set up two browser windows. One into your Ping Identity portal and the second into the Verizon Trusted Connection portal. Perform the following steps from within the Ping Identity potral.

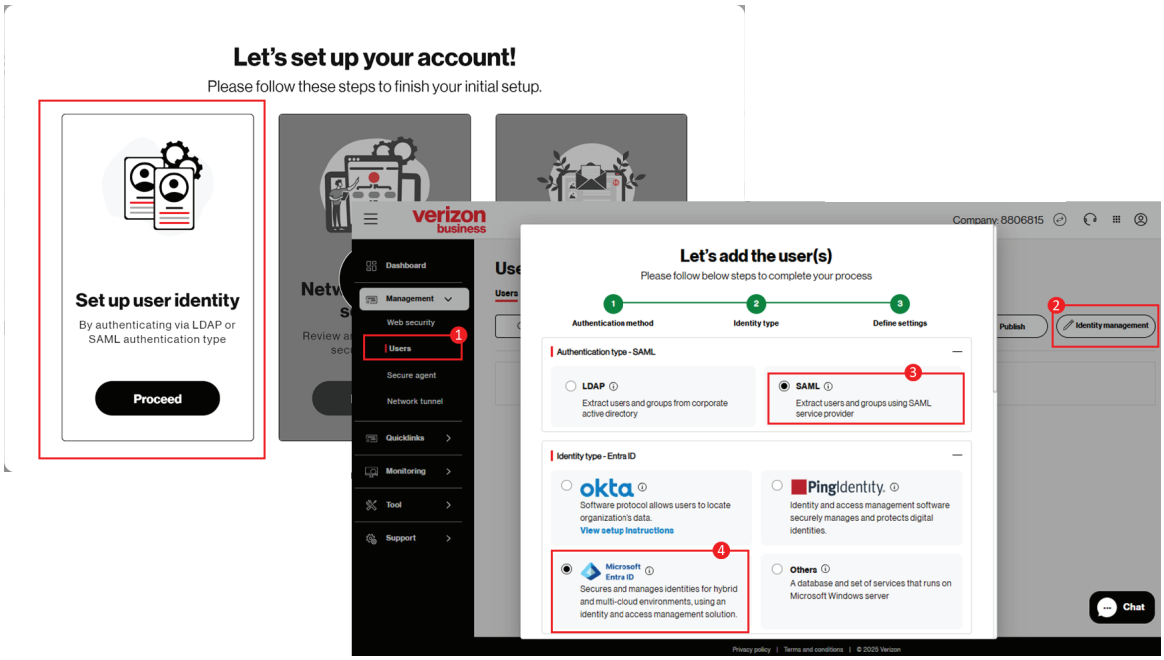
**Step 1:** After logging into the Ping Portal, create an application in Ping by selecting Applications, enter Application Name (as Verizon Trusted Connection), select SAML and click on **"Configure".**



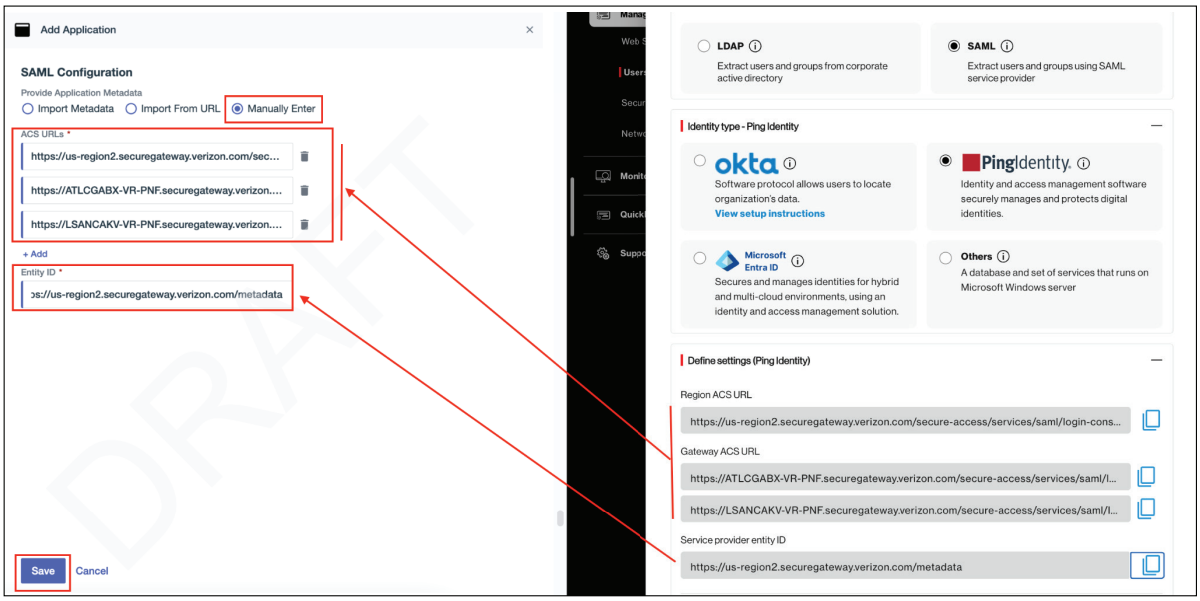
For the next step, you will need to open a browser for Trusted Connection at trustedconnection.verizon.com.

**Step 2:** Navigated to Set up user identity from the setup wizard or the Trusted Connection menu system as shown below:

Accessing user identity via the set up wizard




**Step 3:** Enter the **ACS url, Gateway urls, Entity ID from Trusted Connection** and click on **"Save"**. These values will be found in the Trusted Connection Portal as shown below.

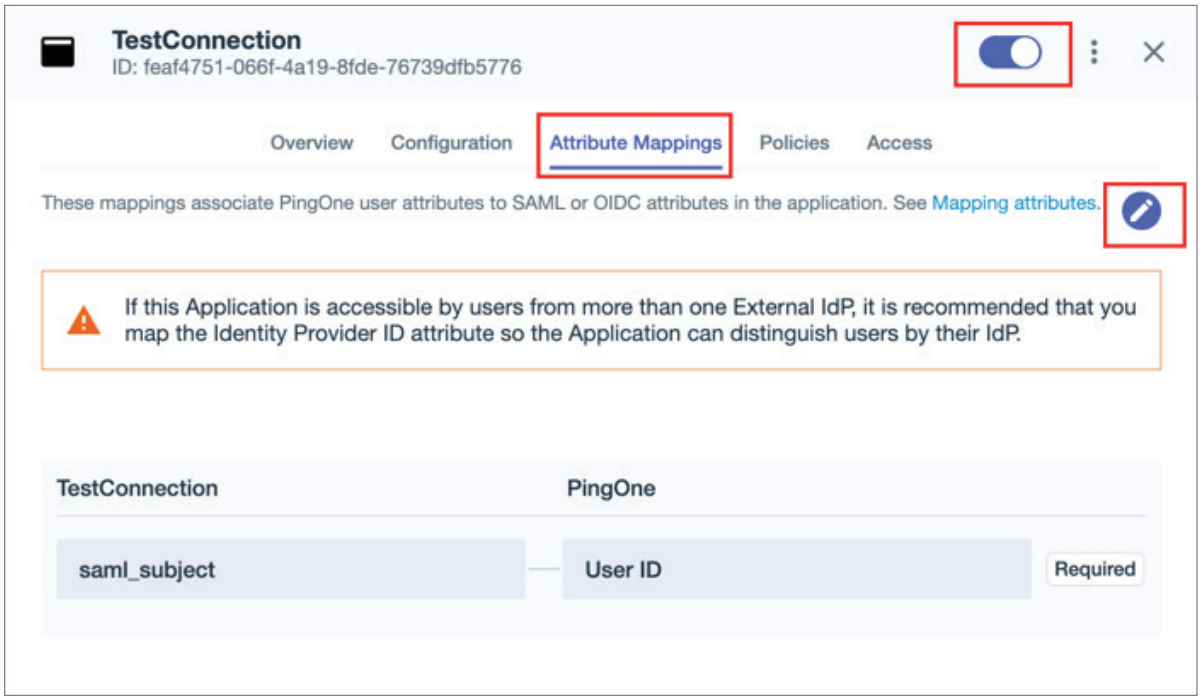



Copy and paste the values into the Ping screen, then click **"Save"**.

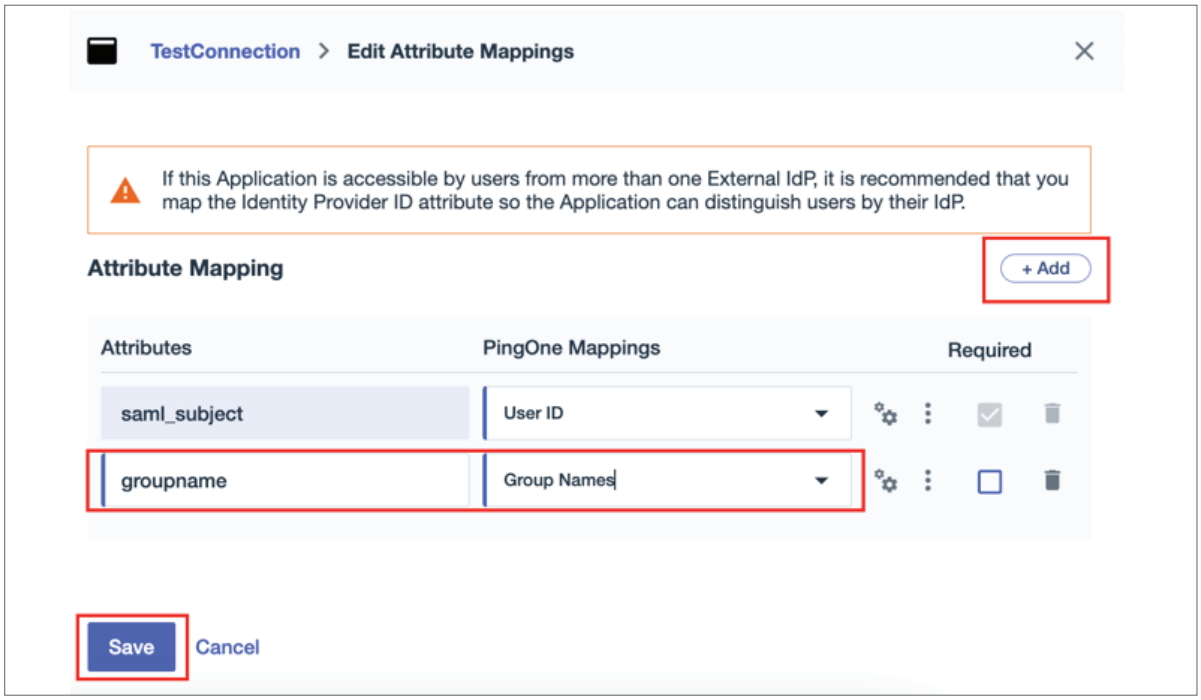
**Step 4:** Once the new SAML application is created and configured,

**a)** Activate the new application by moving the slider to the right on top as shown below.

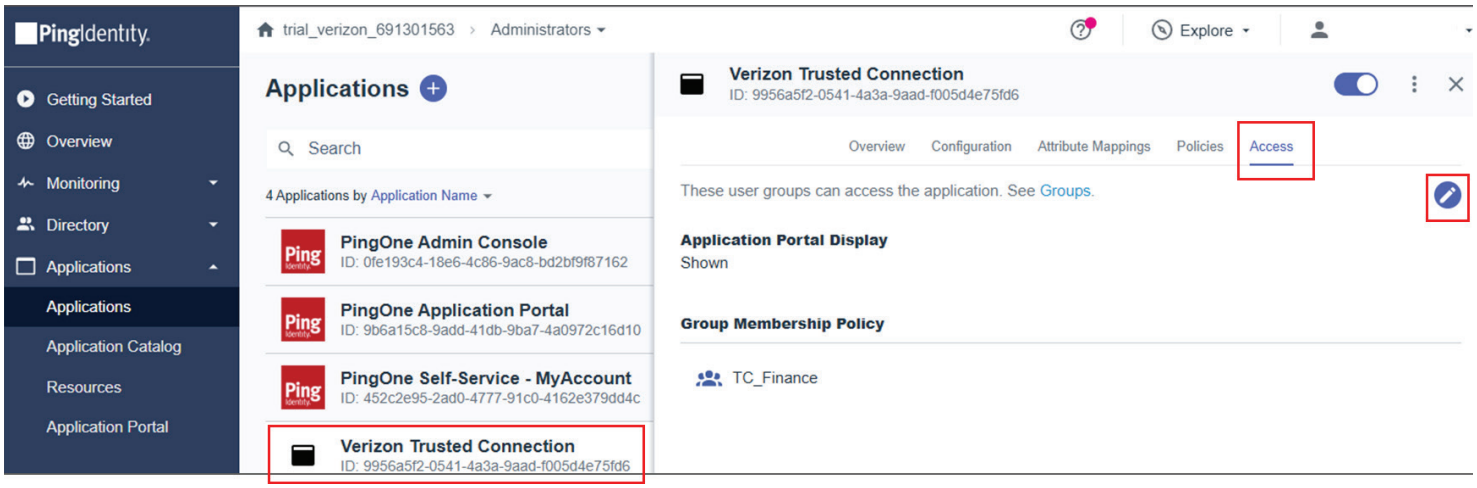
**b)** Go to attribute Mappings and click on the pencil



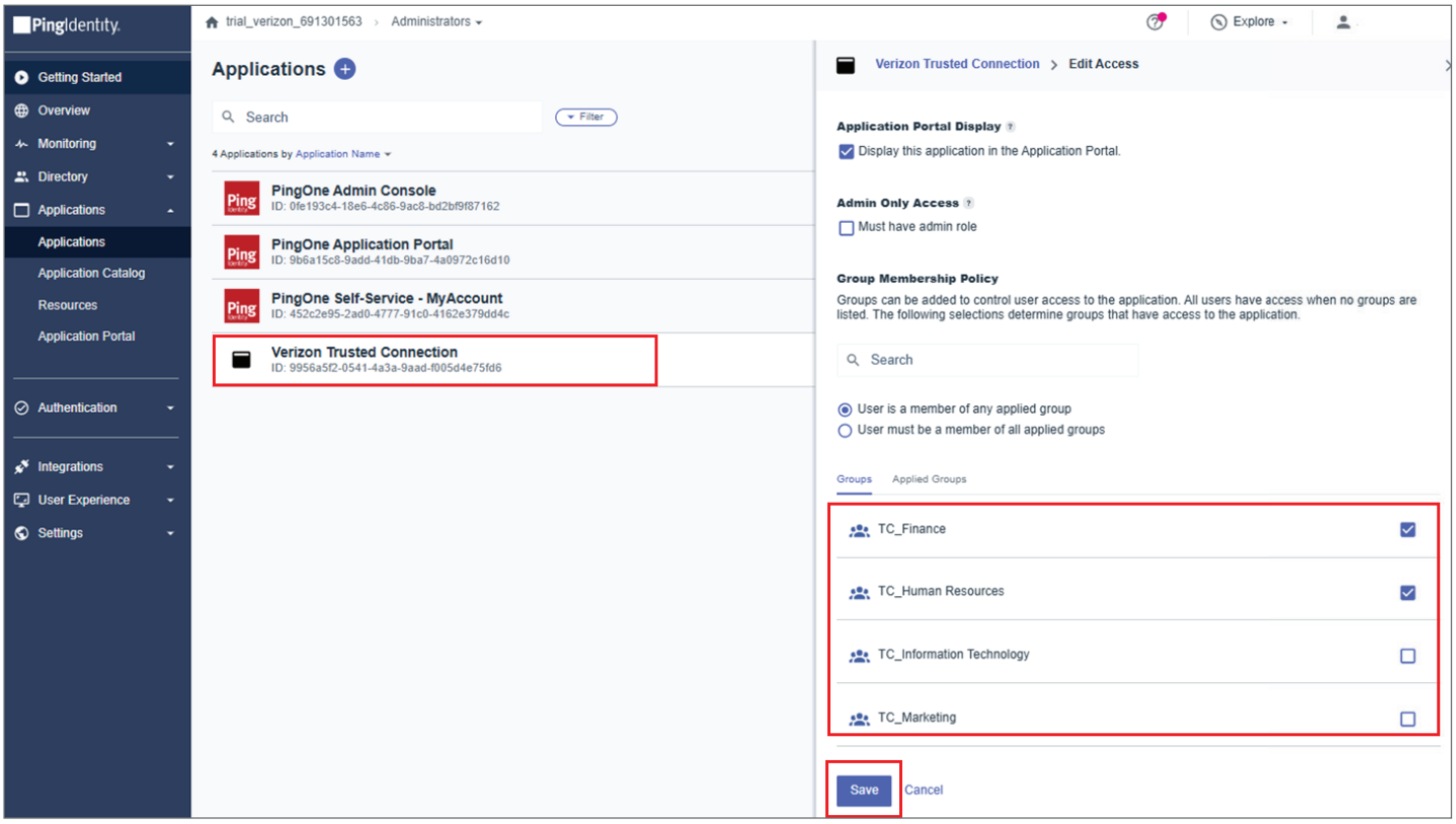

**Step 5:** Click on **"+Add"** as shown below and enter Attribute name as **groupname** and select **"Group Names"** from PingOne Mappings drop down. Click **"Save"**.



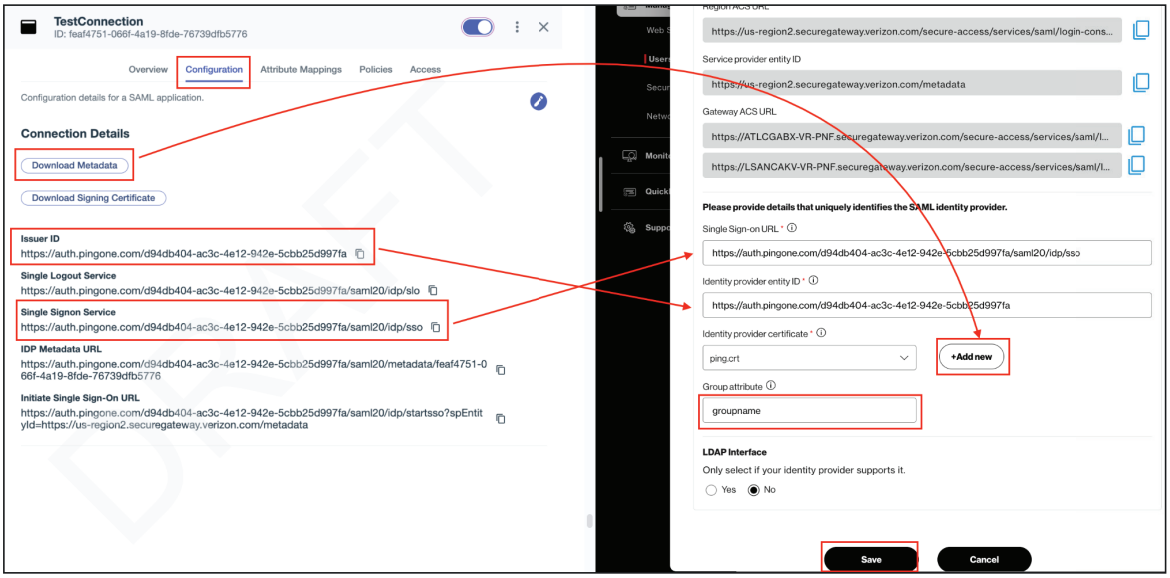
**Step 6:** Click on **Access** in the application and then click on the **pencil icon** to add groups to the application.




**Step 7:** Select the groups to be assigned to Trusted Connection and click **“Save”**.

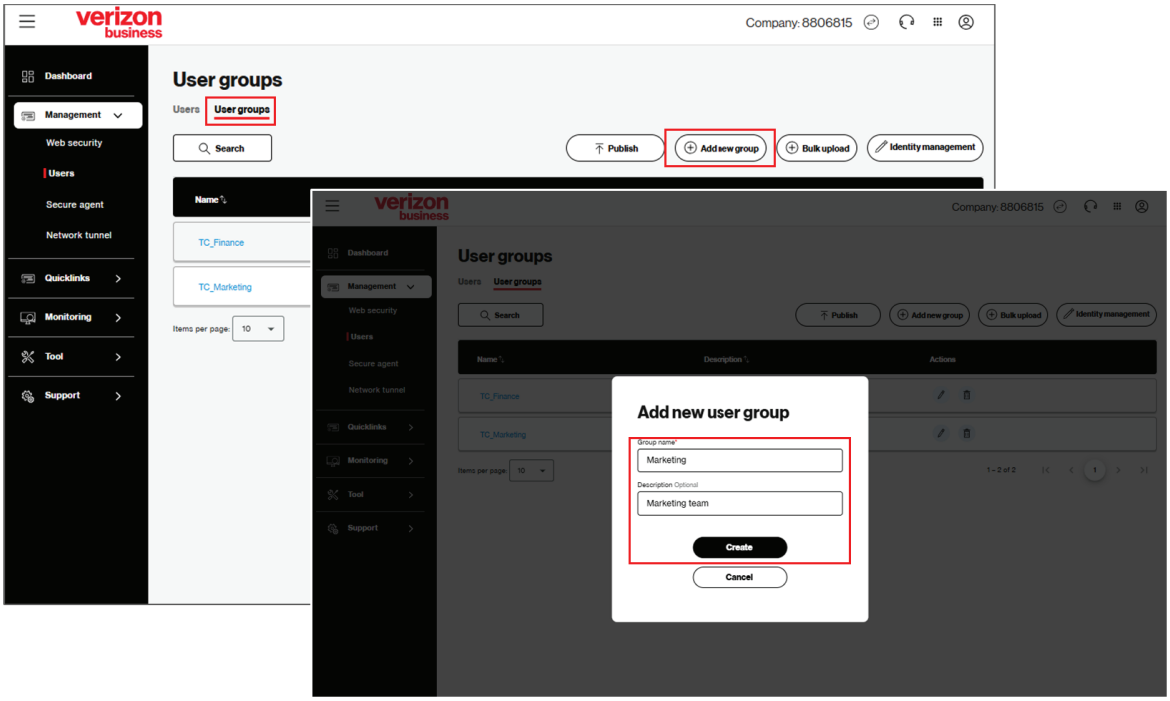


**Step 8:** Copy the Ping Single Signon Service URL and Issuer ID URLs into the Trusted Connection Single Sign-on URL and Identity provider entity ID, respectively, download the Ping Signon certificate and upload into TrustedConnection using the **“+Add new”** button. Specify the Group attribute as **“groupname”**. Press the **“Save”** button.




**Step 9:** Once all the above steps have been completed, go back to the Trusted Connection Setup Wizard to complete the onboarding process.

Finally, you must create User Groups in Trusted Connection that match the identical User Groups in Entra ID. Navigate the **Management** > **Users** on the left side of the screen. Select **“User Groups”** and press the **“(+) Add new group”** button to add your groups, one at a time.



## Windows AD/OpenLDAP integration for LDAP authentication

The OpenLDAP Software suite includes:

- lloadd - stand-alone LDAP Load Balancer Daemon (server or slapd module)
- slapd - stand-alone LDAP daemon (server)
- libraries implementing the LDAP protocol, and utilities, tools, and sample clients.

These directions can be used with Trusted Connection for integrating with any LDAP based IDM service. For organizations using Windows Active Directory (for Microsoft EntraID see the directions above) or other LDAP based system, these directions will point in the right direction.

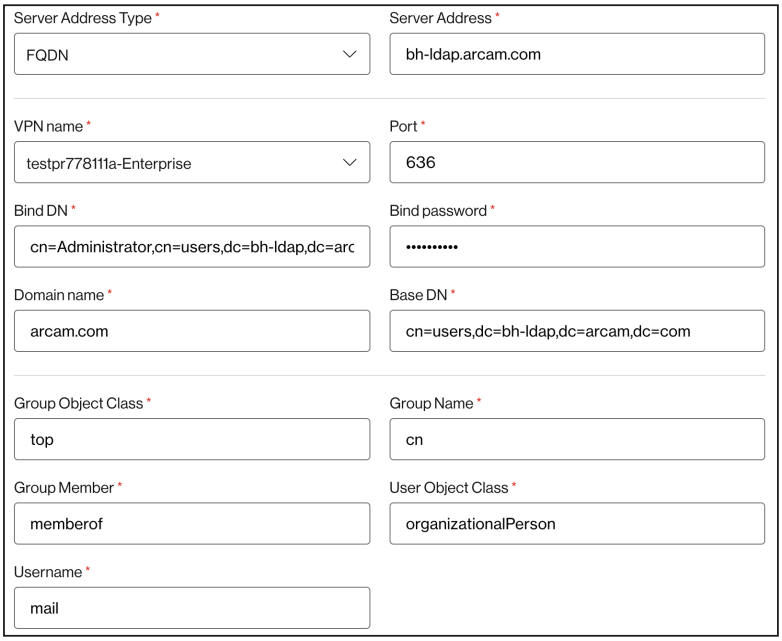
**Step 1:** Make sure the LDAP is open on port 636.

**Step 2:** The following User attributes in LDAP are mandatory - **mail, displayName, firstName, LastName, username**.

To configure LDAP authentication in Trusted connection, use the attributes listed below. Note that the actual values will vary depending on the LDAP server.

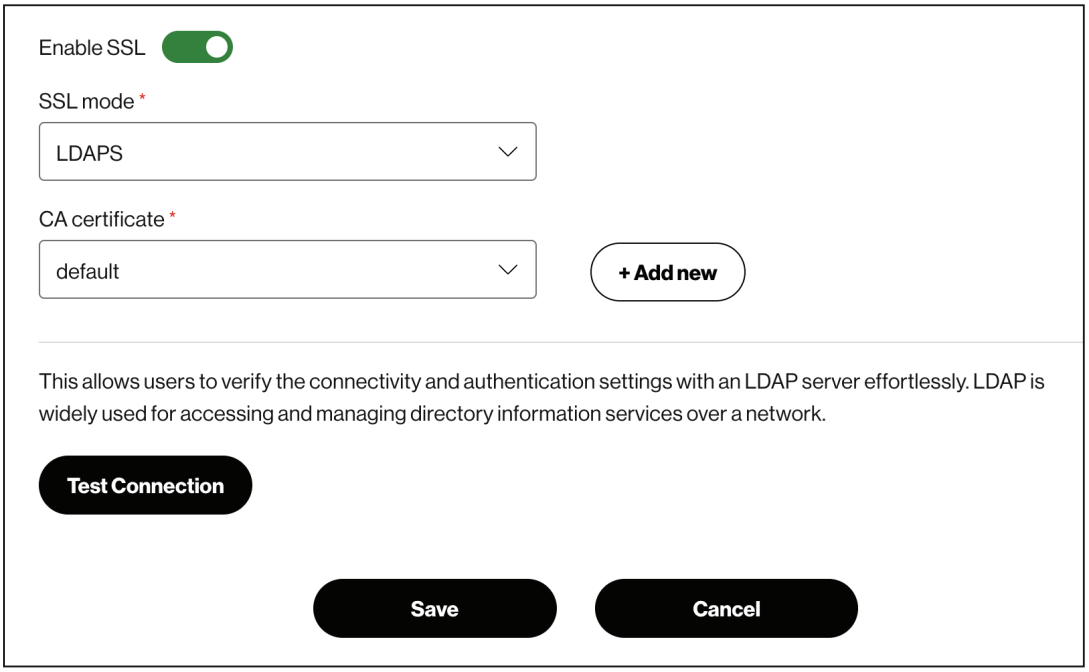
As an example, if the ldap service has the following **FQDN: ldapsecure.example.com** then the attributes would be as follows:

- Bind DN: **cn=Admin,cn=user,dc=ldapsecure,dc=example,dc=com** admin password should match the same in LDAP.
- Domain name: example.com
- Base DN:dc=example,dc=com
- Group Object Class: top
- Group Name: cn
- Group Member: memberOf
- User Object Class: organizationalPerson
- Username: mail/uid (similar to the value in LDAP)



Group attributes should be the default values in most of the case, except if the LDAP administrator wants to make changes to any other specific variable. Once the values have been entered into the Trusted Connection portal, save the configuration. It will take up to 30 mins for the sync with the Trusted Connection gateways to complete.

Enable SSL with LDAPS and select certificate as default from dropdown for encrypted connection.



# Appendix

## LDAP and SAML explained

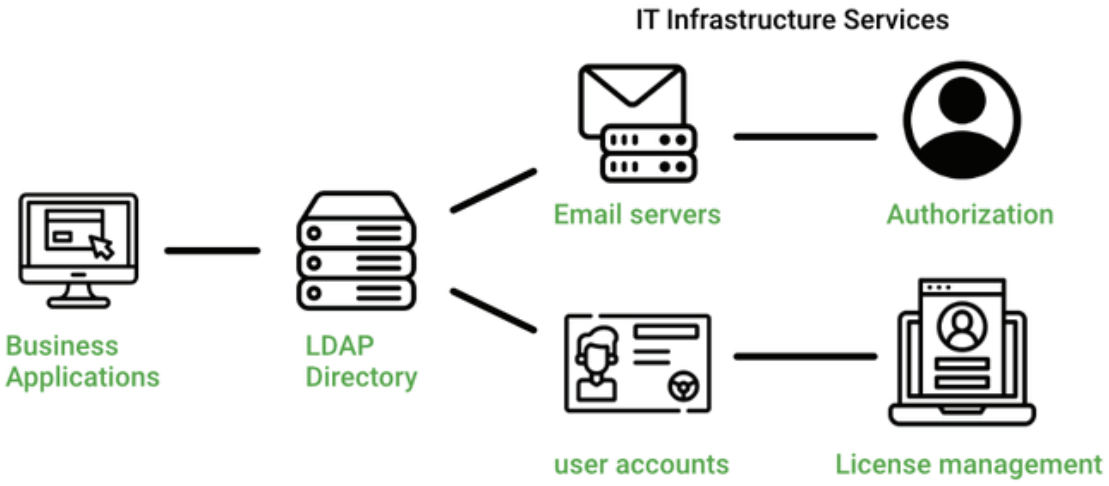
Trusted Connection leverages an organization's own Identity Management Platform (IDM). These systems typically use SAML and LDAP for their authentication protocols, as they are commonly used protocols for the access control and management of large groups of users. Each of these protocols serve somewhat different purposes, so it is helpful to understand how they work and the differences between them.

### Lightweight Directory Access Protocol (LDAP)*

Lightweight directory access protocol (LDAP) is a highly flexible, configurable, open-standard, vendor-agnostic distributed database protocol that can be used for a variety of applications that require keeping track of a large group of objects or users across a WAN network. LDAP has been around as a standard since 2003. It is commonly used for centralizing the management and control of users by verifying users' identities and then giving appropriate access to servers, applications, and even devices. This access control is often referred to as Role Based Access Control (RBAC).

After installing an LDAP client on a user device, it uses the transmission control protocol/internet protocol (TCP/IP) to communicate with a set of distributed directories on the network to access a resource such as an email server, printer, application, data set, or pretty much anything else that a user wants to connect to. Since LDAP also can be used as a secure authenticator, the protocol is often used to verify credentials stored in a dictionary service, such as Active Directory. When an access request is initiated by a user to an LDAP server, the protocol evaluates whether the credential data matches information stored in the directory and if that user is authorized to access that particular resource. LDAP is used by many IDM services, such as EntraID, Okta, and many others.

**How LDAP works**

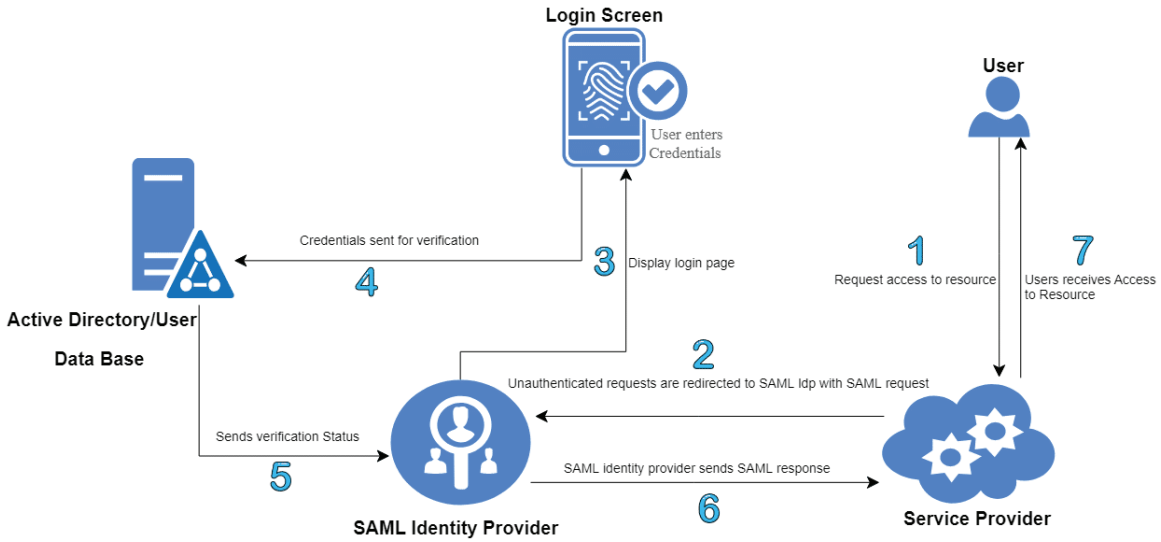


## Security Assertion Markup Language (SAML)*

Security assertion markup language (SAML) is an open-source protocol used to facilitate communication between a user, identity provider, and application. SAML can support virtual private network (VPN), Wi-Fi, and web application services to establish a secure connection, making it useful for cloud-based servers and applications, by allowing users to quickly set up secure connections to their applications over an insecure network.

Developed as an Open Source project launched in November 2002, SAML simplifies the authentication process by exchanging information between an identity provider and a service provider (SP). To do this, a user requests to connect to a service from a service provider or application, which must then request authentication from the identity provider: SAML can be used to streamline this communication by only requiring users to log in once with a single set of credentials, which can make it easier and simpler for end users, who no longer have to reauthenticate every time they connect to the application. When the same credentials and authentication is applied to access multiple services with just one login, SAML can be used to enable single sign-on (SSO) verification.

### Security Assertion Markup Language (SAML) Authentication Process




## SAML versus LDAP

Both SAML and LDAP are similar in their purposes, which is to give users access to organizational resources through secure authentication. They each do this by establishing communication between an IDM that manages and stores the user information and a device, server, or SP (to perform a function). Uniquely, LDAP has the ability to also serve as the repository for the user records.

Another similarity is that both protocols can facilitate SSO verification depending on the configuration of the directory service. However, while both have the capability to authorize and manage access and authenticate the users are the correct entities and are used for authentication and authorization, neither of these services are used for operational accounting. In other words, the protocols will help verify, add, or reject users but not actually track their activities once the connection to the applications has been established.

© 2025 Verizon. VZGD5000625