Guidelines

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.

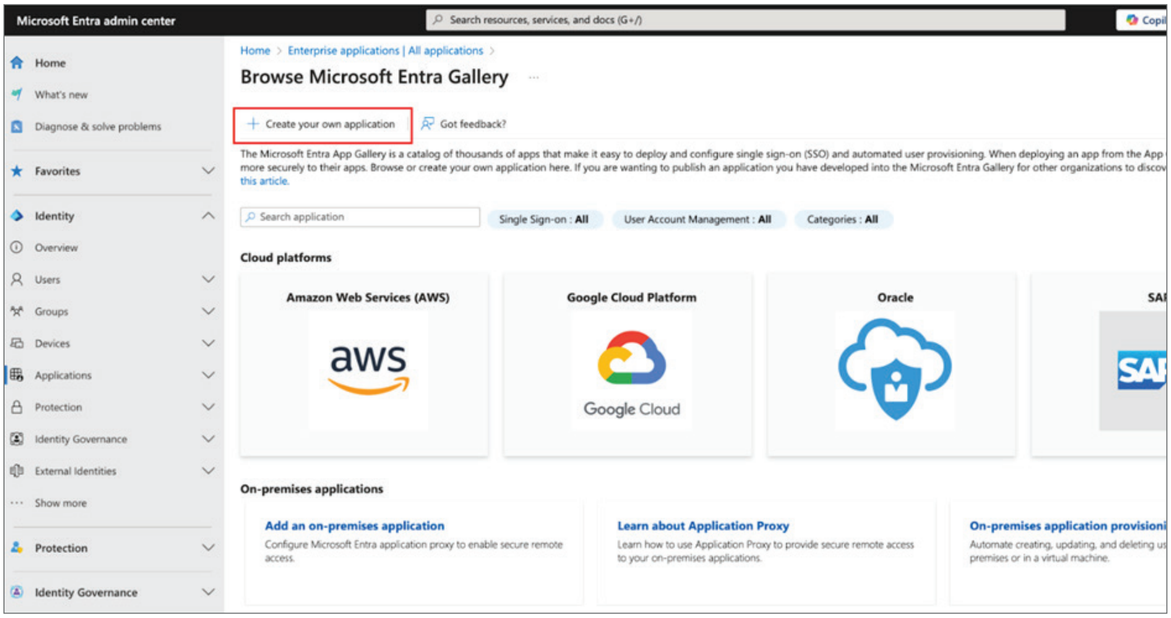
- **Trusted Connection with SAML-only:** Allows creation of Trusted Connection policies that apply to the organization as a whole and policies that target specific User Groups that have been assigned to Trusted Connection in your IDM. User Groups must be manually created within Trusted Connection to 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**".



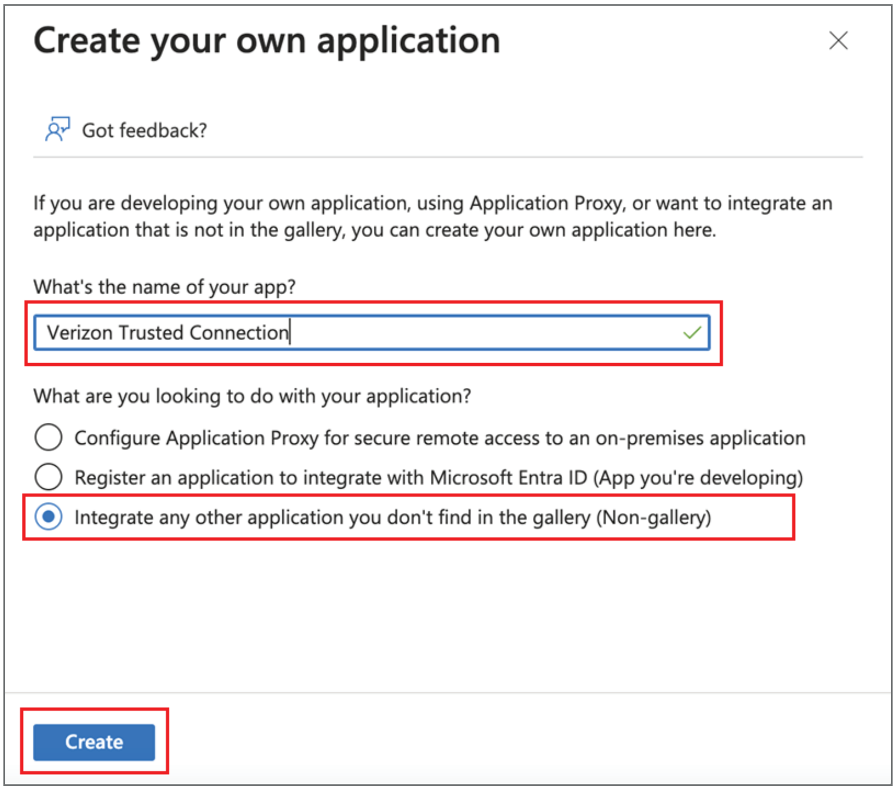
The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App
more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discov
this article.

Add an on-premises application
Configure Microsoft Entra application proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

On-premises application provisioni
Automate creating, updating, and deleting us
premises or in a virtual machine.

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"**.



Create your own application

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Verizon Trusted Connection

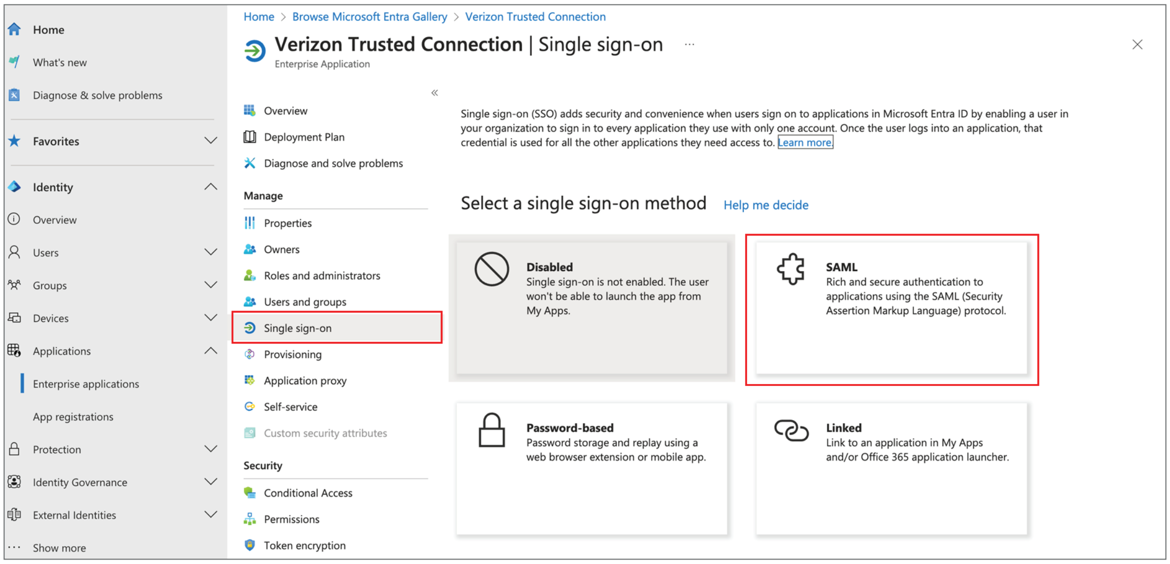
What are you looking to do with your application?

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

○ Register an application to integrate with Microsoft Entra ID (App you're developing)

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

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



Verizon Trusted Connection | Single sign-on

Enterprise Application

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more

Select a single sign-on method Help me decide

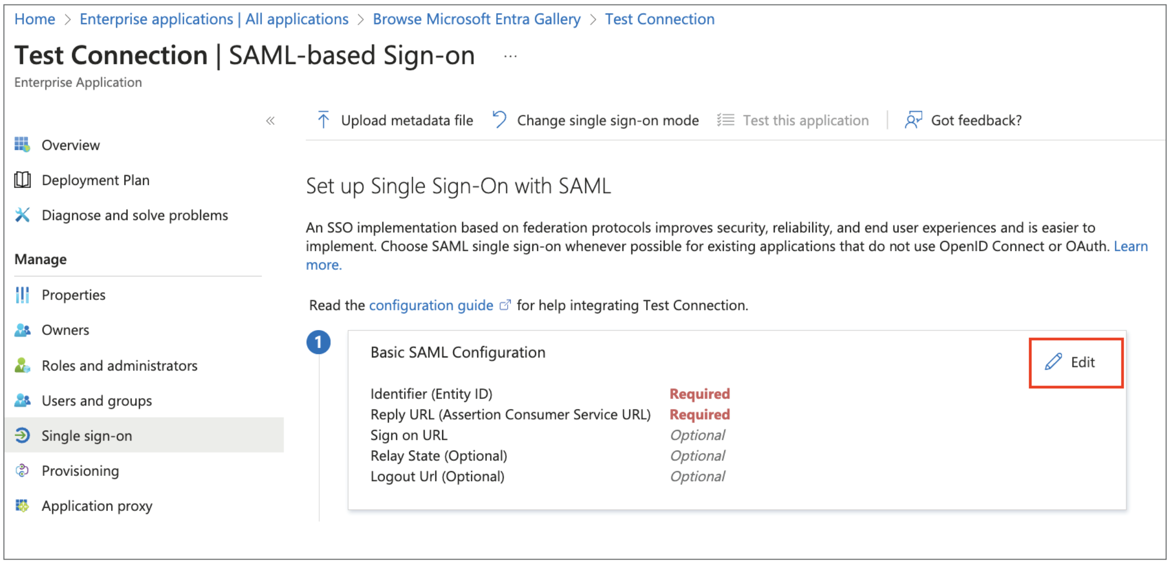
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

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



Test Connection | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating Test Connection.

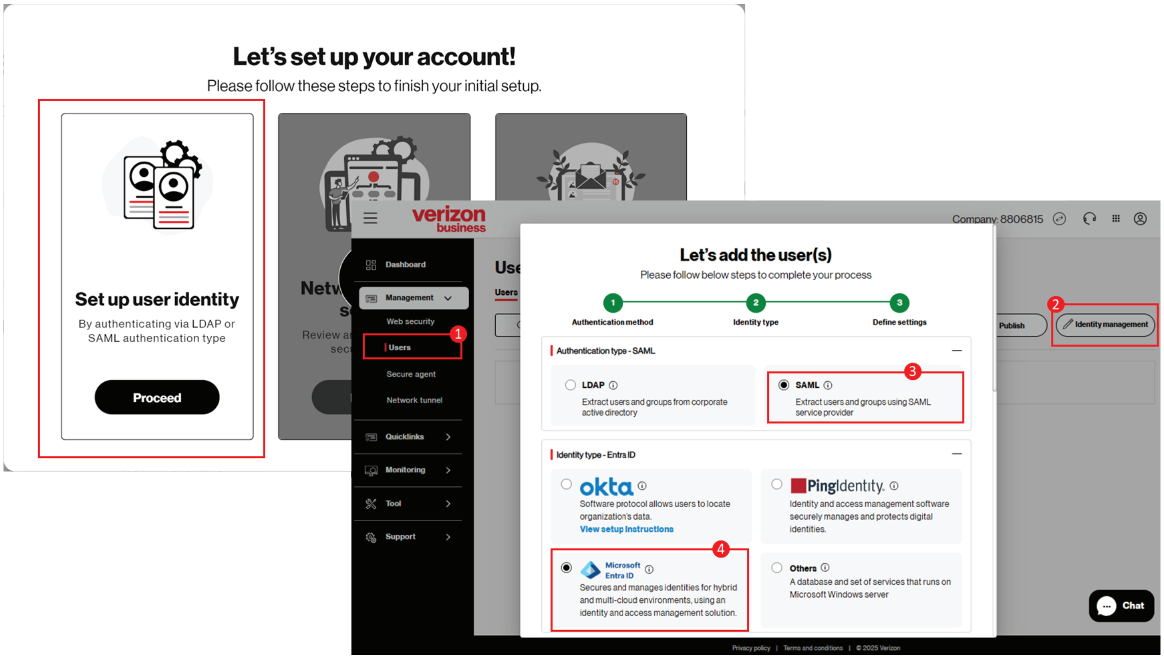
Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	*Optional*
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

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



Let’s set up your account!

Please follow these steps to finish your initial setup.

Set up user identity

By authenticating via LDAP or SAML authentication type

Let’s add the user(s)

Please follow below steps to complete your process

1 Authentication method — 2 Identity type — 3 Define settings

Authentication type - SAML

○ LDAP — Extract users and groups from corporate active directory

● SAML — Extract users and groups using SAML service provider

Identity type - Entra ID

○ okta — Software protocol allows users to locate organization’s data. View setup Instructions

○ PingIdentity. — Identity and access management software securely manages and protects digital identities.

● Microsoft Entra ID — Secures and manages identities for hybrid and multi-cloud environments, using an identity and access management solution.

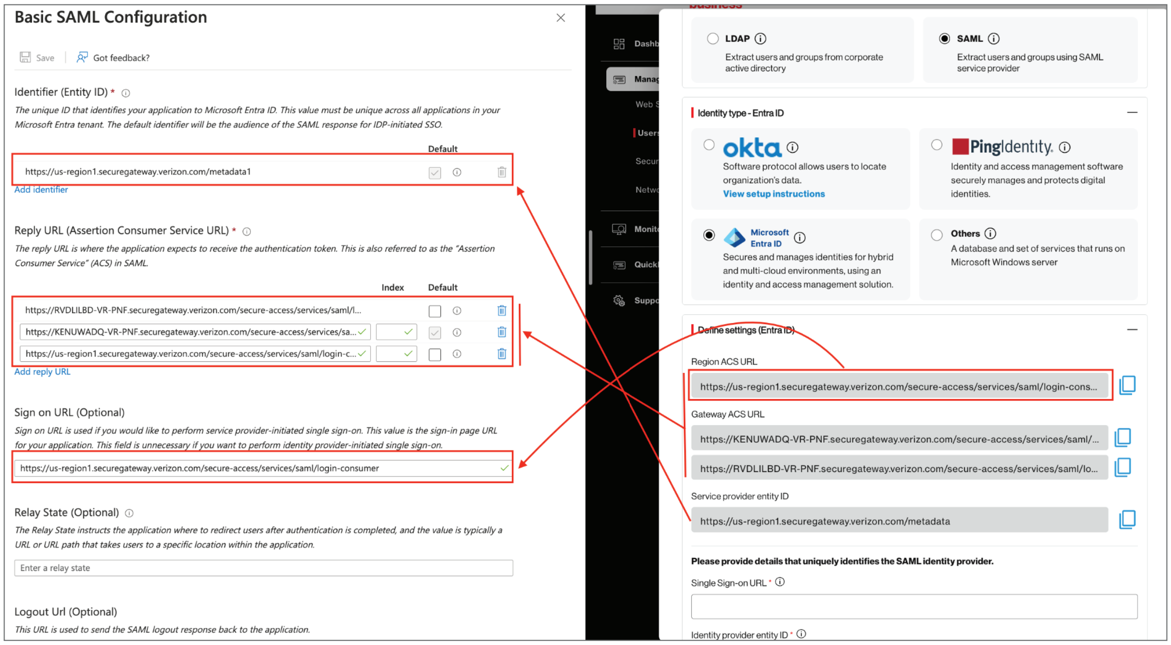
○ Others — A database and set of services that runs on Microsoft Windows server

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.



Basic SAML Configuration

Identifier (Entity ID) *

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

	Default
https://us-region1.securegateway.verizon.com/metadata1	☑

Reply URL (Assertion Consumer Service URL) *

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

	Index	Default
https://RVDLILBD-VR-PNF.securegateway.verizon.com/secure-access/services/saml/l...		□
https://KENUWADQ-VR-PNF.securegateway.verizon.com/secure-access/services/sa...		☑
https://us-region1.securegateway.verizon.com/secure-access/services/saml/login-c...		□

Sign on URL (Optional)

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

https://us-region1.securegateway.verizon.com/secure-access/services/saml/login-consumer

Relay State (Optional)

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

Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

○ LDAP
Extract users and groups from corporate active directory

● SAML
Extract users and groups using SAML service provider

Identity type - Entra ID

○ okta
Software protocol allows users to locate organization's data.
View setup instructions

○ PingIdentity.
Identity and access management software securely manages and protects digital identities.

● Microsoft Entra ID
Secures and manages identities for hybrid and multi-cloud environments, using an identity and access management solution.

○ Others
A database and set of services that runs on Microsoft Windows server

Define settings (Entra ID)

Region ACS URL
https://us-region1.securegateway.verizon.com/secure-access/services/saml/login-cons...

Gateway ACS URL
https://KENUWADQ-VR-PNF.securegateway.verizon.com/secure-access/services/saml/...
https://RVDLILBD-VR-PNF.securegateway.verizon.com/secure-access/services/saml/lo...

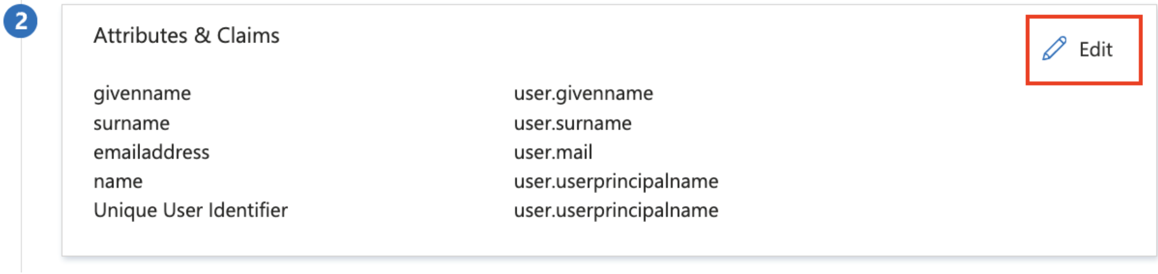
Service provider entity ID
https://us-region1.securegateway.verizon.com/metadata

Please provide details that uniquely identifies the SAML identity provider.

Single Sign-on URL *

Identity provider entity ID *

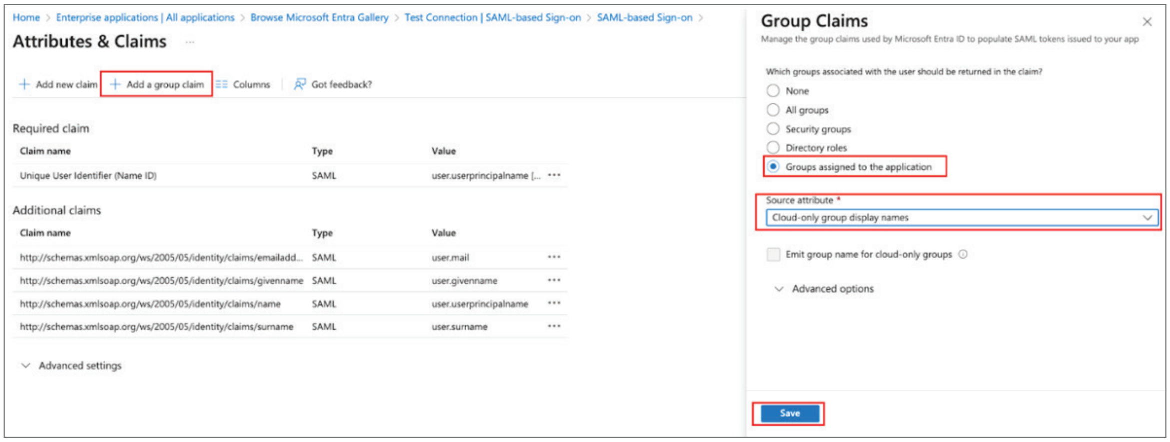
Step 7: Once the previous step is saved, you'll be back to the Set-up Single sign-on with SAML screen in the Entra portal. Click "**Edit"** on **Attributes & Claims** to add group claim.



Attributes & Claims

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

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



Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Test Connection | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

Required claim

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

Additional claims

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

Advanced settings

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
○ All groups
○ Security groups
○ Directory roles
● Groups assigned to the application

Source attribute *: Cloud-only group display names

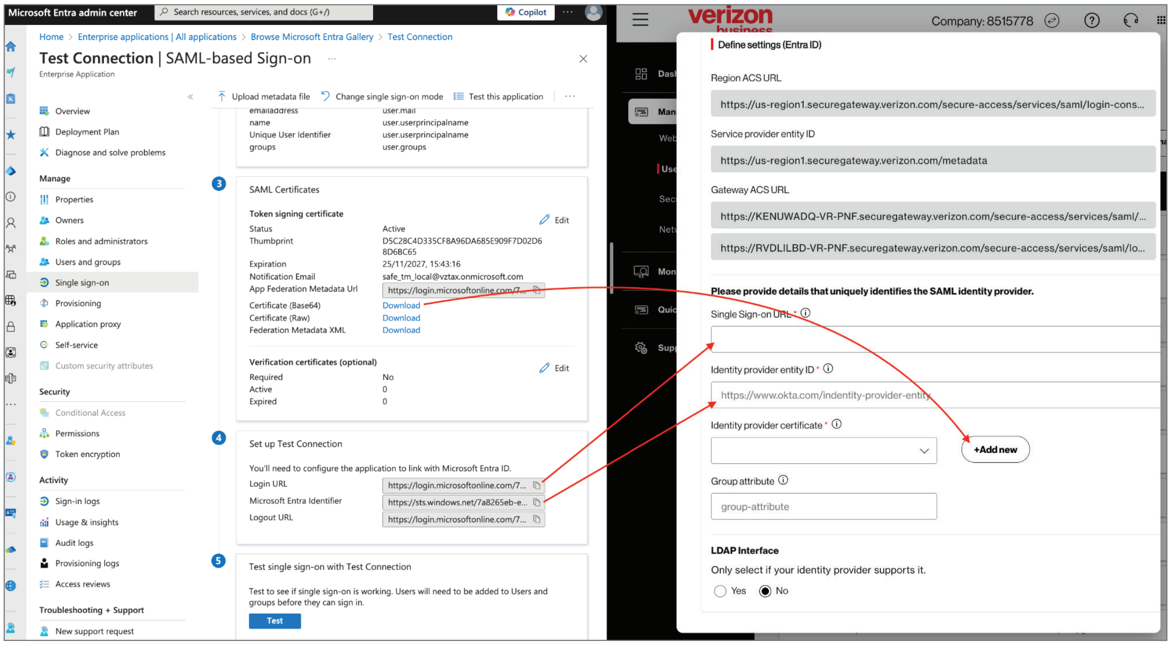
□ Emit group name for cloud-only groups

Advanced options

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.



Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Test Connection

Test Connection | SAML-based Sign-on

Enterprise Application

emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
groups	user.groups

3 SAML Certificates

Token signing certificate

Status	Active
Thumbprint	D5C28C4D335CF8A96DA685E909F7D02D6 8D6BC65
Expiration	25/11/2027, 15:43:16
Notification Email	safe_tm_local@vztax.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/7...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

4 Set up Test Connection

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

Login URL	https://login.microsoftonline.com/7...
Microsoft Entra Identifier	https://sts.windows.net/7a8265eb-e...
Logout URL	https://login.microsoftonline.com/7...

5 Test single sign-on with Test Connection

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

Define settings (Entra ID)

Region ACS URL: https://us-region1.securegateway.verizon.com/secure-access/services/saml/login-cons...

Service provider entity ID: https://us-region1.securegateway.verizon.com/metadata

Gateway ACS URL:
https://KENUWADQ-VR-PNF.securegateway.verizon.com/secure-access/services/saml/...
https://RVDLILBD-VR-PNF.securegateway.verizon.com/secure-access/services/saml/lo...

Please provide details that uniquely identifies the SAML identity provider.

Single Sign-on URL *

Identity provider entity ID *: https://www.okta.com/indentity-provider-entity

Identity provider certificate *

Group attribute: group-attribute

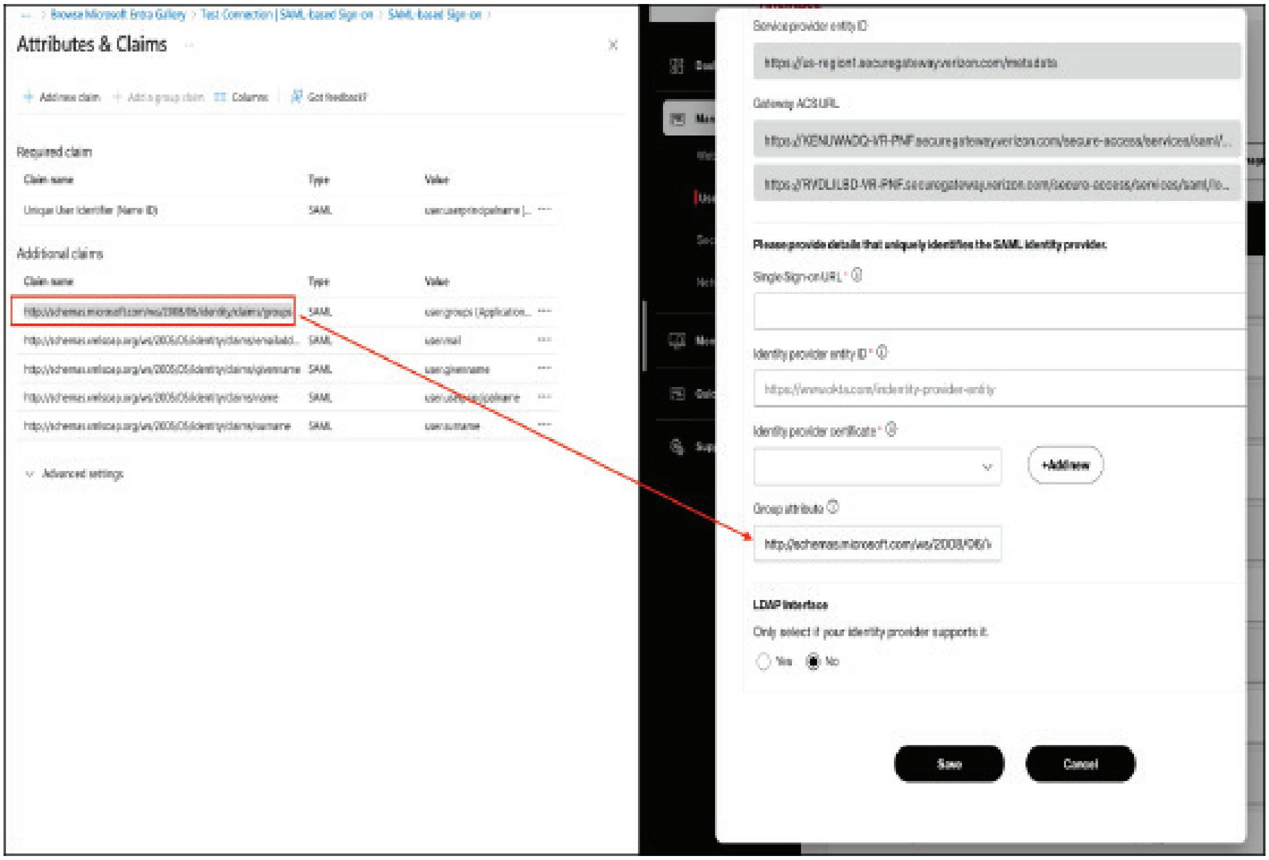
LDAP Interface

Only select if your identity provider supports it.

○ Yes ● No

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.



Browse Microsoft Entra Gallery > Test Connection | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

+ Add new claim
+ Add a group claim
Columns
Got feedback?

Required claim

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

Additional claims

Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [Application...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Service provider entity ID: https://us-region1.securegateway.verizon.com/metadata

Gateway ACS URL:
https://KENUWADQ-VR-PNF.securegateway.verizon.com/secure-access/services/saml/...
https://RYDLJLBD-VR-PNF.securegateway.verizon.com/secure-access/services/saml/lo...

Please provide details that uniquely identifies the SAML identity provider.

Single-Sign-on URL *:

Identity provider entity ID *: https://www.okta.com/identity-provider-entity

Identity provider certificate *:

Group attribute: http://schemas.microsoft.com/ws/2008/06/i

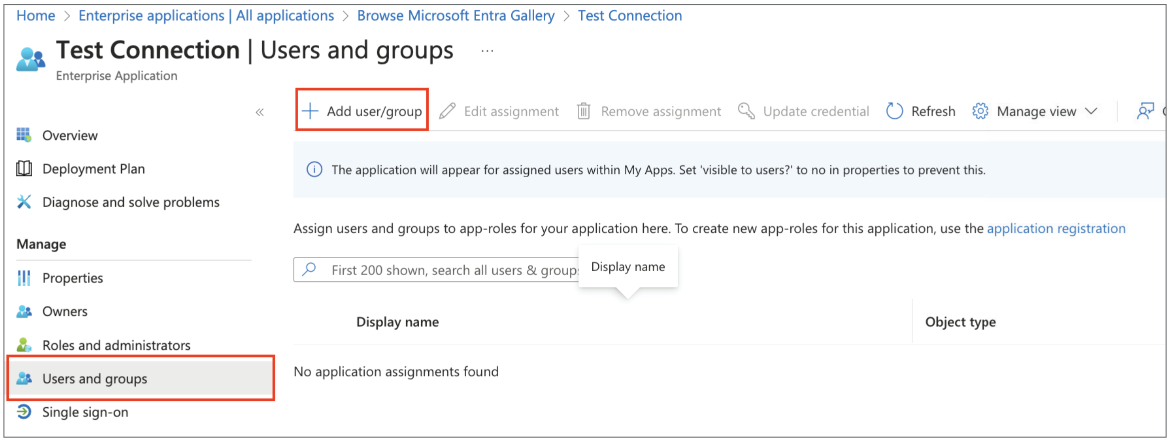
LDAP Interface

Only select if your identity provider supports it.

○ Yes ● No

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"**



Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Test Connection

Test Connection | Users and groups

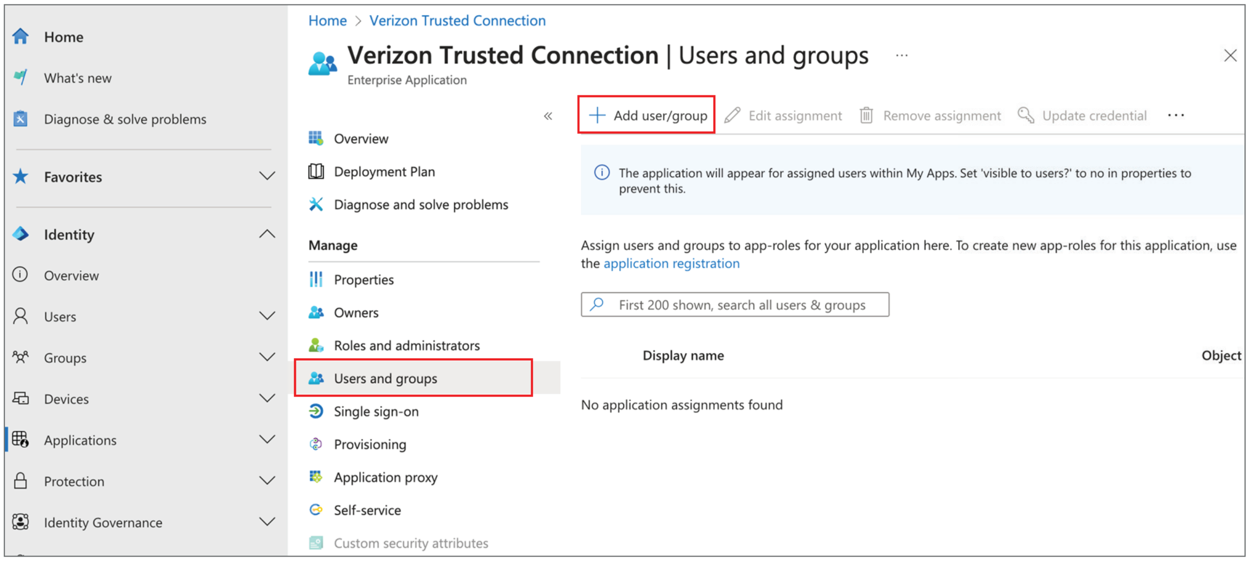
Enterprise Application

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

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration

Display name	Object type
No application assignments found	

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

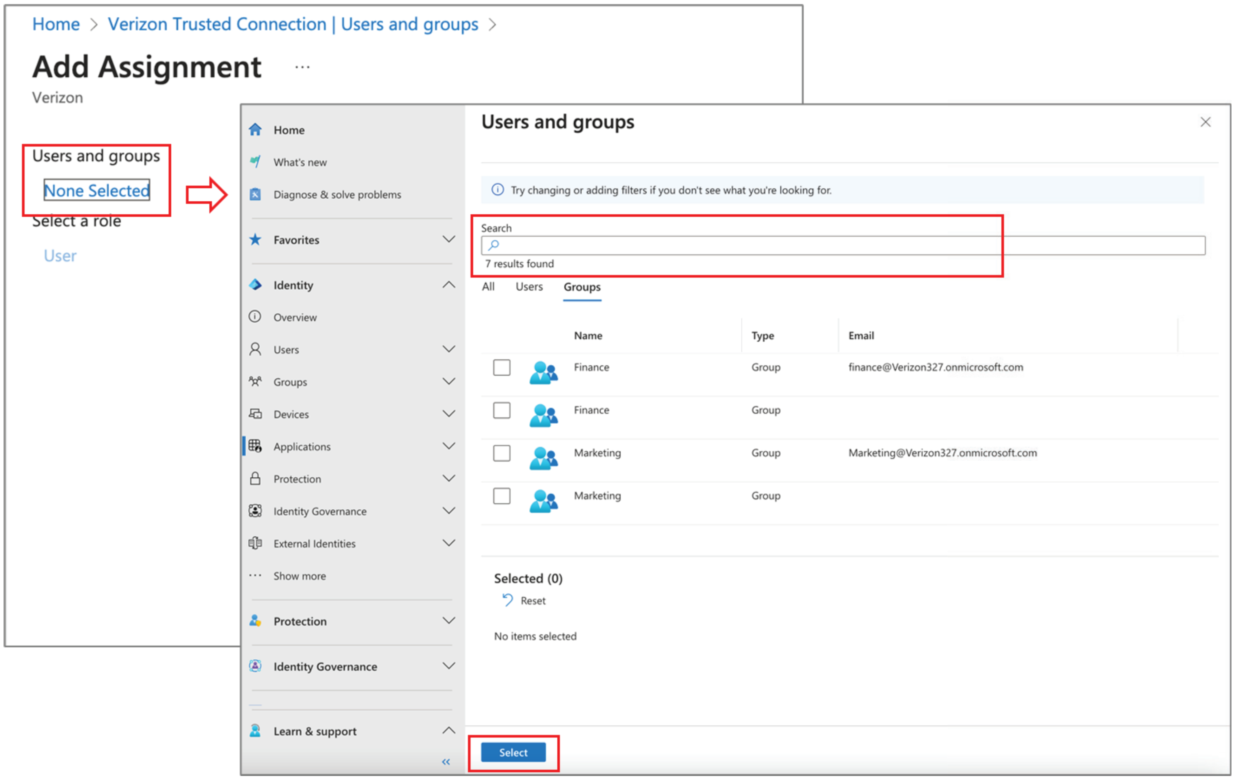


The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration

No application assignments found

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



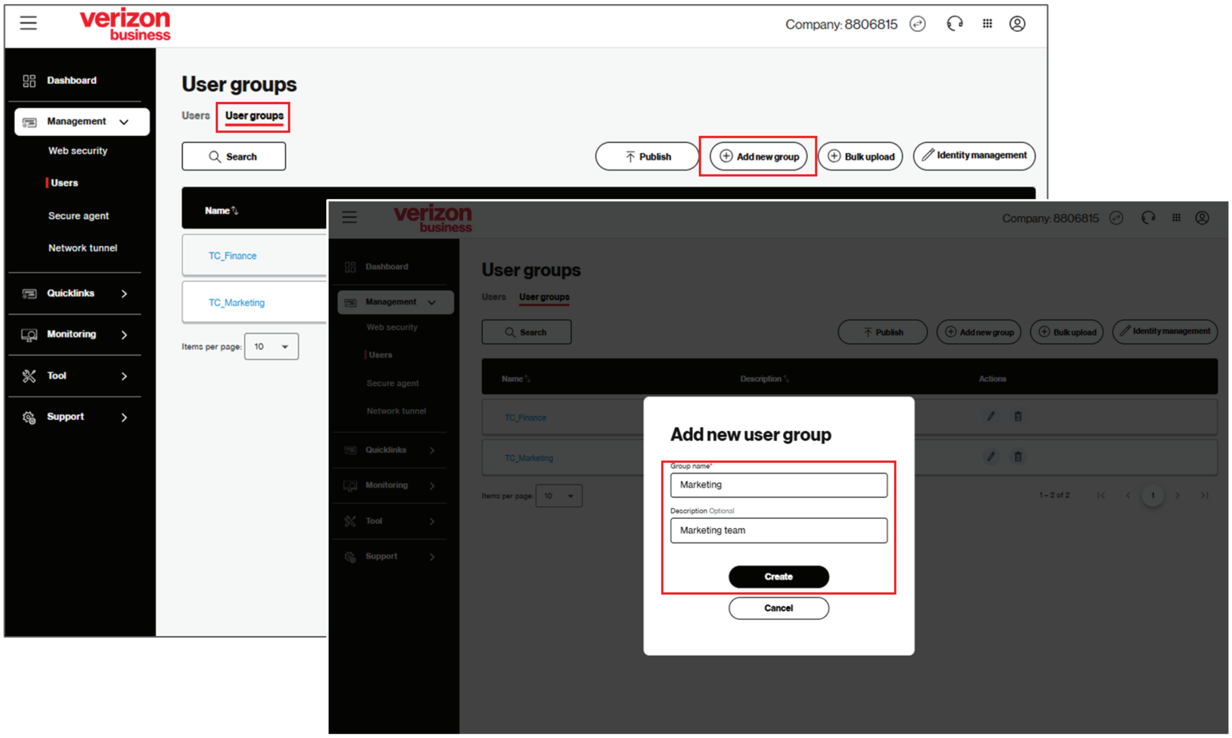
Try changing or adding filters if you don't see what you're looking for.

	Name	Type	Email
□	Finance	Group	finance@Verizon327.onmicrosoft.com
□	Finance	Group	
□	Marketing	Group	Marketing@Verizon327.onmicrosoft.com
□	Marketing	Group	

No items selected

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.



Add new user group

Group name*: Marketing

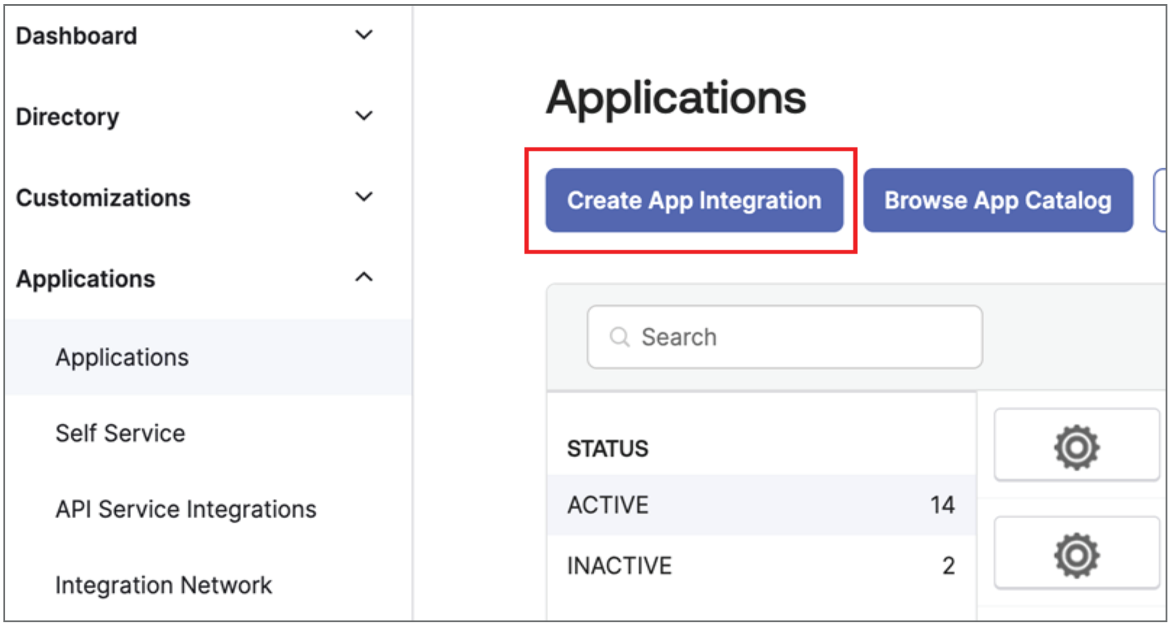
Description Optional: Marketing team

Okta Integration for SAML Authentication

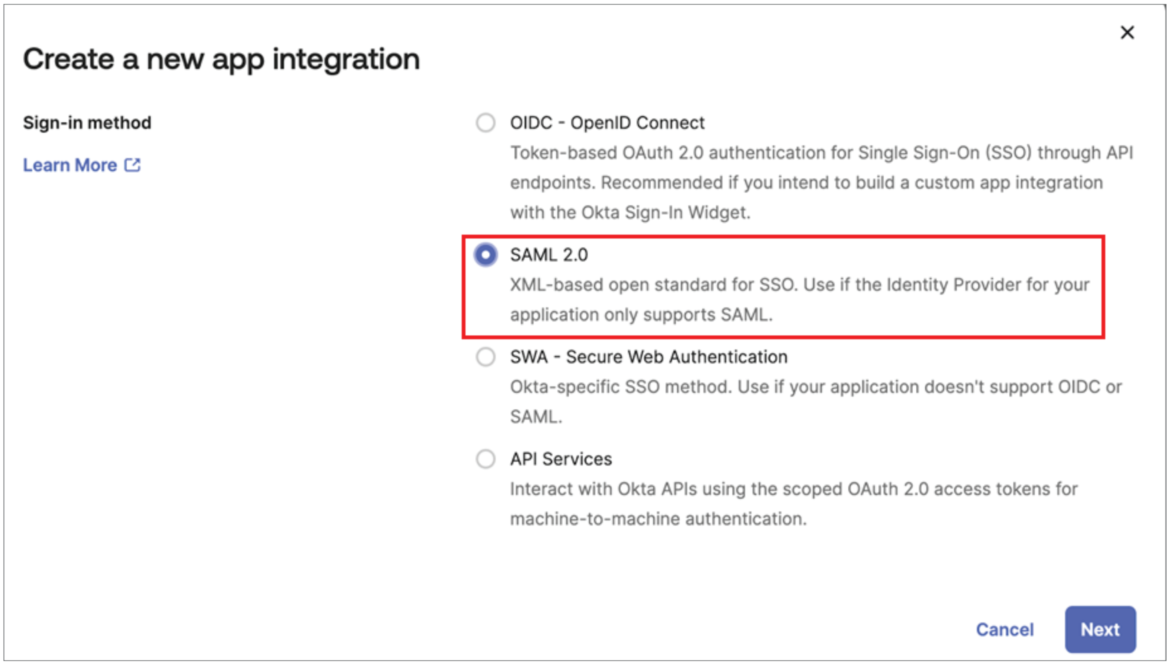
The following steps demonstrate how to integrateTrusted Connection with Okta, for SAML authentication. Instructions on how to integrate with the OKTA LDAP interface are located in the next section.

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"**.



Create a new app integration

Sign-in method

Learn More

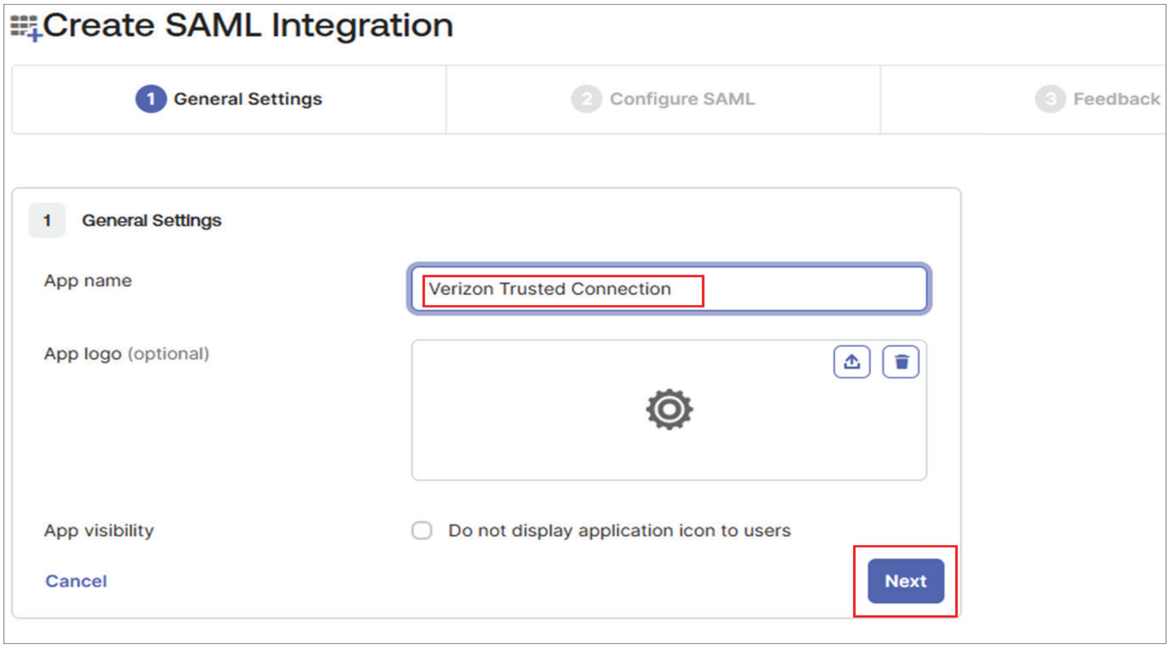
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

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



Create SAML Integration

1 General Settings

App name: Verizon Trusted Connection

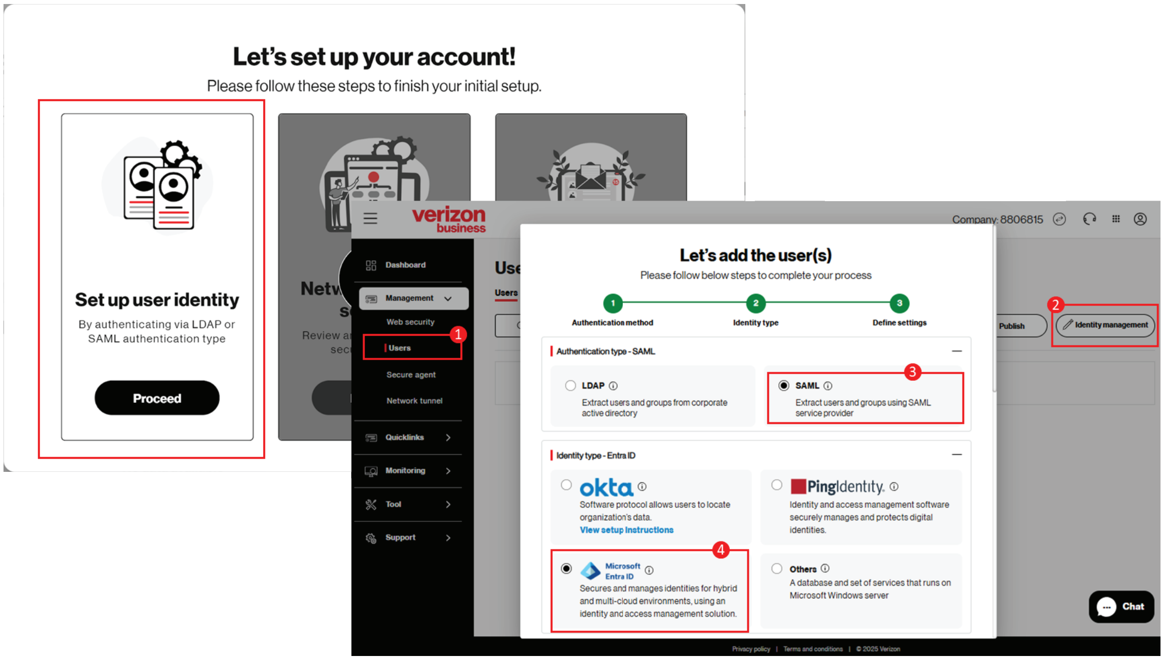
App logo (optional)

App visibility: □ Do not display application icon to users

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



Let's set up your account!

Please follow these steps to finish your initial setup.

Set up user identity

By authenticating via LDAP or SAML authentication type

Let's add the user(s)

Please follow below steps to complete your process

Authentication type - SAML

○ LDAP ⓘ Extract users and groups from corporate active directory

● SAML ⓘ Extract users and groups using SAML service provider

Identity type - Entra ID

○ okta ⓘ Software protocol allows users to locate organization's data. View setup instructions

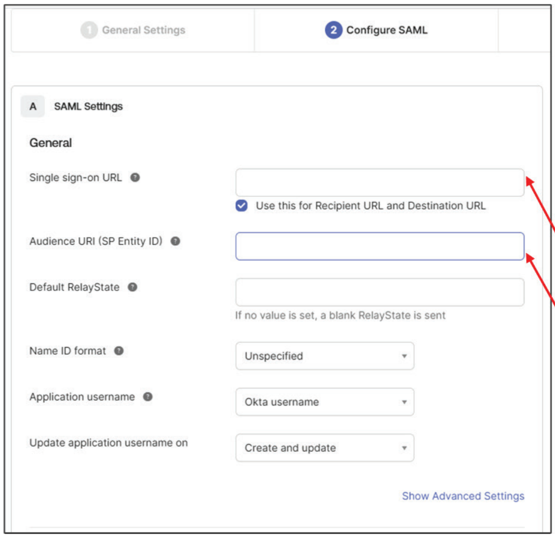
○ PingIdentity. ⓘ Identity and access management software securely manages and protects digital identities.

● Microsoft Entra ID ⓘ Secures and manages identities for hybrid and multi-cloud environments, using an identity and access management solution.

○ Others ⓘ A database and set of services that runs on Microsoft Windows server

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.



A SAML Settings

General

Single sign-on URL:

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID):

Default RelayState:

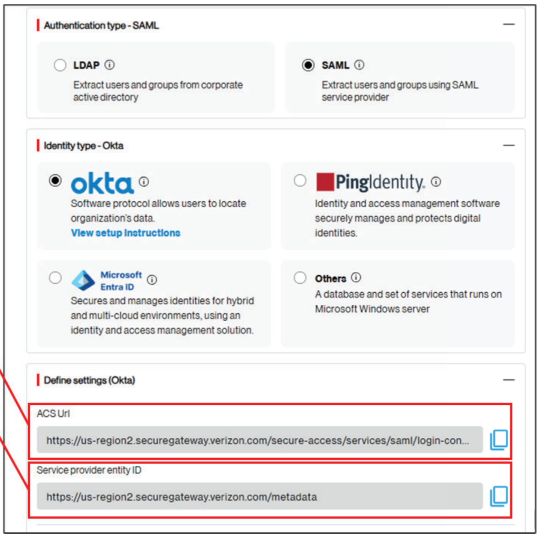
If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

Update application username on: Create and update

Entry ID browser tab



Authentication type - SAML

○ LDAP ⓘ Extract users and groups from corporate active directory

● SAML ⓘ Extract users and groups using SAML service provider

Identity type - Okta

● okta ⓘ Software protocol allows users to locate organization's data. View setup instructions

○ PingIdentity. ⓘ Identity and access management software securely manages and protects digital identities.

○ Microsoft Entra ID ⓘ Secures and manages identities for hybrid and multi-cloud environments, using an identity and access management solution.

○ Others ⓘ A database and set of services that runs on Microsoft Windows server

Define settings (Okta)

ACS Url: https://us-region2.securegateway.verizon.com/secure-access/services/saml/login-con...

Service provider entity ID: https://us-region2.securegateway.verizon.com/metadata

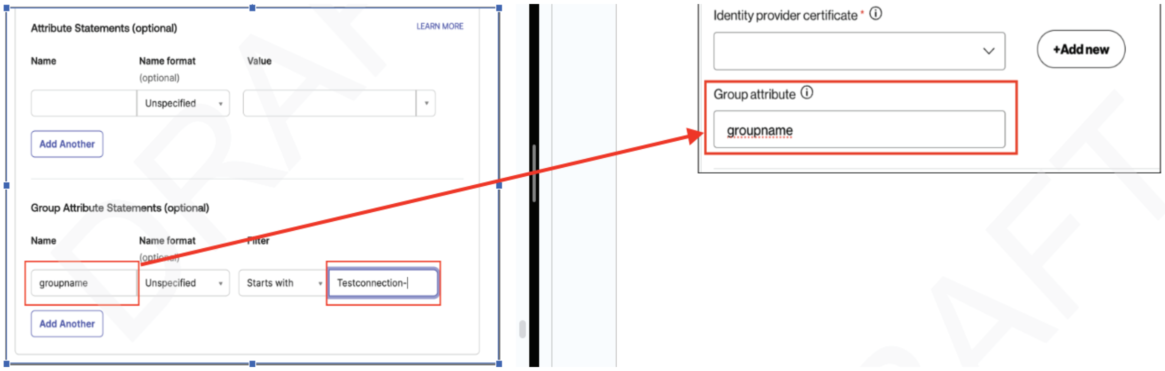
Trusted Connection browser tab

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.



Attribute Statements (optional)

Name	Name format (optional)	Value
	Unspecified	

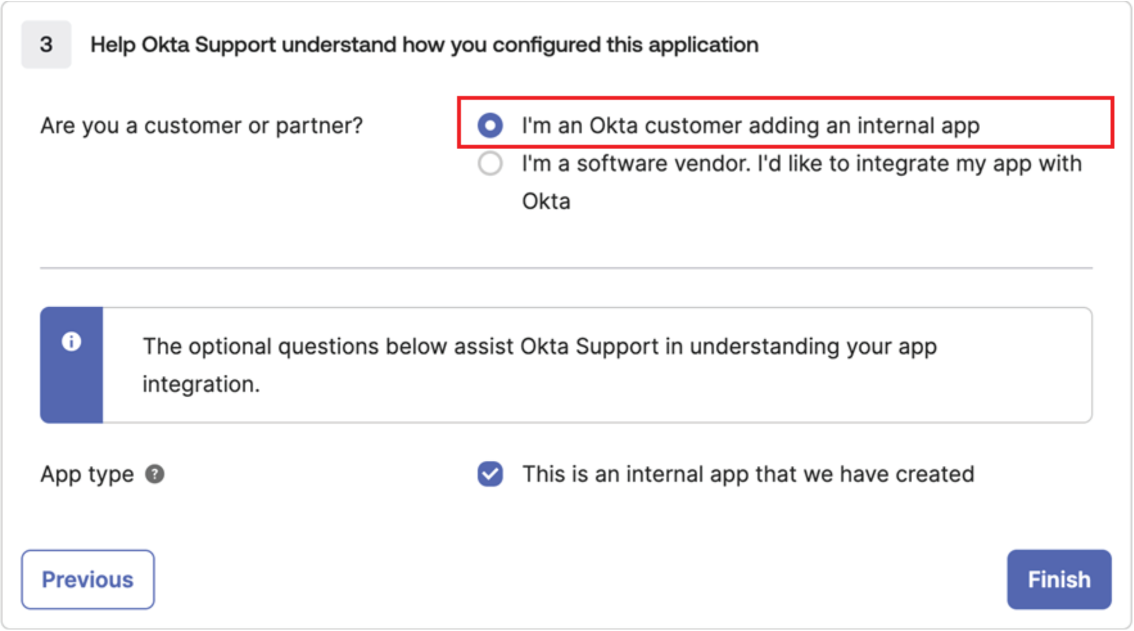
Group Attribute Statements (optional)

Name	Name format (optional)	Filter	
groupname	Unspecified	Starts with	Testconnection-

Identity provider certificate *

Group attribute: groupname

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



3 Help Okta Support understand how you configured this application

Are you a customer or partner?

● I'm an Okta customer adding an internal app

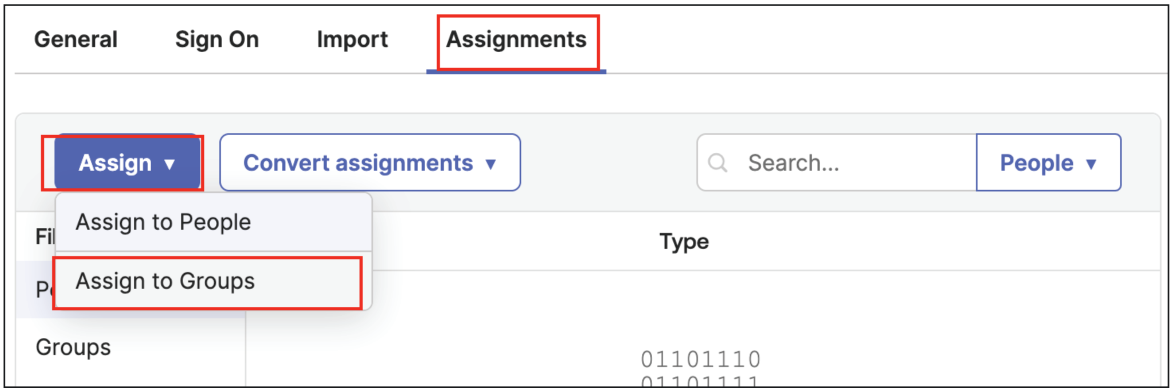
○ I'm a software vendor. I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

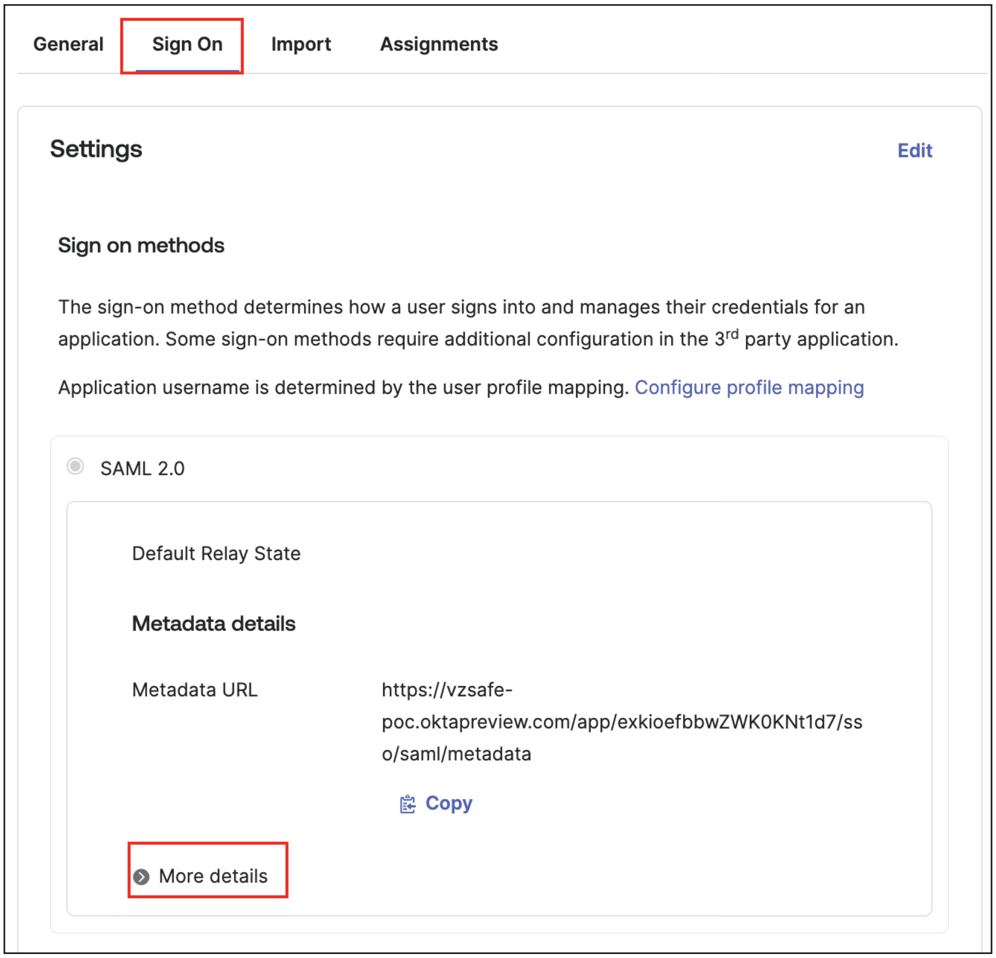
App type ☑ This is an internal app that we have created

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**”.



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

○ SAML 2.0

Default Relay State

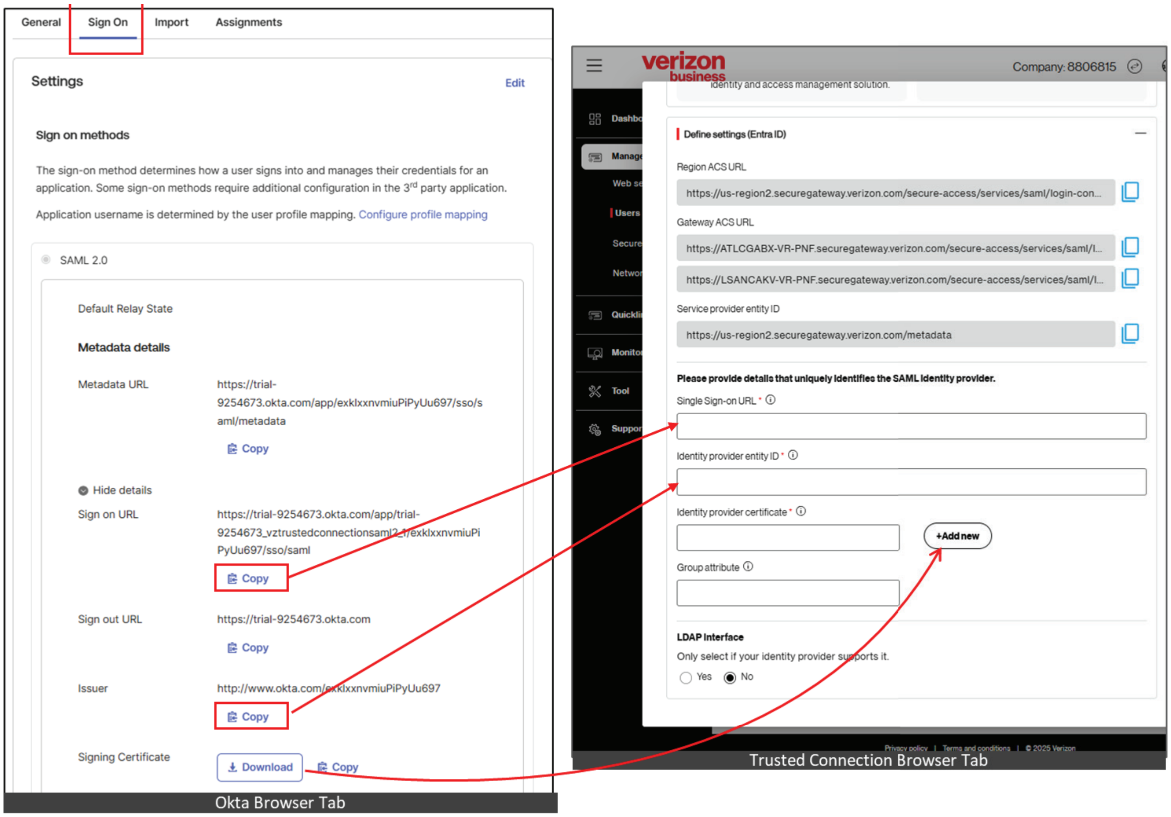
Metadata details

Metadata URL https://vzsafe-poc.oktapreview.com/app/exkioefbbwZWK0KNt1d7/sso/saml/metadata

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.



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

SAML 2.0

Default Relay State

Metadata details

Metadata URL: https://trial-9254673.okta.com/app/exklxxnvmiuPiPyUu697/sso/saml/metadata

Hide details

Sign on URL: https://trial-9254673.okta.com/app/trial-9254673_vztrustedconnectionsaml2_1/exklxxnvmiuPiPyUu697/sso/saml

Sign out URL: https://trial-9254673.okta.com

Issuer: http://www.okta.com/exklxxnvmiuPiPyUu697

Signing Certificate

Okta Browser Tab

Company: 8806815

identity and access management solution.

Define settings (Entra ID)

Region ACS URL: https://us-region2.securegateway.verizon.com/secure-access/services/saml/login-con...

Gateway ACS URL: https://ATLCGABX-VR-PNF.securegateway.verizon.com/secure-access/services/saml/l...
https://LSANCAKV-VR-PNF.securegateway.verizon.com/secure-access/services/saml/l...

Service provider entity ID: https://us-region2.securegateway.verizon.com/metadata

Please provide details that uniquely identifies the SAML identity provider.

Single Sign-on URL *

Identity provider entity ID *

Identity provider certificate *

Group attribute

LDAP Interface

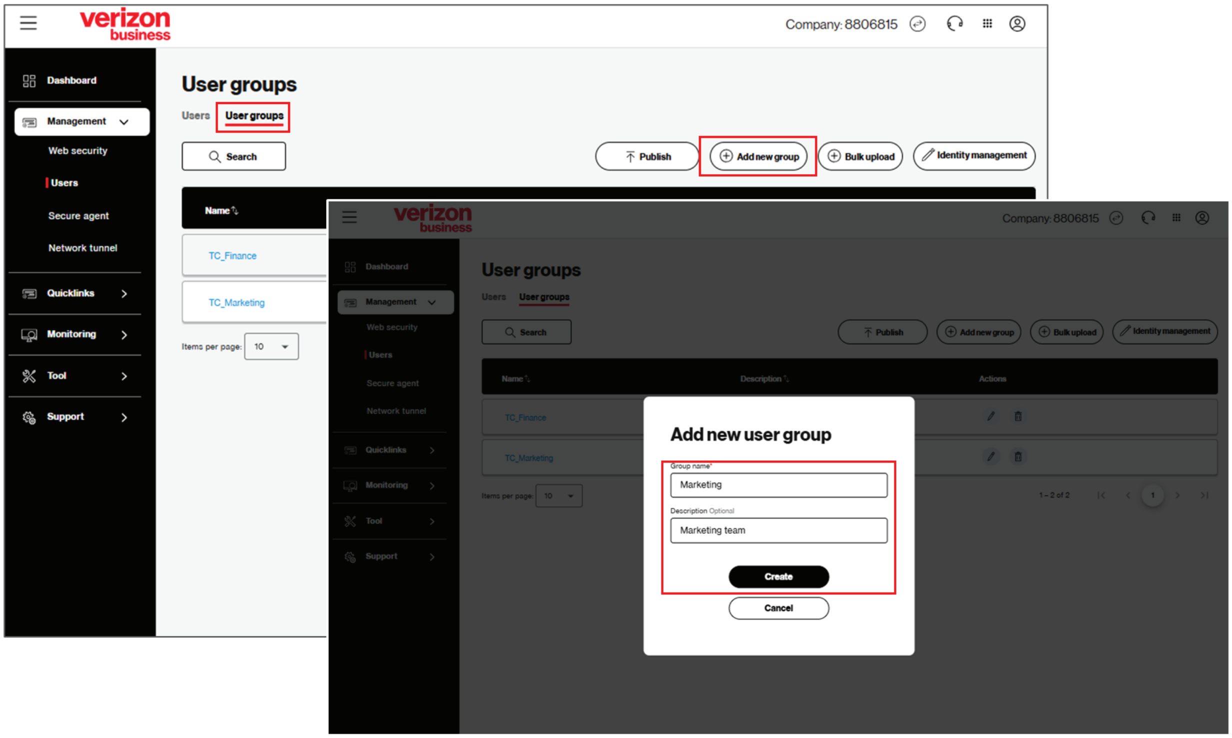
Only select if your identity provider supports it.

○ Yes ● No

Trusted Connection Browser Tab

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.



Add new user group

Group name*: Marketing

Description Optional: Marketing team

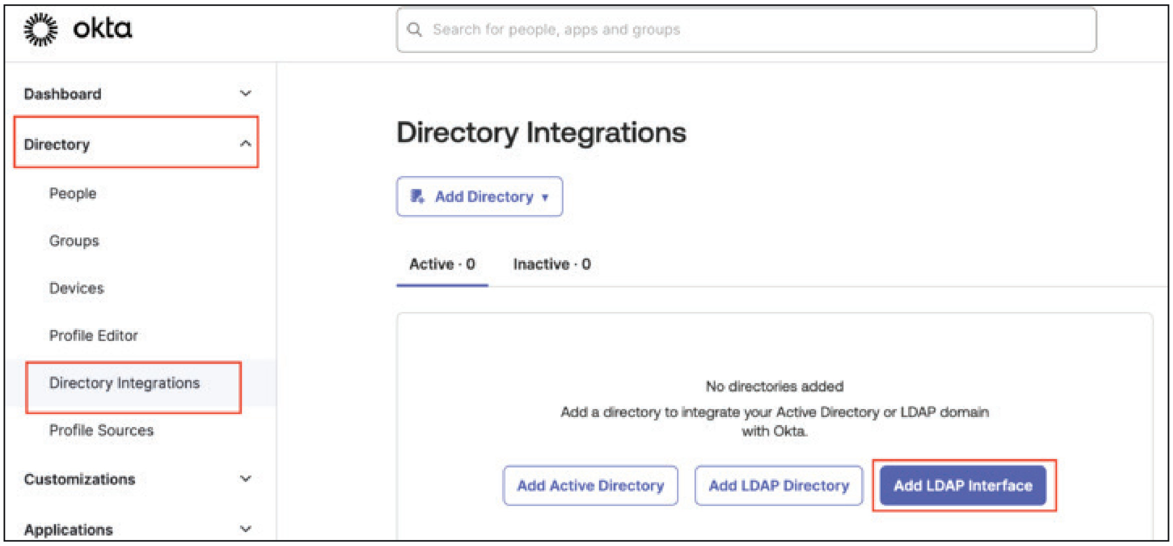
Create

Cancel

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”**.

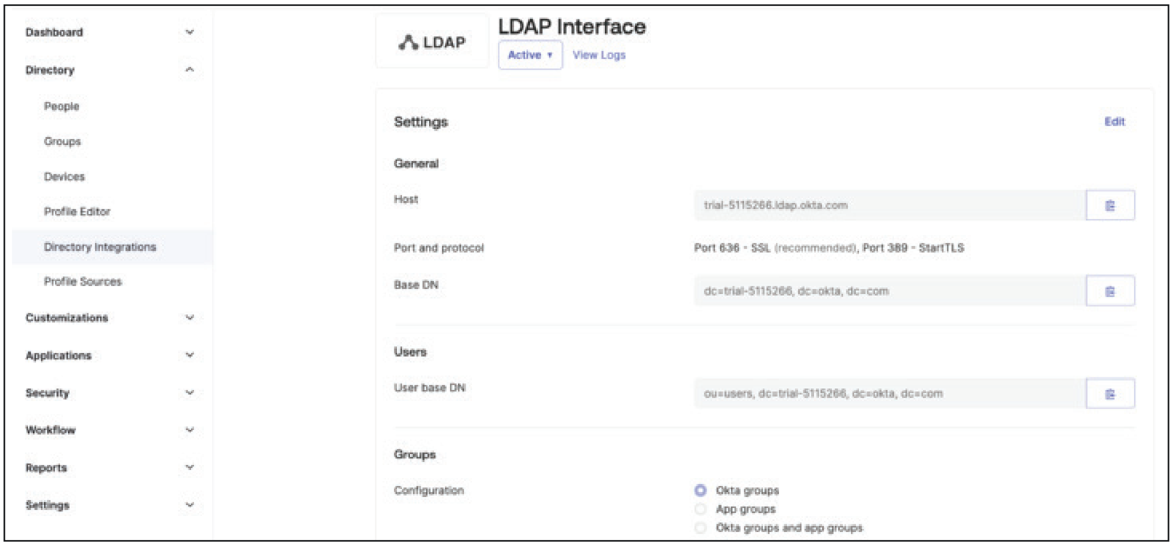


No directories added

Add a directory to integrate your Active Directory or LDAP domain with Okta.

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.



Host: trial-5115266.ldap.okta.com

Port and protocol: Port 636 - SSL (recommended), Port 389 - StartTLS

Base DN: dc=trial-5115266, dc=okta, dc=com

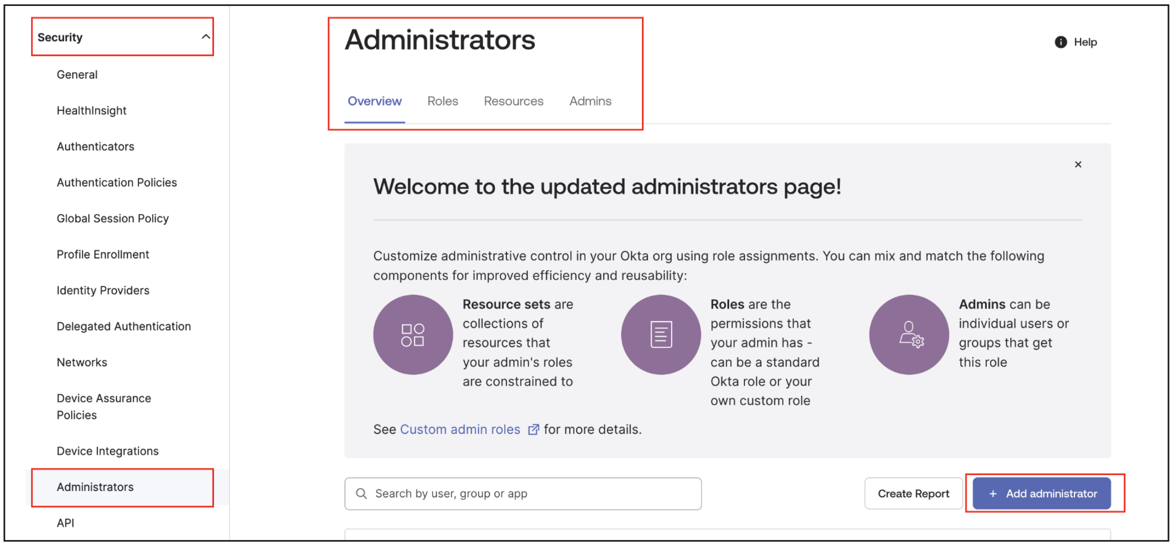
User base DN: ou=users, dc=trial-5115266, dc=okta, dc=com

Configuration: ● Okta groups ○ App groups ○ Okta groups and app groups

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.



Administrators

Welcome to the updated administrators page!

Customize administrative control in your Okta org using role assignments. You can mix and match the following components for improved efficiency and reusability:

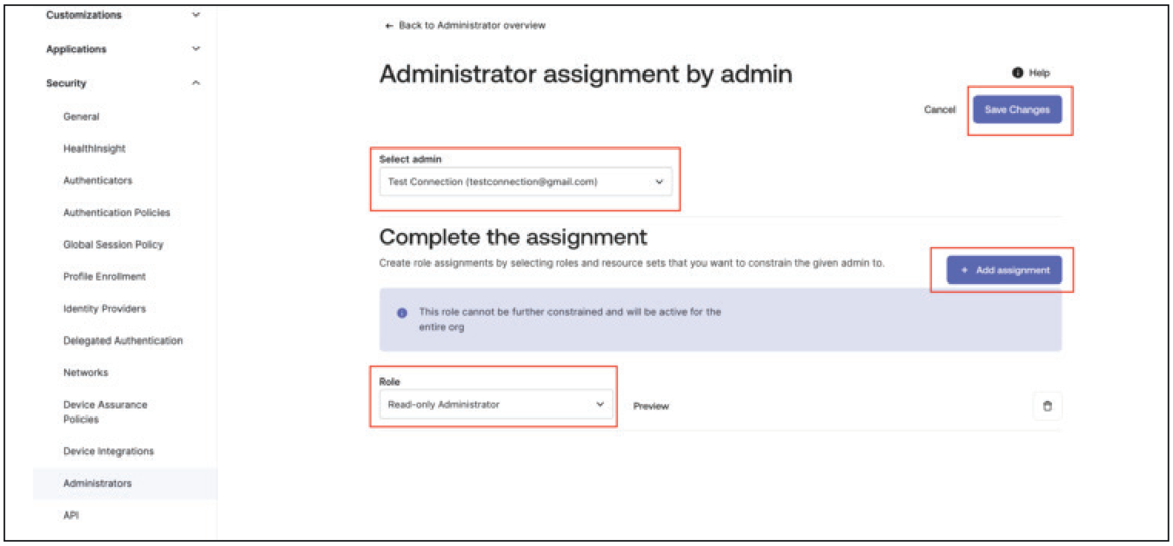
Resource sets are collections of resources that your admin's roles are constrained to

Roles are the permissions that your admin has - can be a standard Okta role or your own custom role

Admins can be individual users or groups that get this role

See Custom admin roles for more details.

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”**.



Administrator assignment by admin

Select admin: Test Connection (testconnection@gmail.com)

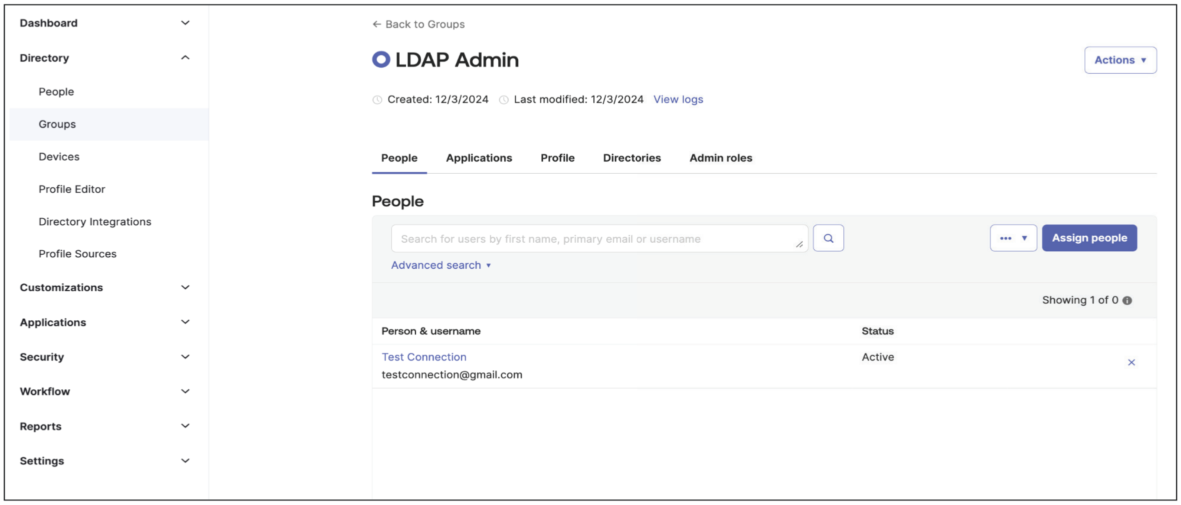
Complete the assignment

Create role assignments by selecting roles and resource sets that you want to constrain the given admin to.

This role cannot be further constrained and will be active for the entire org

Role: Read-only Administrator

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.



LDAP Admin

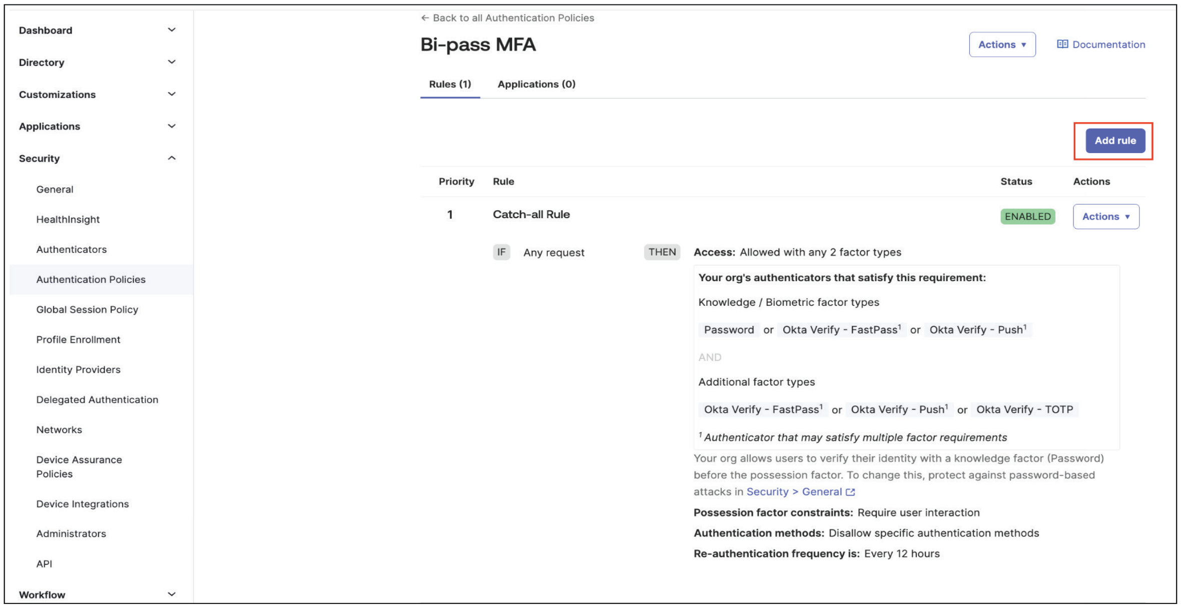
Created: 12/3/2024 Last modified: 12/3/2024 View logs

People

Showing 1 of 0

Person & username	Status
Test Connection testconnection@gmail.com	Active

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"**.



Bi-pass MFA

Priority	Rule	Status	Actions
1	Catch-all Rule	ENABLED	Actions ▾

IF Any request THEN **Access:** Allowed with any 2 factor types

Your org's authenticators that satisfy this requirement:

Knowledge / Biometric factor types

Password or Okta Verify - FastPass[1] or Okta Verify - Push[1]

AND

Additional factor types

Okta Verify - FastPass[1] or Okta Verify - Push[1] or Okta Verify - TOTP

[1] *Authenticator that may satisfy multiple factor requirements*

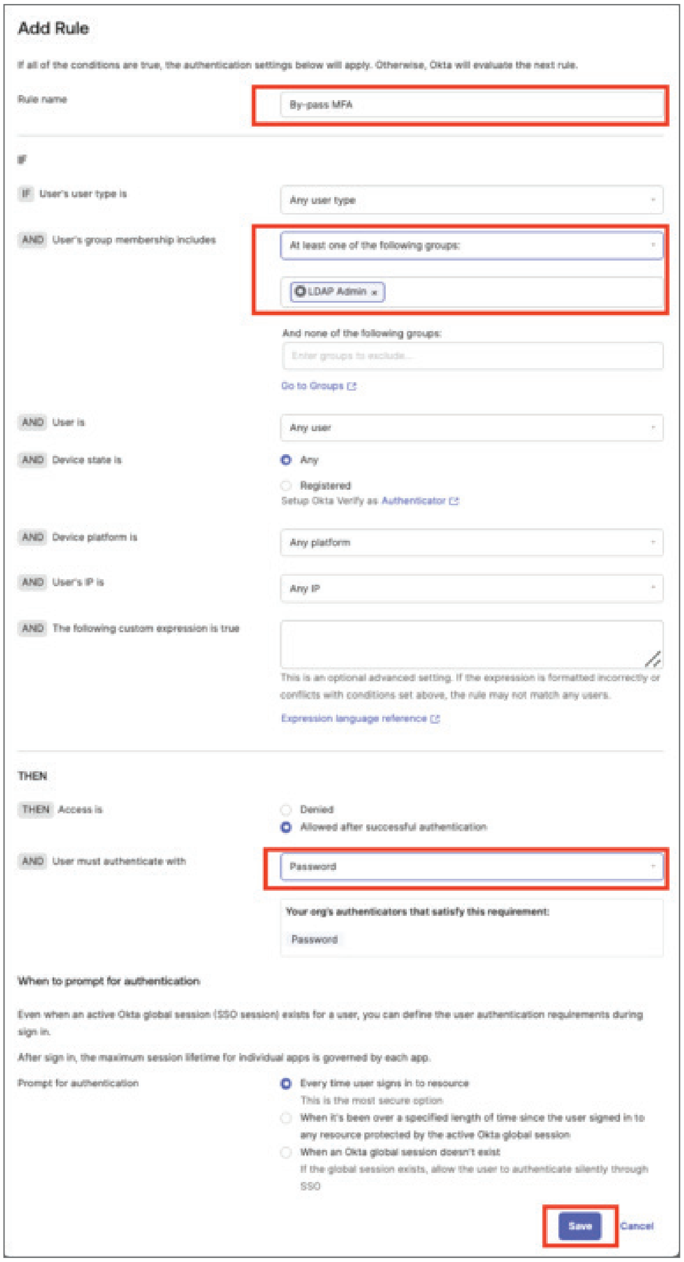
Your org allows users to verify their identity with a knowledge factor (Password) before the possession factor. To change this, protect against password-based attacks in Security > General

Possession factor constraints: Require user interaction

Authentication methods: Disallow specific authentication methods

Re-authentication frequency is: Every 12 hours

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.



Add Rule

If all of the conditions are true, the authentication settings below will apply. Otherwise, Okta will evaluate the next rule.

Rule name: By-pass MFA

IF

IF User's user type is: Any user type

AND User's group membership includes: At least one of the following groups: LDAP Admin ×

And none of the following groups: Enter groups to exclude...

Go to Groups

AND User is: Any user

AND Device state is:
● Any
○ Registered
Setup Okta Verify as Authenticator

AND Device platform is: Any platform

AND User's IP is: Any IP

AND The following custom expression is true:

This is an optional advanced setting. If the expression is formatted incorrectly or conflicts with conditions set above, the rule may not match any users.

Expression language reference

THEN

THEN Access is:
○ Denied
● Allowed after successful authentication

AND User must authenticate with: Password

Your org's authenticators that satisfy this requirement:

Password

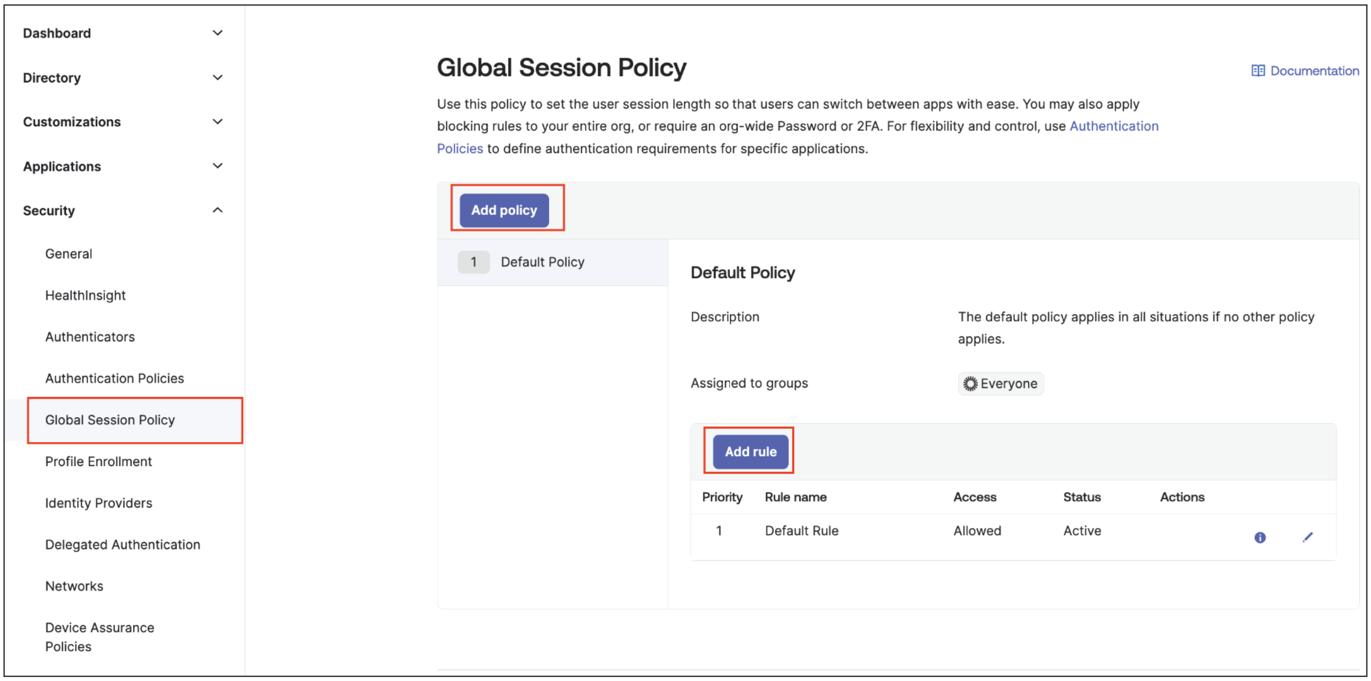
When to prompt for authentication

Even when an active Okta global session (SSO session) exists for a user, you can define the user authentication requirements during sign in.

After sign in, the maximum session lifetime for individual apps is governed by each app.

Prompt for authentication:
● Every time user signs in to resource
This is the most secure option
○ When it's been over a specified length of time since the user signed in to any resource protected by the active Okta global session
○ When an Okta global session doesn't exist
If the global session exists, allow the user to authenticate silently through SSO

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”**.



Global Session Policy

Use this policy to set the user session length so that users can switch between apps with ease. You may also apply blocking rules to your entire org, or require an org-wide Password or 2FA. For flexibility and control, use Authentication Policies to define authentication requirements for specific applications.

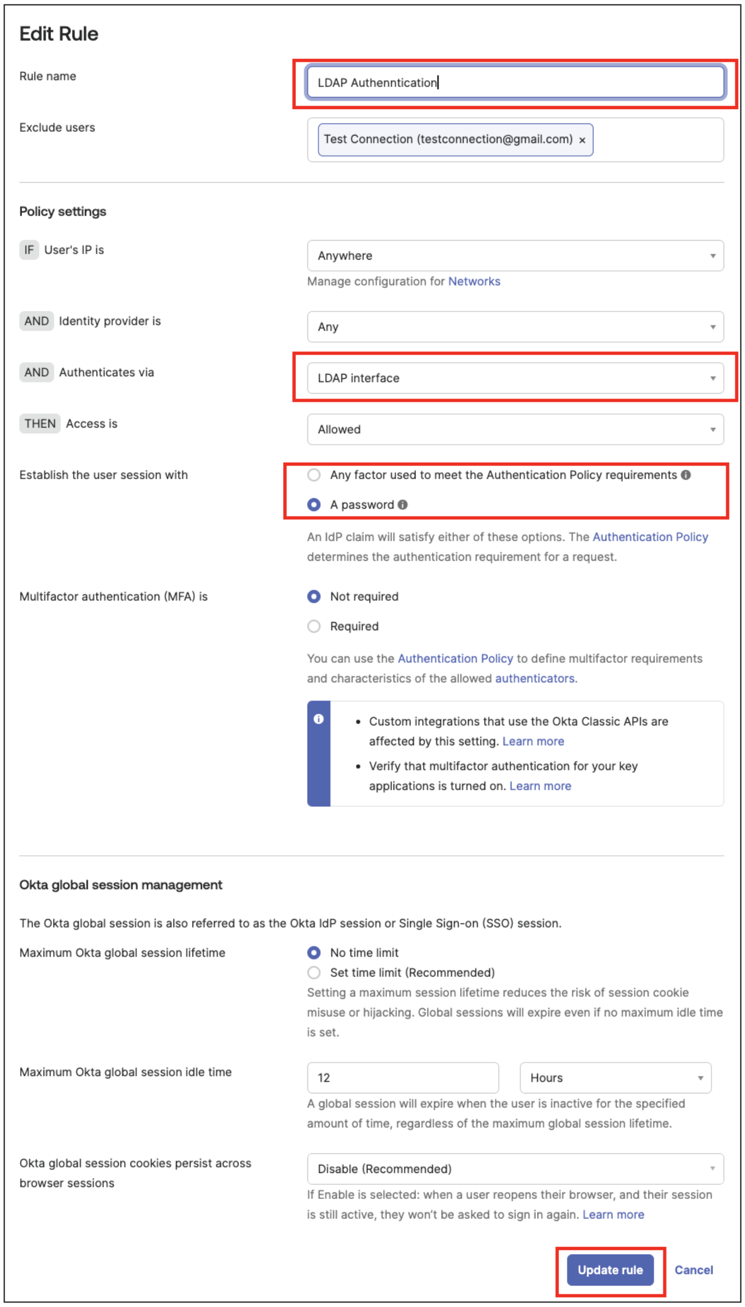
Default Policy

Description: The default policy applies in all situations if no other policy applies.

Assigned to groups: Everyone

Priority	Rule name	Access	Status	Actions
1	Default Rule	Allowed	Active	

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"**.



Edit Rule

Rule name: LDAP Authenntication

Exclude users: Test Connection (testconnection@gmail.com) ×

Policy settings

IF User's IP is: Anywhere

Manage configuration for Networks

AND Identity provider is: Any

AND Authenticates via: LDAP interface

THEN Access is: Allowed

Establish the user session with:

○ Any factor used to meet the Authentication Policy requirements

● A password

An IdP claim will satisfy either of these options. The Authentication Policy determines the authentication requirement for a request.

Multifactor authentication (MFA) is:

● Not required

○ Required

You can use the Authentication Policy to define multifactor requirements and characteristics of the allowed authenticators.

- Custom integrations that use the Okta Classic APIs are affected by this setting. Learn more
- Verify that multifactor authentication for your key applications is turned on. Learn more

Okta global session management

The Okta global session is also referred to as the Okta IdP session or Single Sign-on (SSO) session.

Maximum Okta global session lifetime:

● No time limit

○ Set time limit (Recommended)

Setting a maximum session lifetime reduces the risk of session cookie misuse or hijacking. Global sessions will expire even if no maximum idle time is set.

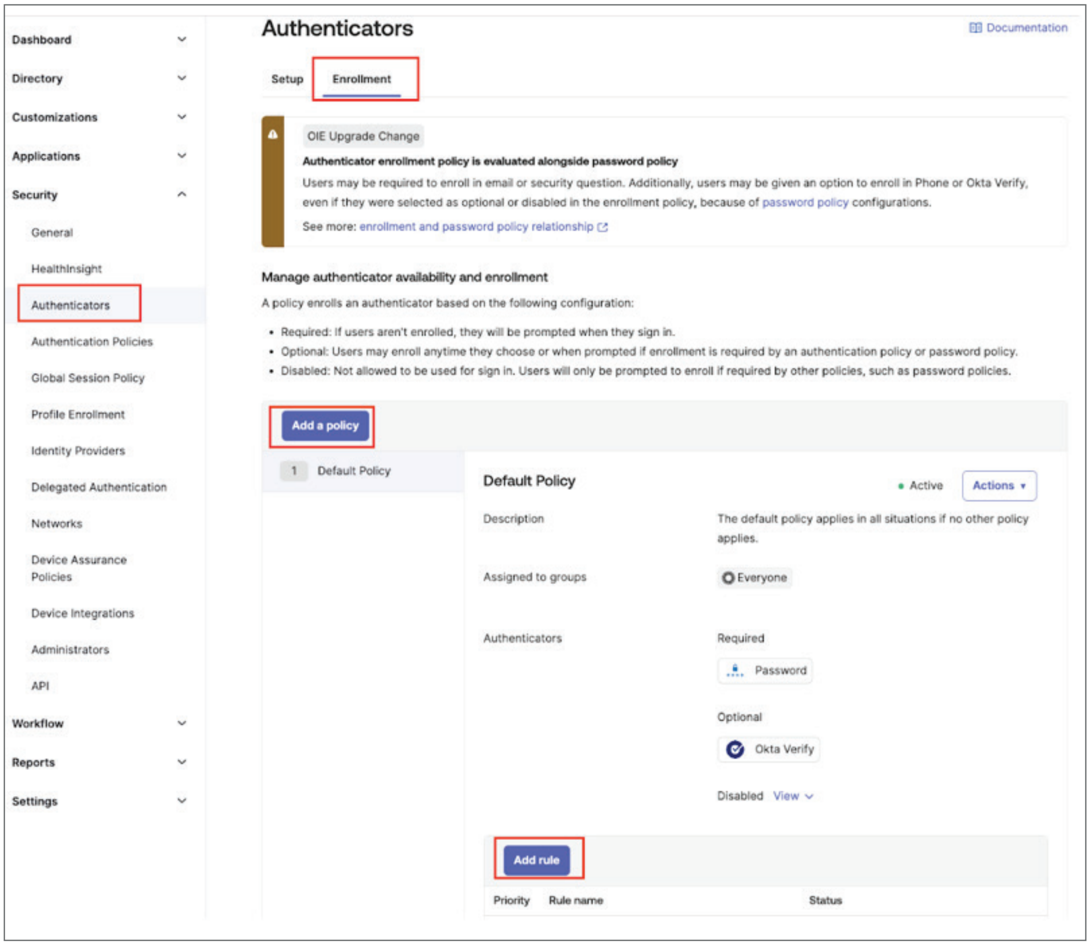
Maximum Okta global session idle time: 12 Hours

A global session will expire when the user is inactive for the specified amount of time, regardless of the maximum global session lifetime.

Okta global session cookies persist across browser sessions: Disable (Recommended)

If Enable is selected: when a user reopens their browser, and their session is still active, they won't be asked to sign in again. Learn more

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



Authenticators

OIE Upgrade Change

Authenticator enrollment policy is evaluated alongside password policy

Users may be required to enroll in email or security question. Additionally, users may be given an option to enroll in Phone or Okta Verify, even if they were selected as optional or disabled in the enrollment policy, because of password policy configurations.

See more: enrollment and password policy relationship

Manage authenticator availability and enrollment

A policy enrolls an authenticator based on the following configuration:

- Required: If users aren't enrolled, they will be prompted when they sign in.
- Optional: Users may enroll anytime they choose or when prompted if enrollment is required by an authentication policy or password policy.
- Disabled: Not allowed to be used for sign in. Users will only be prompted to enroll if required by other policies, such as password policies.

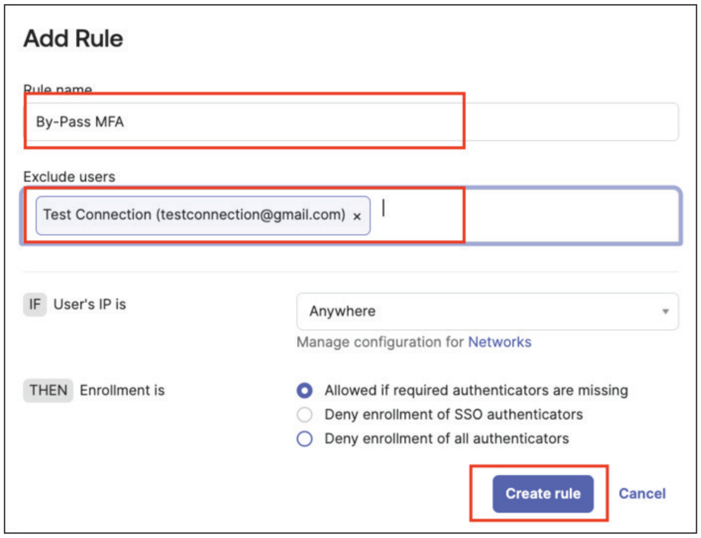
1 Default Policy

Default Policy ● Active

Description	The default policy applies in all situations if no other policy applies.
Assigned to groups	Everyone
Authenticators	Required Password Optional Okta Verify Disabled View ⌄

Priority	Rule name	Status

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"**.



Add Rule

Rule name: By-Pass MFA

Exclude users: Test Connection (testconnection@gmail.com) ×

IF User's IP is: Anywhere

Manage configuration for Networks

THEN Enrollment is

● Allowed if required authenticators are missing
○ Deny enrollment of SSO authenticators
○ Deny enrollment of all authenticators

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:

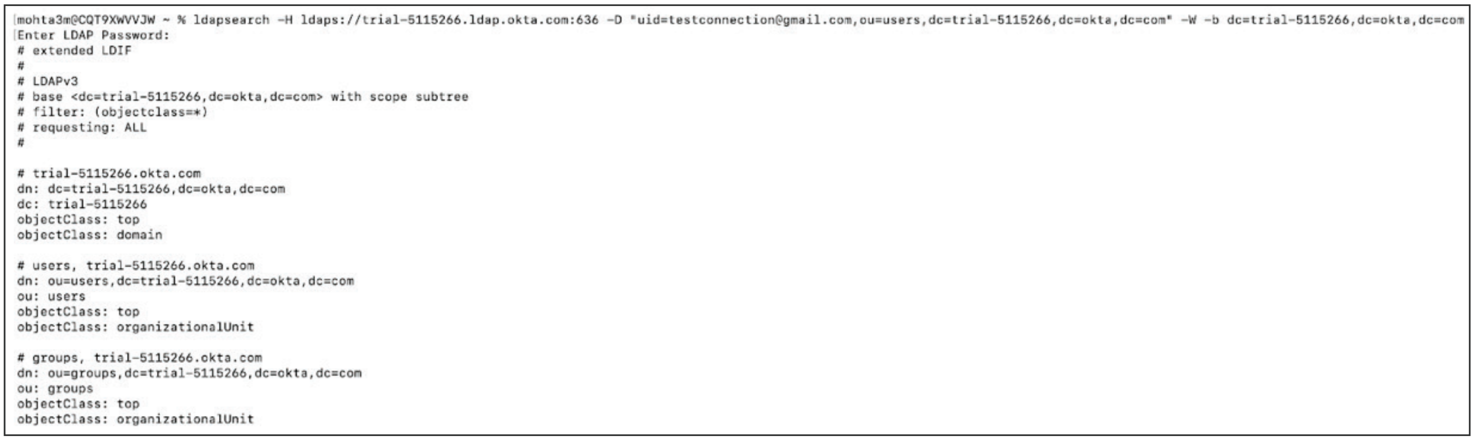
ldapsearch -H ldaps://[subdomain].ldap.okta.com:636 -D “uid=[user@domain.com],ou=users,dc=[subdomain],dc=okta,dc=com” -W -b dc=[subdomain],dc=okta,dc=com

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



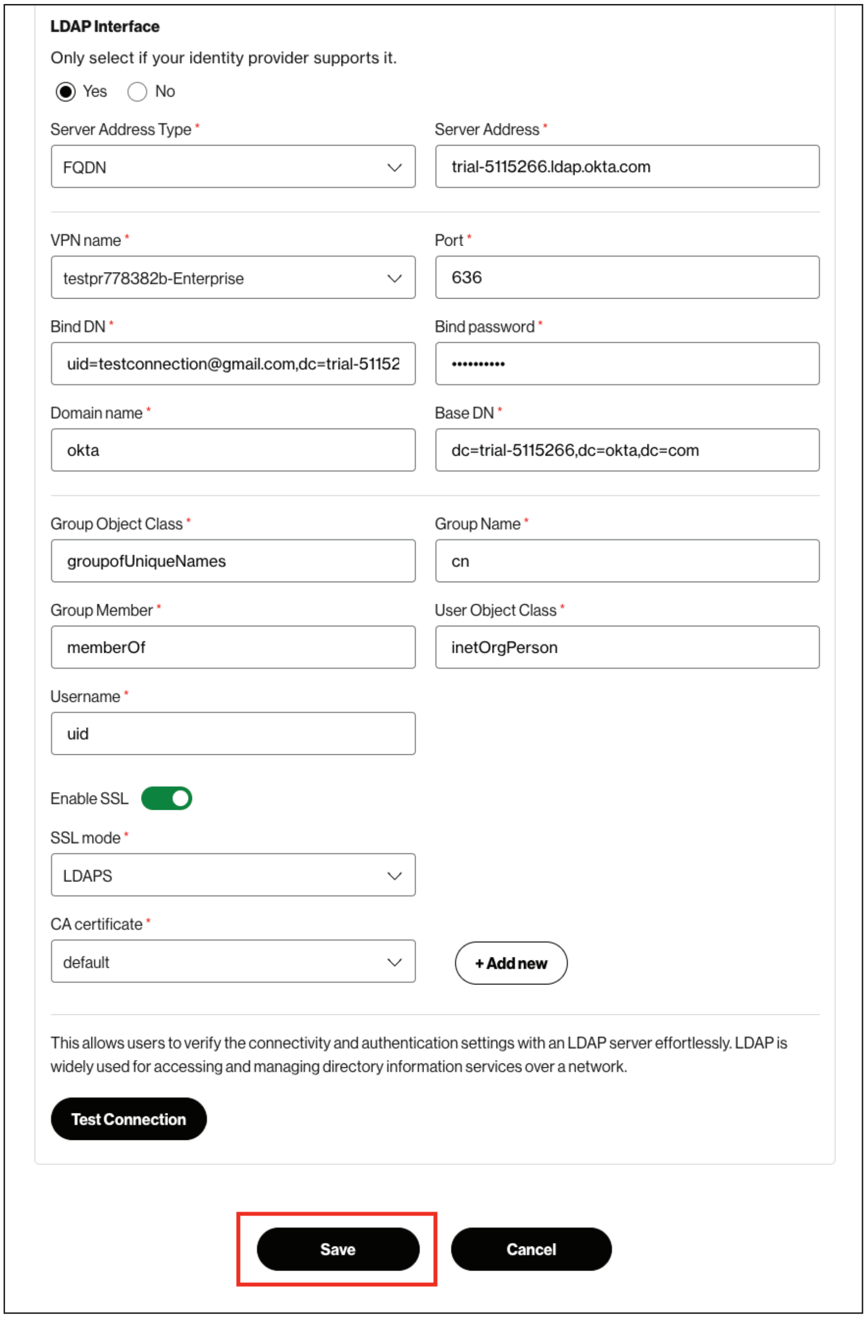
```
mohta3m@CQT9XWVVJW ~ % ldapsearch -H ldaps://trial-5115266.ldap.okta.com:636 -D "uid=testconnection@gmail.com,ou=users,dc=trial-5115266,dc=okta,dc=com" -W -b dc=trial-5115266,dc=okta,dc=com
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=trial-5115266,dc=okta,dc=com> with scope subtree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



LDAP Interface

Only select if your identity provider supports it.

● Yes ○ No

Server Address Type *	Server Address *
FQDN	trial-5115266.ldap.okta.com
VPN name *	Port *
testpr778382b-Enterprise	636
Bind DN *	Bind password *
uid=testconnection@gmail.com,dc=trial-51152	••••••••••
Domain name *	Base DN *
okta	dc=trial-5115266,dc=okta,dc=com
Group Object Class *	Group Name *
groupofUniqueNames	cn
Group Member *	User Object Class *
memberOf	inetOrgPerson
Username *	
uid	

Enable SSL

SSL mode *: LDAPS

CA certificate *: default

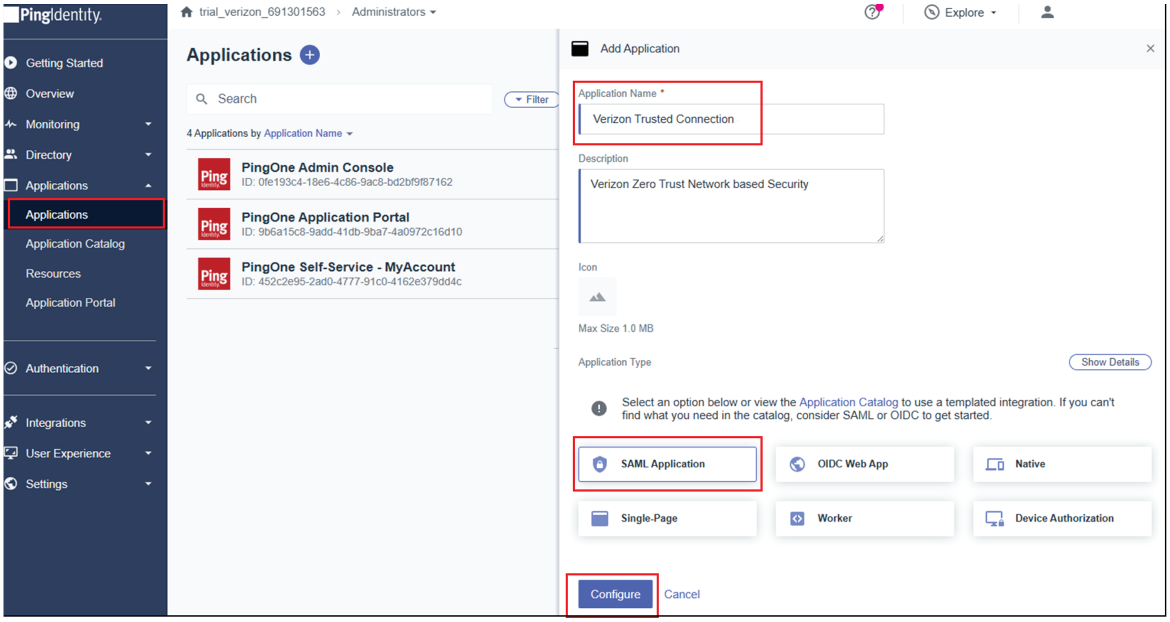
This allows users to verify the connectivity and authentication settings with an LDAP server effortlessly. LDAP is widely used for accessing and managing directory information services over a network.

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".**



PingOne Admin Console
ID: 0fe193c4-18e6-4c86-9ac8-bd2bf9f87162

PingOne Application Portal
ID: 9b6a15c8-9add-41db-9ba7-4a0972c16d10

PingOne Self-Service - MyAccount
ID: 452c2e95-2ad0-4777-91c0-4162e379dd4c

Application Name *
Verizon Trusted Connection

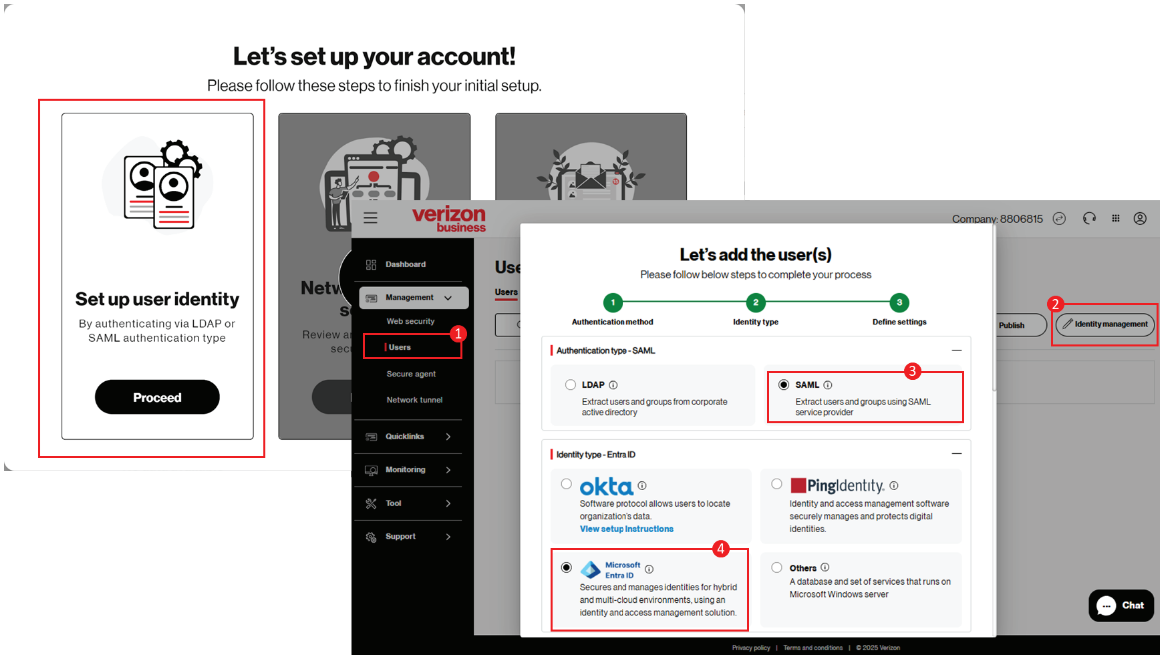
Description
Verizon Zero Trust Network based Security

Select an option below or view the Application Catalog to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

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



Let's set up your account!

Please follow these steps to finish your initial setup.

Set up user identity

By authenticating via LDAP or SAML authentication type

Proceed

verizon business

Company: 8806815

Let's add the user(s)

Please follow below steps to complete your process

1 Authentication method — 2 Identity type — 3 Define settings

Authentication type - SAML

○ LDAP ⓘ Extract users and groups from corporate active directory

3 ● SAML ⓘ Extract users and groups using SAML service provider

Identity type - Entra ID

○ okta ⓘ Software protocol allows users to locate organization's data. View setup Instructions

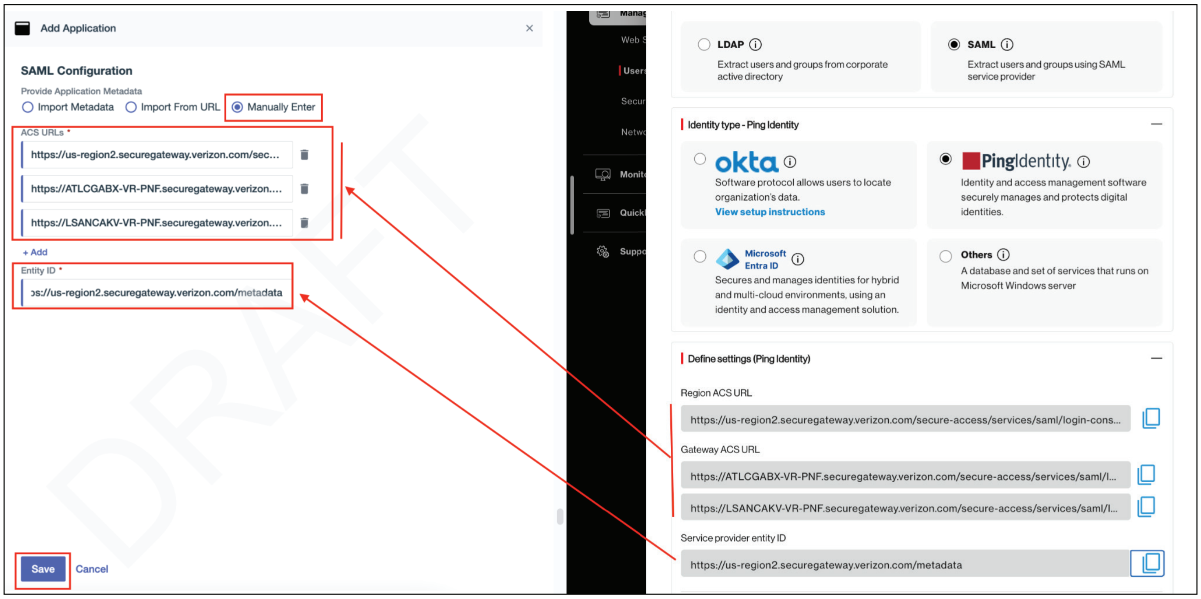
○ PingIdentity. ⓘ Identity and access management software securely manages and protects digital identities.

4 ● Microsoft Entra ID ⓘ Secures and manages identities for hybrid and multi-cloud environments, using an identity and access management solution.

○ Others ⓘ A database and set of services that runs on Microsoft Windows server

Privacy policy | Terms and conditions | © 2025 Verizon

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.



Add Application

SAML Configuration

Provide Application Metadata

○ Import Metadata ○ Import From URL ● Manually Enter

ACS URLs *

https://us-region2.securegateway.verizon.com/sec...

https://ATLCGABX-VR-PNF.securegateway.verizon....

https://LSANCAKV-VR-PNF.securegateway.verizon....

+ Add

Entity ID *

ɔs://us-region2.securegateway.verizon.com/metadata

Save Cancel

○ LDAP ⓘ Extract users and groups from corporate active directory

● SAML ⓘ Extract users and groups using SAML service provider

Identity type - Ping Identity

○ okta ⓘ Software protocol allows users to locate organization's data. View setup instructions

● PingIdentity. ⓘ Identity and access management software securely manages and protects digital identities.

○ Microsoft Entra ID ⓘ Secures and manages identities for hybrid and multi-cloud environments, using an identity and access management solution.

○ Others ⓘ A database and set of services that runs on Microsoft Windows server

Define settings (Ping Identity)

Region ACS URL

https://us-region2.securegateway.verizon.com/secure-access/services/saml/login-cons...

Gateway ACS URL

https://ATLCGABX-VR-PNF.securegateway.verizon.com/secure-access/services/saml/l...

https://LSANCAKV-VR-PNF.securegateway.verizon.com/secure-access/services/saml/l...

Service provider entity ID

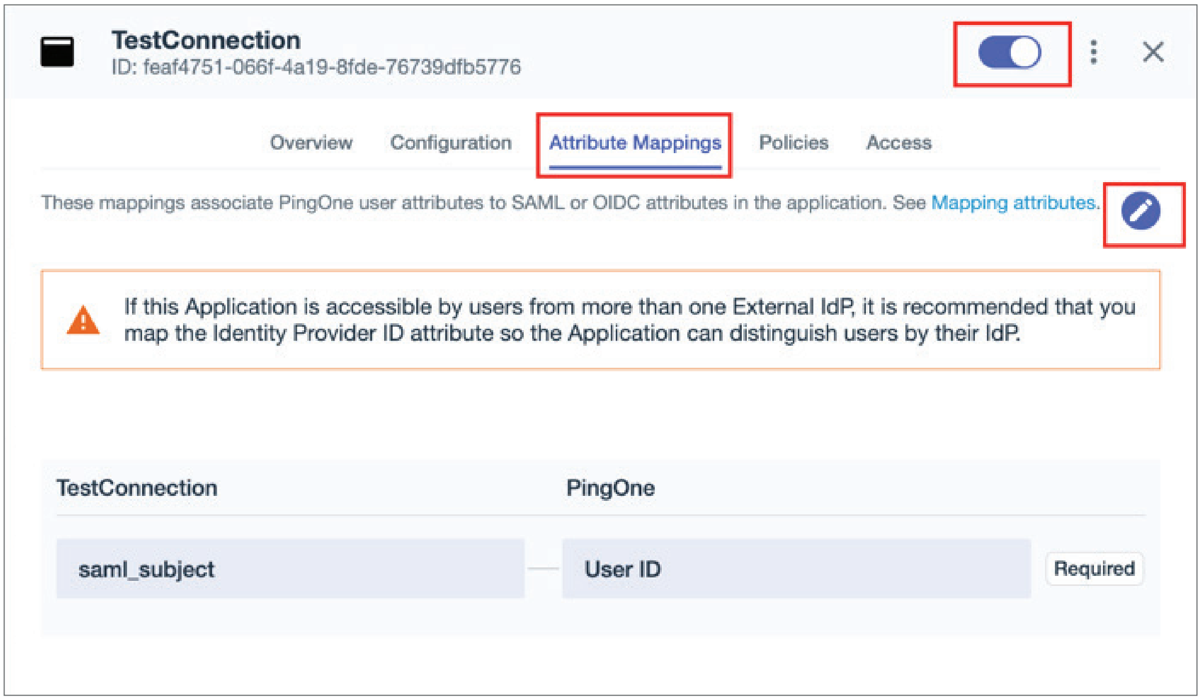
https://us-region2.securegateway.verizon.com/metadata

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

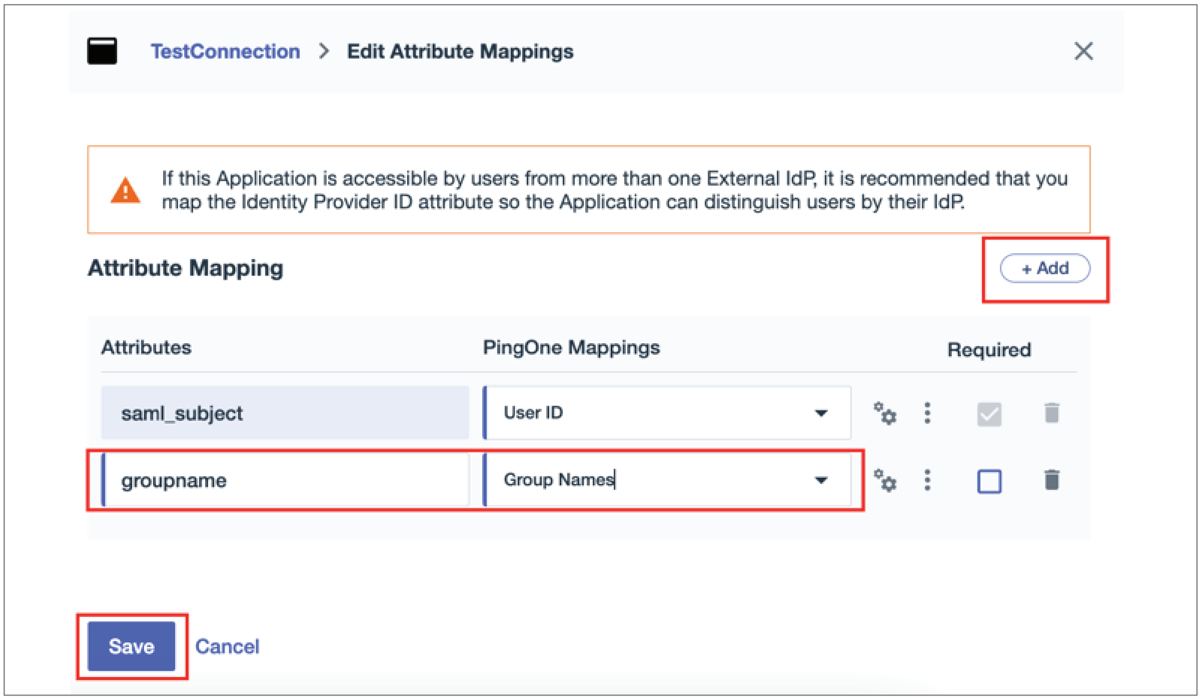


These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See Mapping attributes.

If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

TestConnection	PingOne	
saml_subject	User ID	Required

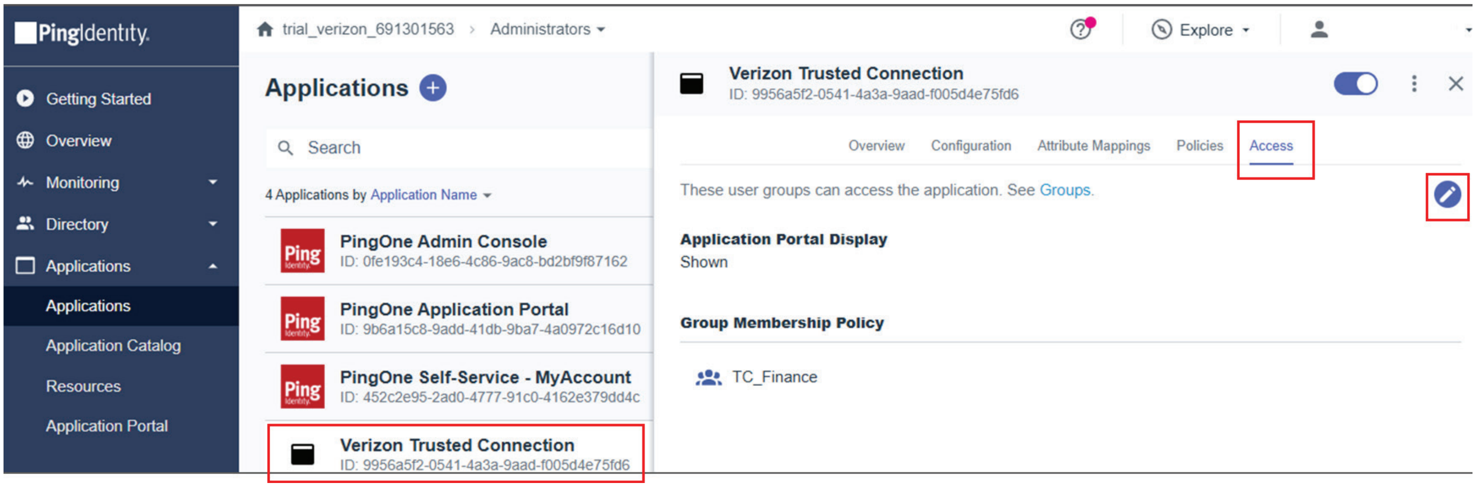
Step 5: Click on **"+Add"** as shown below and enter Attribute name as **groupname** and select **"Group Names"** from PingOne Mappings drop down. Click **"Save"**.



If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

Attributes	PingOne Mappings	Required
saml_subject	User ID	☑
groupname	Group Names	□

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



PingIdentity.

trial_verizon_691301563 › Administrators

Explore

- Getting Started
- Overview
- Monitoring
- Directory
- Applications
  - Applications
  - Application Catalog
  - Resources
  - Application Portal

Applications

Search

4 Applications by Application Name

PingOne Admin Console
ID: 0fe193c4-18e6-4c86-9ac8-bd2bf9f87162

PingOne Application Portal
ID: 9b6a15c8-9add-41db-9ba7-4a0972c16d10

PingOne Self-Service - MyAccount
ID: 452c2e95-2ad0-4777-91c0-4162e379dd4c

Verizon Trusted Connection
ID: 9956a5f2-0541-4a3a-9aad-f005d4e75fd6

Verizon Trusted Connection
ID: 9956a5f2-0541-4a3a-9aad-f005d4e75fd6

Overview | Configuration | Attribute Mappings | Policies | Access

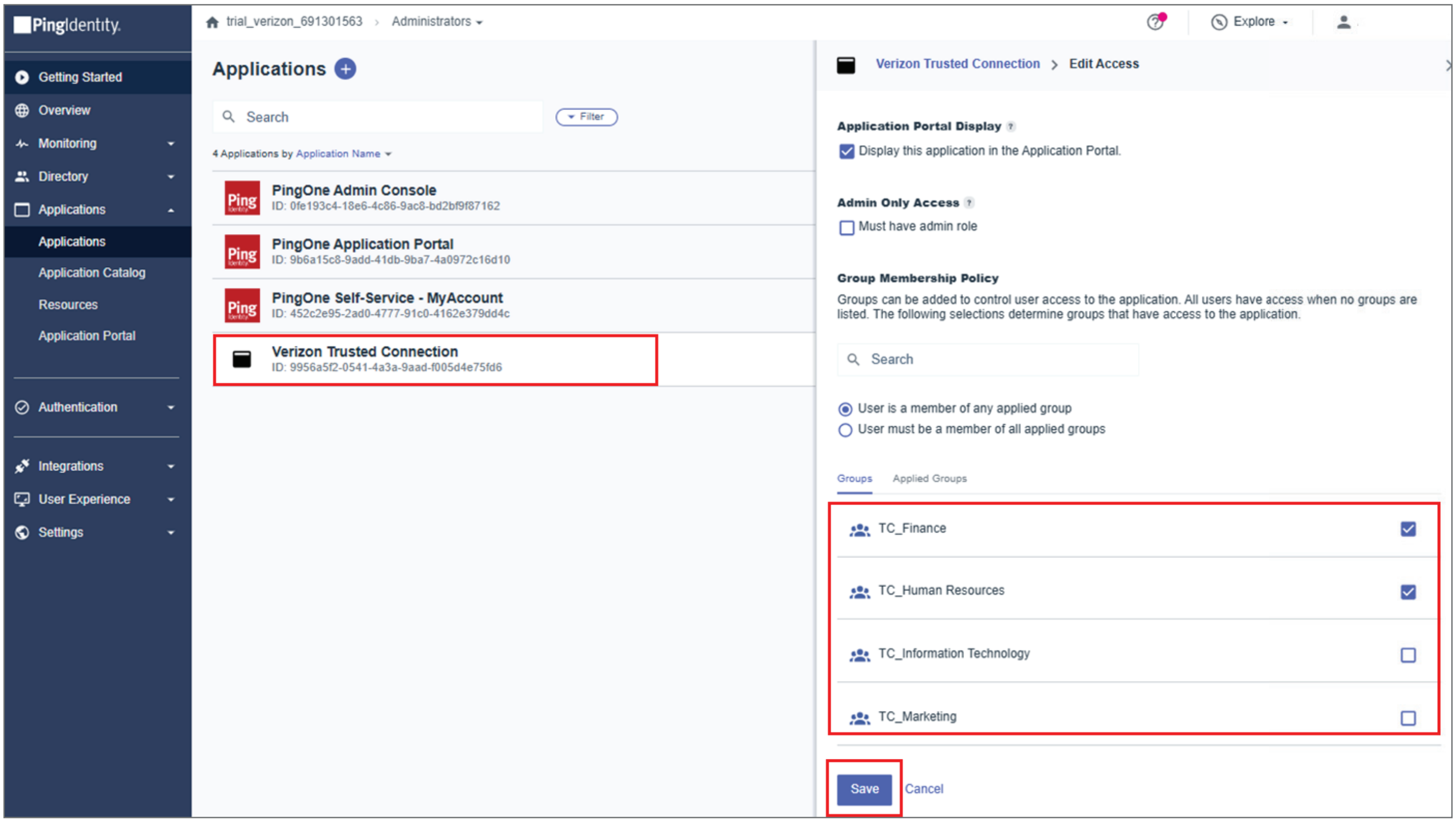
These user groups can access the application. See Groups.

Application Portal Display
Shown

Group Membership Policy

TC_Finance

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



PingIdentity.

trial_verizon_691301563 › Administrators

Explore

- Getting Started
- Overview
- Monitoring
- Directory
- Applications
  - Applications
  - Application Catalog
  - Resources
  - Application Portal
- Authentication
- Integrations
- User Experience
- Settings

Applications

Search | Filter

4 Applications by Application Name

PingOne Admin Console
ID: 0fe193c4-18e6-4c86-9ac8-bd2bf9f87162

PingOne Application Portal
ID: 9b6a15c8-9add-41db-9ba7-4a0972c16d10

PingOne Self-Service - MyAccount
ID: 452c2e95-2ad0-4777-91c0-4162e379dd4c

Verizon Trusted Connection
ID: 9956a5f2-0541-4a3a-9aad-f005d4e75fd6

Verizon Trusted Connection › Edit Access

Application Portal Display ?
☑ Display this application in the Application Portal.

Admin Only Access ?
□ Must have admin role

Group Membership Policy
Groups can be added to control user access to the application. All users have access when no groups are listed. The following selections determine groups that have access to the application.

Search

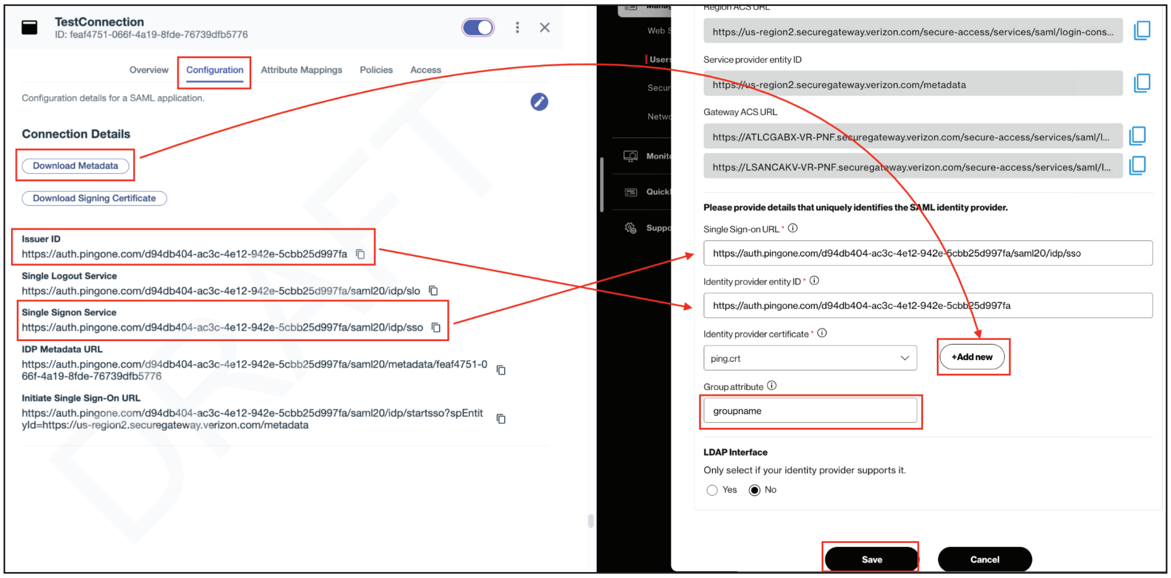
● User is a member of any applied group
○ User must be a member of all applied groups

Groups | Applied Groups

TC_Finance	☑
TC_Human Resources	☑
TC_Information Technology	□
TC_Marketing	□

Save | Cancel

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.



TestConnection
ID: feaf4751-066f-4a19-8fde-76739dfb5776

Configuration details for a SAML application.

Connection Details

Issuer ID
https://auth.pingone.com/d94db404-ac3c-4e12-942e-5cbb25d997fa

Single Logout Service
https://auth.pingone.com/d94db404-ac3c-4e12-942e-5cbb25d997fa/saml20/idp/slo

Single Signon Service
https://auth.pingone.com/d94db404-ac3c-4e12-942e-5cbb25d997fa/saml20/idp/sso

IDP Metadata URL
https://auth.pingone.com/d94db404-ac3c-4e12-942e-5cbb25d997fa/saml20/metadata/feaf4751-066f-4a19-8fde-76739dfb5776

Initiate Single Sign-On URL
https://auth.pingone.com/d94db404-ac3c-4e12-942e-5cbb25d997fa/saml20/idp/startsso?spEntityId=https://us-region2.securegateway.verizon.com/metadata

Region ACS URL
https://us-region2.securegateway.verizon.com/secure-access/services/saml/login-cons...

Service provider entity ID
https://us-region2.securegateway.verizon.com/metadata

Gateway ACS URL
https://ATLCGABX-VR-PNF.securegateway.verizon.com/secure-access/services/saml/l...
https://LSANCAKV-VR-PNF.securegateway.verizon.com/secure-access/services/saml/l...

Please provide details that uniquely identifies the SAML identity provider.

Single Sign-on URL *
https://auth.pingone.com/d94db404-ac3c-4e12-942e-5cbb25d997fa/saml20/idp/sso

Identity provider entity ID *
https://auth.pingone.com/d94db404-ac3c-4e12-942e-5cbb25d997fa

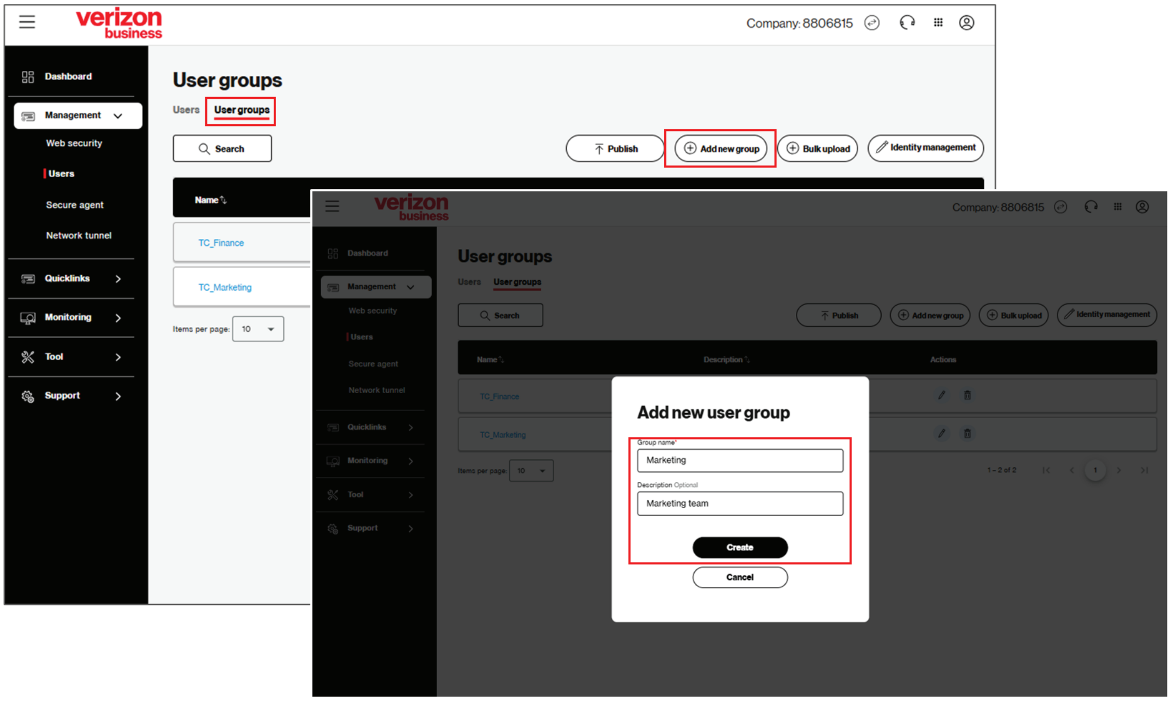
Identity provider certificate *
ping.crt

Group attribute
groupname

LDAP Interface
Only select if your identity provider supports it.
○ Yes ● No

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.



User groups

TC_Finance
TC_Marketing

Items per page: 10

1 – 2 of 2

Add new user group

Group name*
Marketing

Description Optional
Marketing team

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.

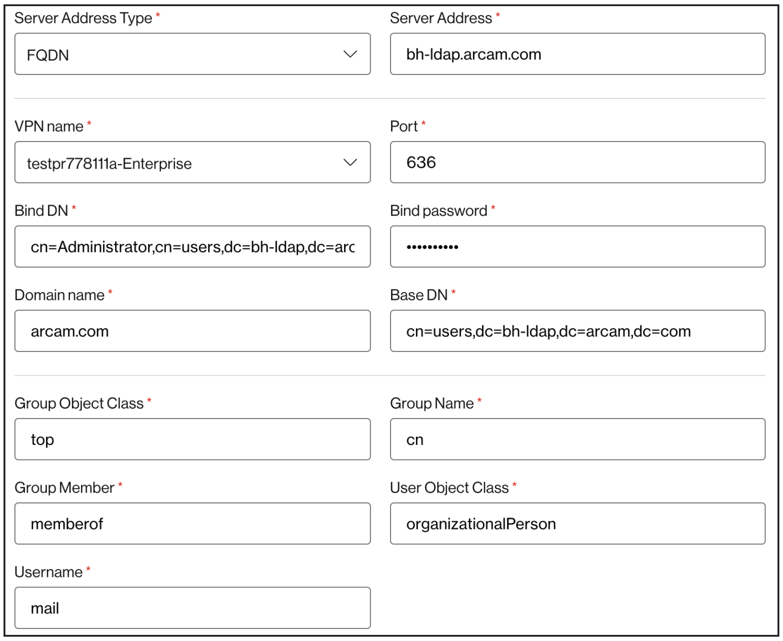
Step 1: Make sure the LDAP is open on port 636.

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:

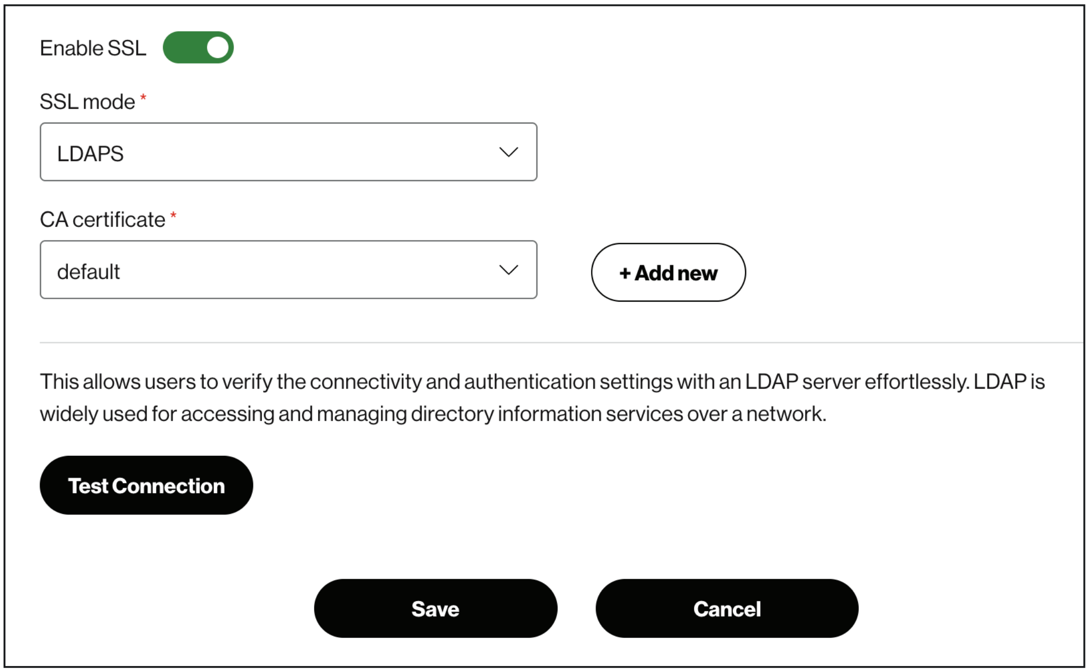
- Bind DN: **cn=Admin,cn=user,dc=ldapsecure,dc=example,dc=com** admin password should match the same in LDAP.
- Domain name: example.com
- Base DN:dc=example,dc=com
- Group Object Class: top
- Group Name: cn
- Group Member: memberOf
- User Object Class: organizationalPerson
- Username: mail/uid (similar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



Server Address Type *	FQDN	Server Address *	bh-ldap.arcam.com
VPN name *	testpr778111a-Enterprise	Port *	636
Bind DN *	cn=Administrator,cn=users,dc=bh-ldap,dc=arc	Bind password *	••••••••••
Domain name *	arcam.com	Base DN *	cn=users,dc=bh-ldap,dc=arcam,dc=com
Group Object Class *	top	Group Name *	cn
Group Member *	memberof	User Object Class *	organizationalPerson
Username *	mail		

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.



Enable SSL

SSL mode *

LDAPS

CA certificate *

default

This allows users to verify the connectivity and authentication settings with an LDAP server effortlessly. LDAP is widely used for accessing and managing directory information services over a network.

Appendix

LDAP and SAML explained

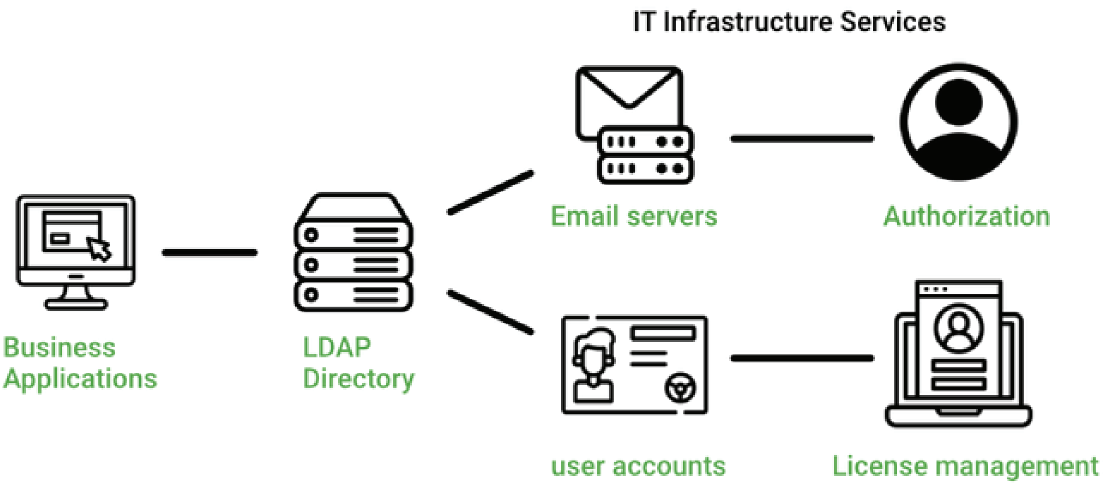
Trusted Connection leverages an organization's own Identity Management Platform (IDM). These systems typically use SAML and LDAP for their authentication protocols, as they are commonly used protocols for the access control and management of large groups of users. Each of these protocols serve somewhat 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

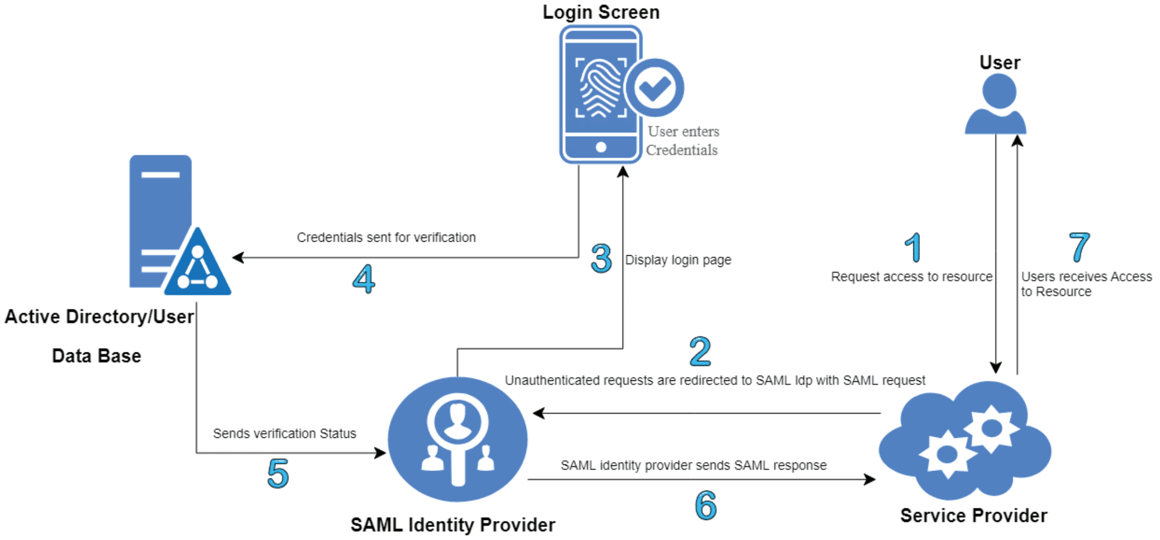


Security Assertion Markup Language (SAML)*

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


Login Screen
User enters Credentials
User
Active Directory/User Data Base
Credentials sent for verification
4
3
Display login page
1
Request access to resource
7
Users receives Access to Resource
2
Unauthenticated requests are redirected to SAML Idp with SAML request
Sends verification Status
5
SAML identity provider sends SAML response
6
SAML Identity Provider
Service Provider

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.