

Trusted Connection Guide

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



Contents

Introduction.....3

Document purpose.....3

Use cases.....3

Directions for Integrating IDM applications.....4

Microsoft EntraID integration for SAML authentication.....5

Okta integration for SAML authentication.....12

Okta LDAP interface configuration18

Ping integration for SAML authentication.....26

Windows AD/OpenLDAP integration for LDAP authentication.....30

Appendix.....36

LDAP and SAML explained.....36

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 IDs that support both the Security Assertion Markup Language (SAML) and Lightweight directory access Protocol (LDAP) authentication 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 IDs. 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)
<u>Microsoft EntraID</u>	SAML	Manual
<u>Okta</u>	SAML	Manual
<u>Okta</u>	SAML + LDAP	Automated
<u>Ping Identity</u>	SAML	Manual
<u>Windows AD/OpenLDAP</u>	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.

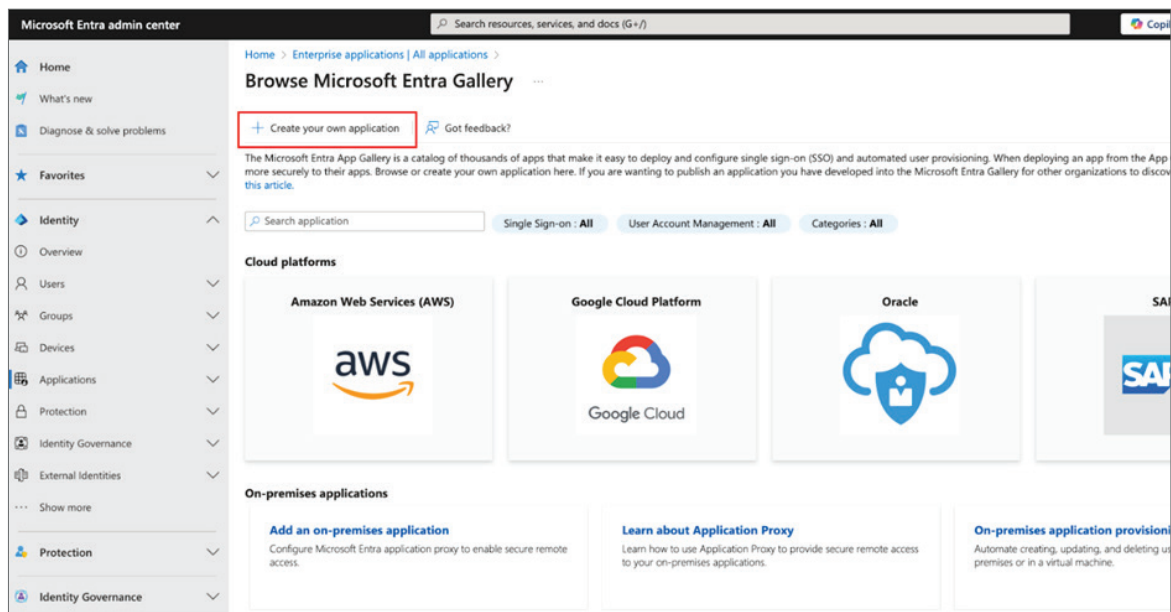
- **Trusted Connection with SAML-only:** Allows creation of Trusted Connection policies that apply to the organization as a whole and policies that target specific User Groups that have been assigned to Trusted Connection in your IDM. User Groups must be manually created within Trusted Connection to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

Create your own application

Got feedback?

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)

Create

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

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Enterprise applications

App registrations

Protection

Identity Governance

External Identities

Show more

Home > Browse Microsoft Entra Gallery > Verizon Trusted Connection

Verizon Trusted Connection | Single sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

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.

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

Test Connection | SAML-based Sign-on

Enterprise Application

Overview | Deployment Plan | Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy

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.

1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

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

Proceed

Let's add the user(s)
Please follow below steps to complete your process

1. Authentication method: **SAML** (Selected)

2. Identity type: **Microsoft Entra ID** (Selected)

3. Define settings: **Identity management** (Selected)

4. **Microsoft Entra ID** (Selected)

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

Save | Got feedback?

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.

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

Add identifier

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
1	https://RVDLILBD-VR-PNF.securegateway.verizon.com/secure-access/services/saml/login-cons...
2	https://KENUWADQ-VR-PNF.securegateway.verizon.com/secure-access/services/sa...
3	https://us-region1.securegateway.verizon.com/secure-access/services/saml/login-c...

Add reply URL

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.

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.

2

Attributes & Claims

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

Edit

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

The screenshot shows the 'Group Claims' configuration page in the Microsoft Entra admin center. On the left, under 'Attributes & Claims', the 'Add a group claim' button is highlighted with a red box. The main area shows a table of claims with columns 'Claim name', 'Type', and 'Value'. The 'Groups assigned to the application' radio button is selected. The 'Source attribute' dropdown is set to 'Cloud-only group display names' and is highlighted with a red box. The 'Save' button at the bottom right is highlighted with a red box.

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.

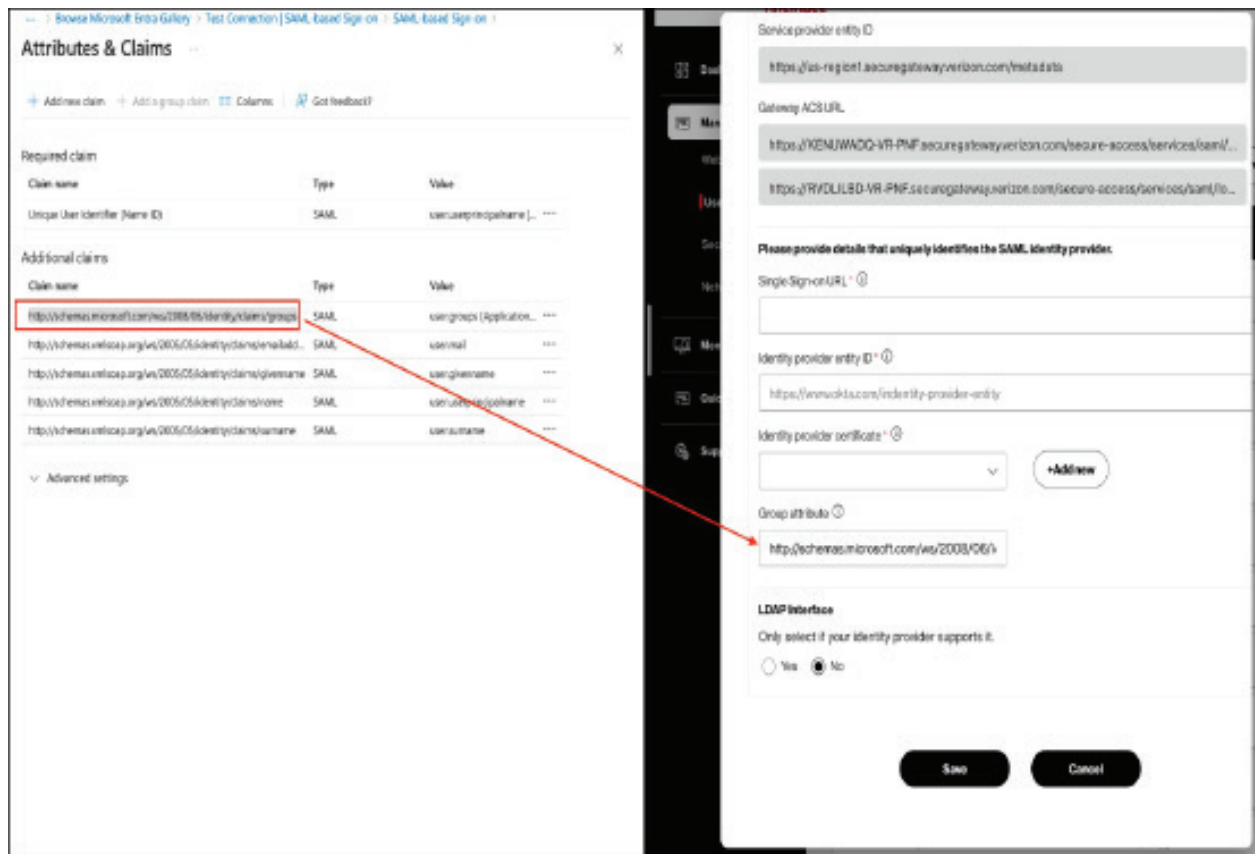
Important note

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

The screenshot shows the 'Test Connection | SAML-based Sign-on' page in the Microsoft Entra admin center. Red arrows point from the 'Download' links for 'Certificate (Base64)' and 'Microsoft Entity Identifier' to the 'Identity provider certificate' and 'Identity provider entity ID' fields in the Verizon Business 'Define settings (Entra ID)' form. The 'Identity provider entity ID' field has a note: 'Please provide details that uniquely identifies the SAML identity provider.'

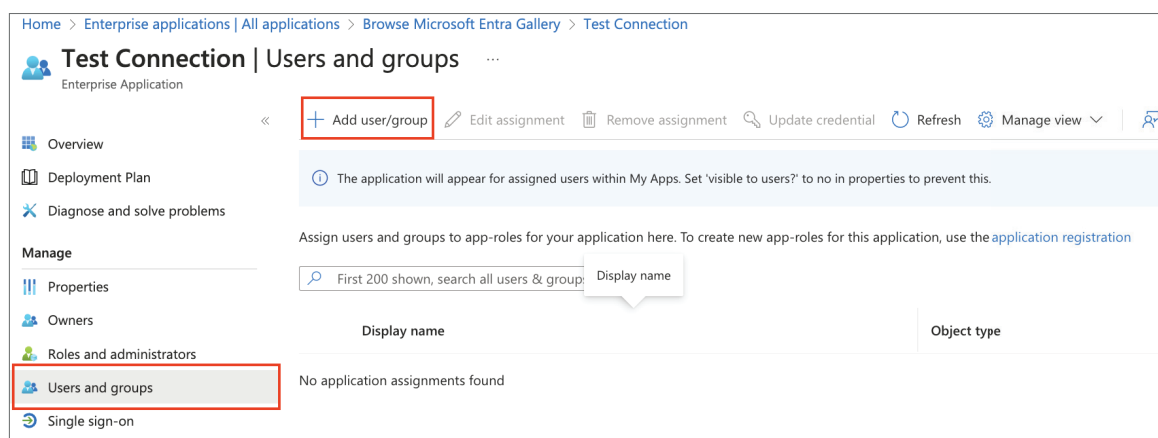
Step 10: Go back to the Attributes and Claims section from Step 7. Copy the user.groups claim name and paste it in the Trusted Connection portal's Group attribute field as shown below.

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”.

Home > Verizon Trusted Connection

Verizon Trusted Connection | Users and groups

Enterprise Application

« **+ Add user/group** Edit assignment Remove assignment Update credential ...

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

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](#)

First 200 shown, search all users & groups

Display name	Object
No application assignments found	

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

Home > Verizon Trusted Connection | Users and groups >

Add Assignment

Verizon

Users and groups

None Selected

Select a role

User

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

Search

7 results found

All	Users	Groups
☐	☐	☒
☐	☐	☒
☐	☐	☒
☐	☐	☒

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

Selected (0)

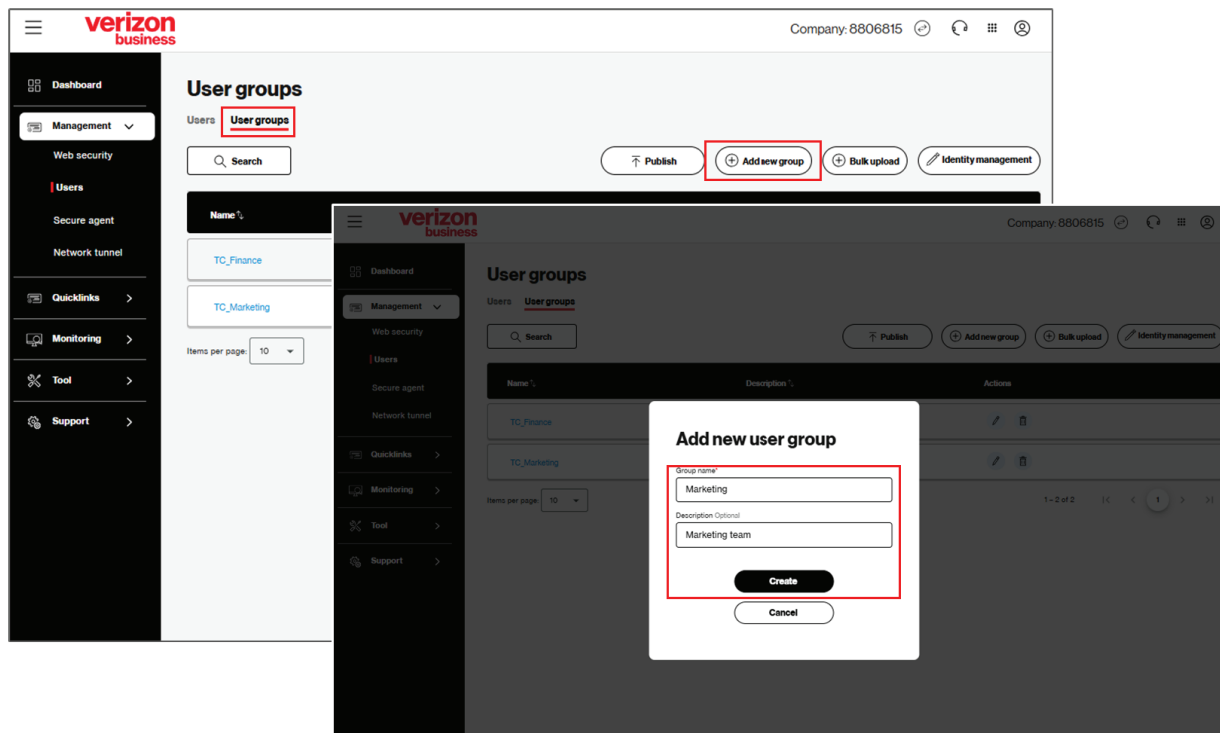
Reset

No items selected

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.

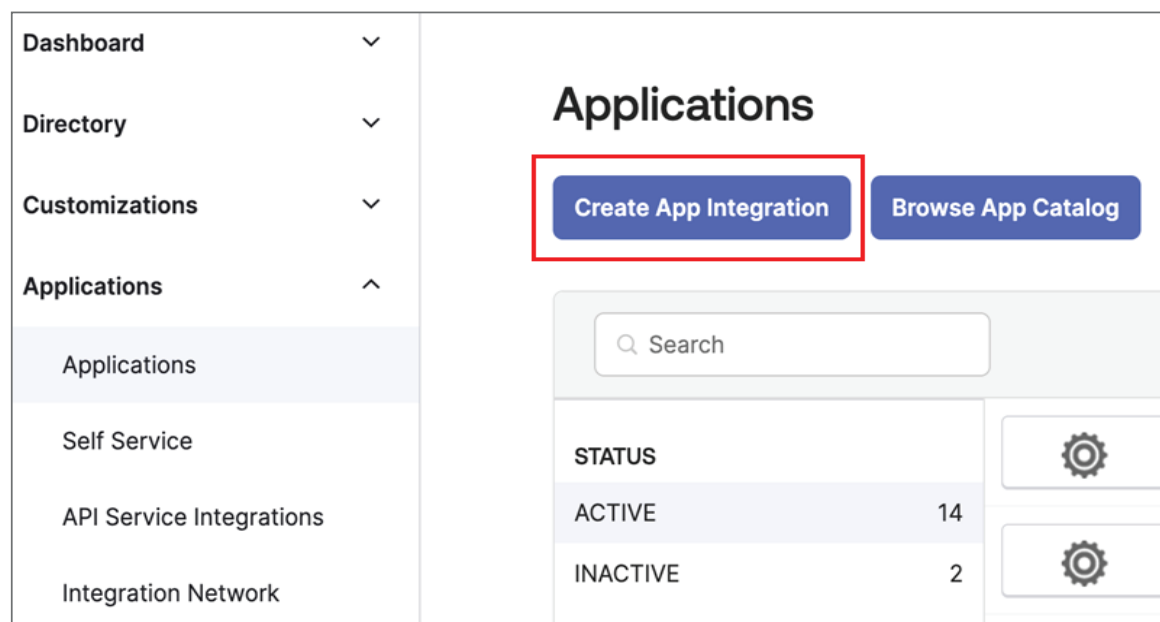


Okta Integration for SAML Authentication

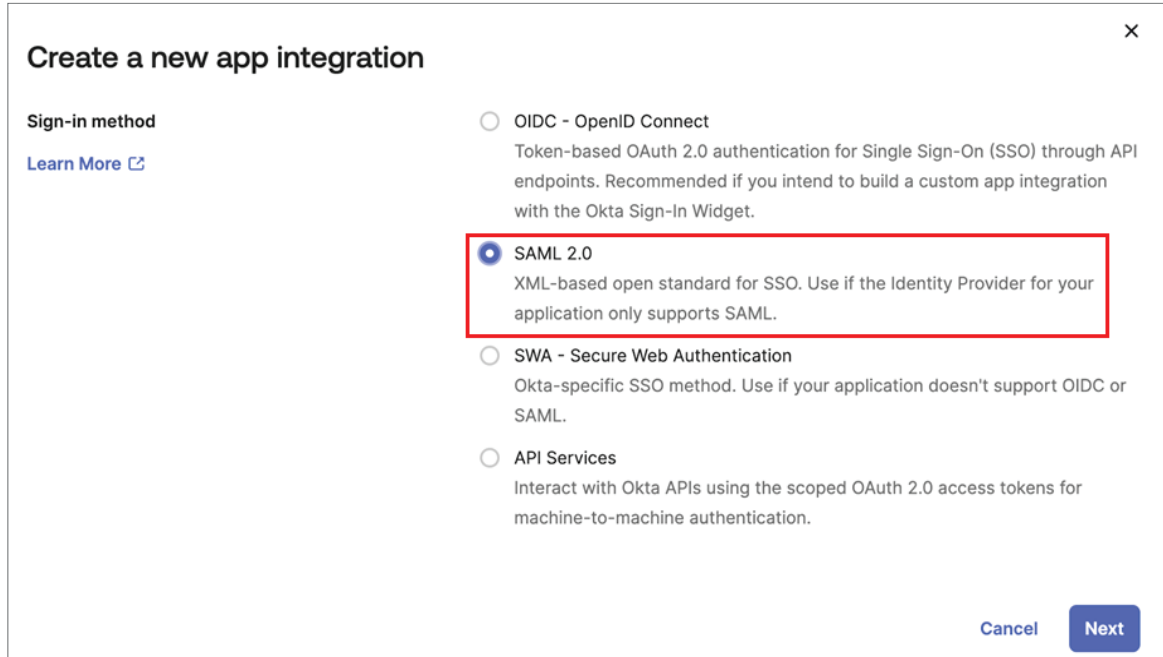
The following steps demonstrate how to integrate Trusted Connection with Okta, for SAML authentication. Instructions on how to integrate with the OKTA LDAP interface are located in the next section.

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”**.



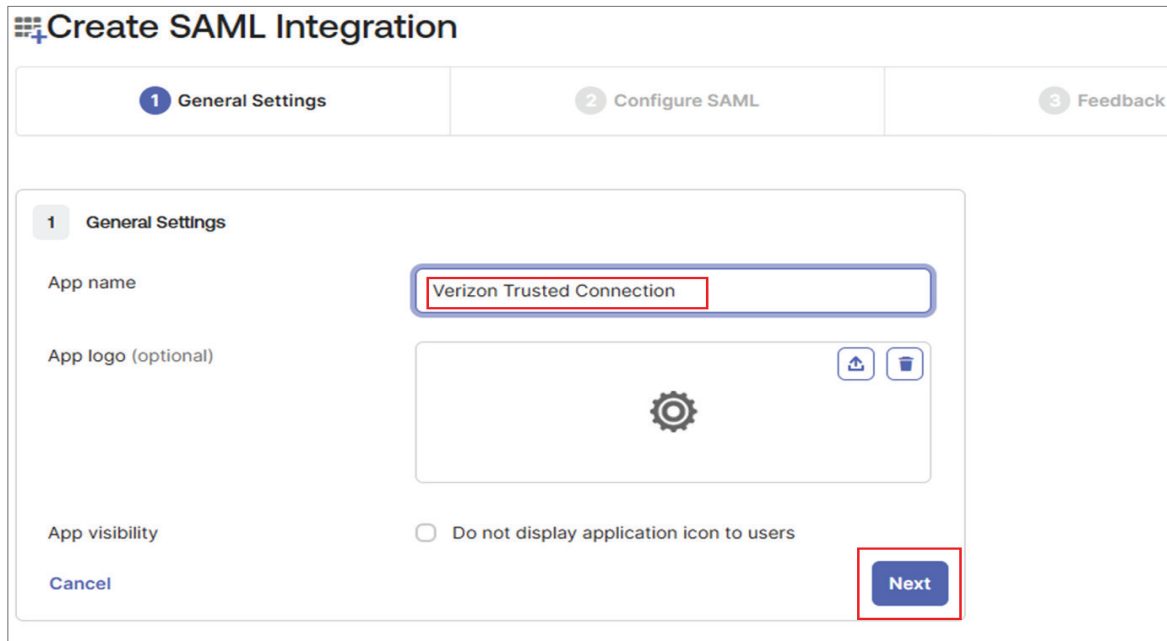
Create a new app integration ×

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.

[Cancel](#) [Next](#)

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 2 Configure SAML 3 Feedback

1 General Settings

App name

App logo (optional)   

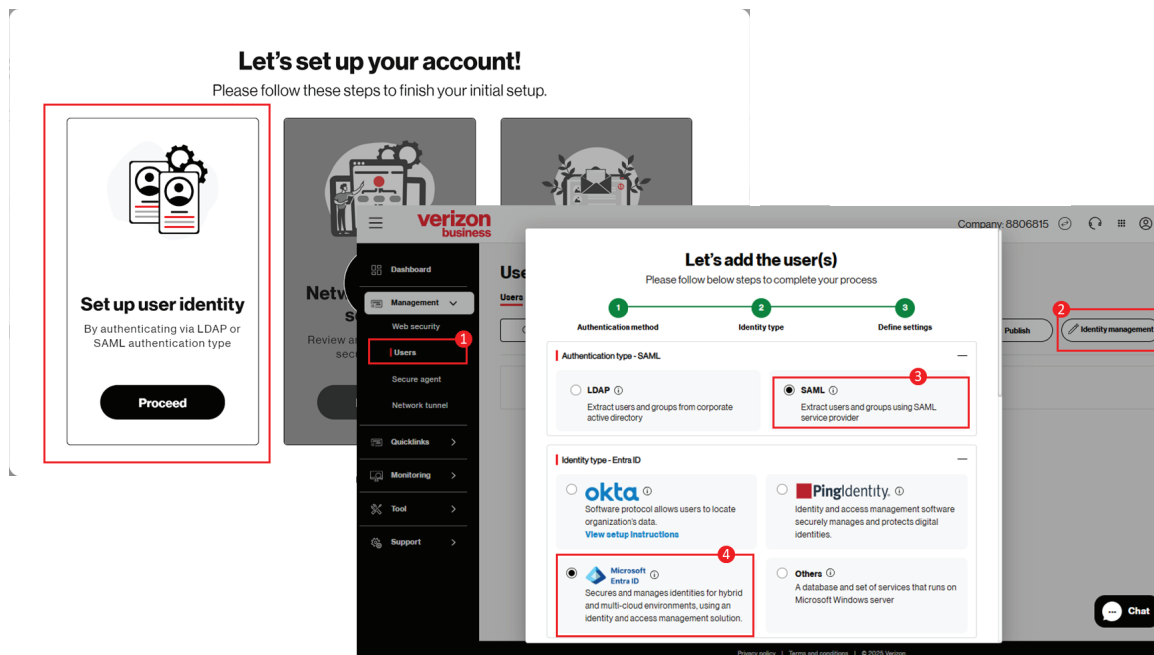
App visibility ☐ Do not display application icon to users

[Cancel](#) [Next](#)

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

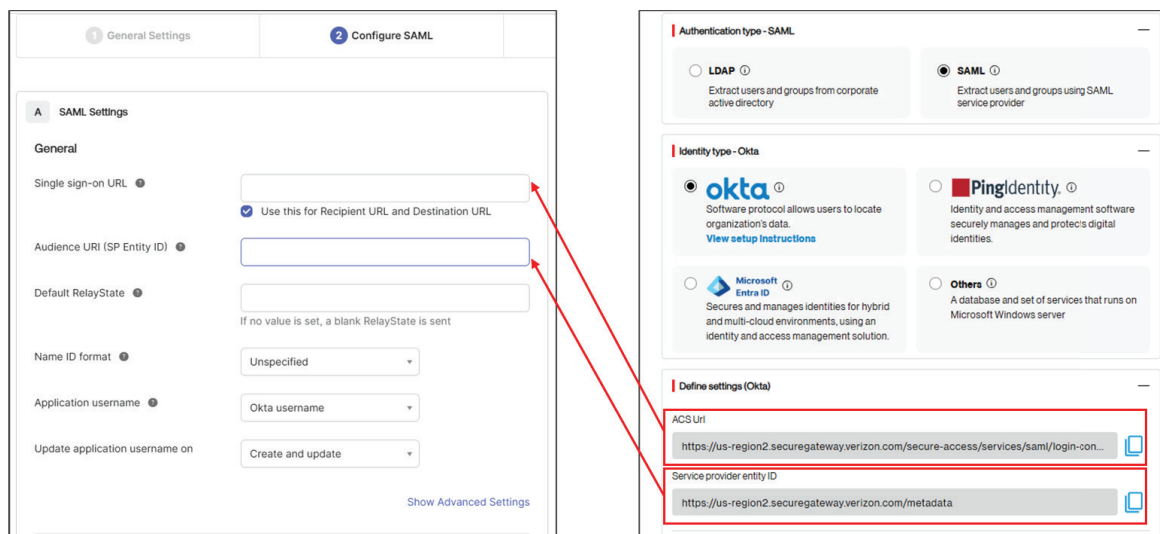
Step 4: Navigated to Set up user identity from the setup wizard or the Trusted Connection menu system as shown below:

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.

The screenshot shows two configuration panels. The left panel, titled 'Attribute Statements (optional)', contains a table with columns 'Name', 'Name format (optional)', and 'Value'. Below it is a section for 'Group Attribute Statements (optional)' with columns 'Name', 'Name format (optional)', and 'Filter'. A red box highlights the 'groupname' entry in the 'Name' column. The right panel, titled 'Identity provider certificate * ①', has a 'Group attribute ①' field with a red box around it containing the text 'groupname'. A red arrow points from the 'groupname' in the left panel to the 'groupname' in the right panel.

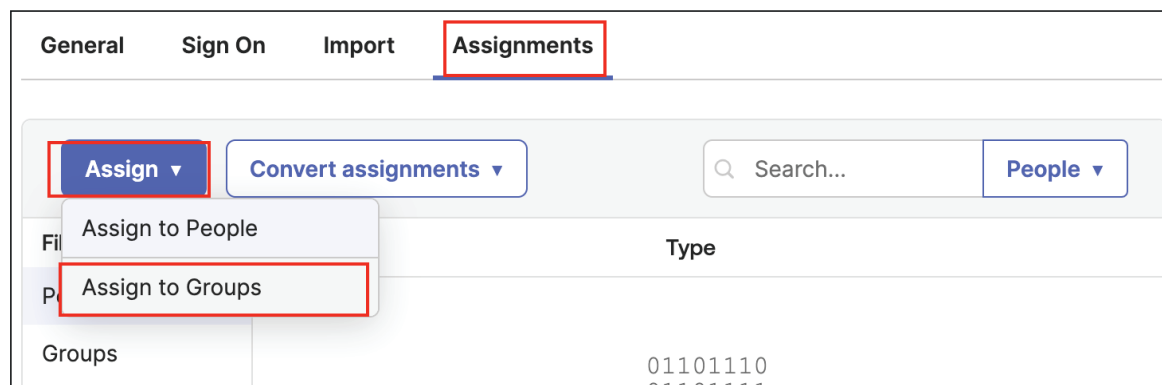
Step 7: Set the following items to their default values and click on finish. This creates an app integration in Okta

The screenshot shows a configuration screen with the following elements:

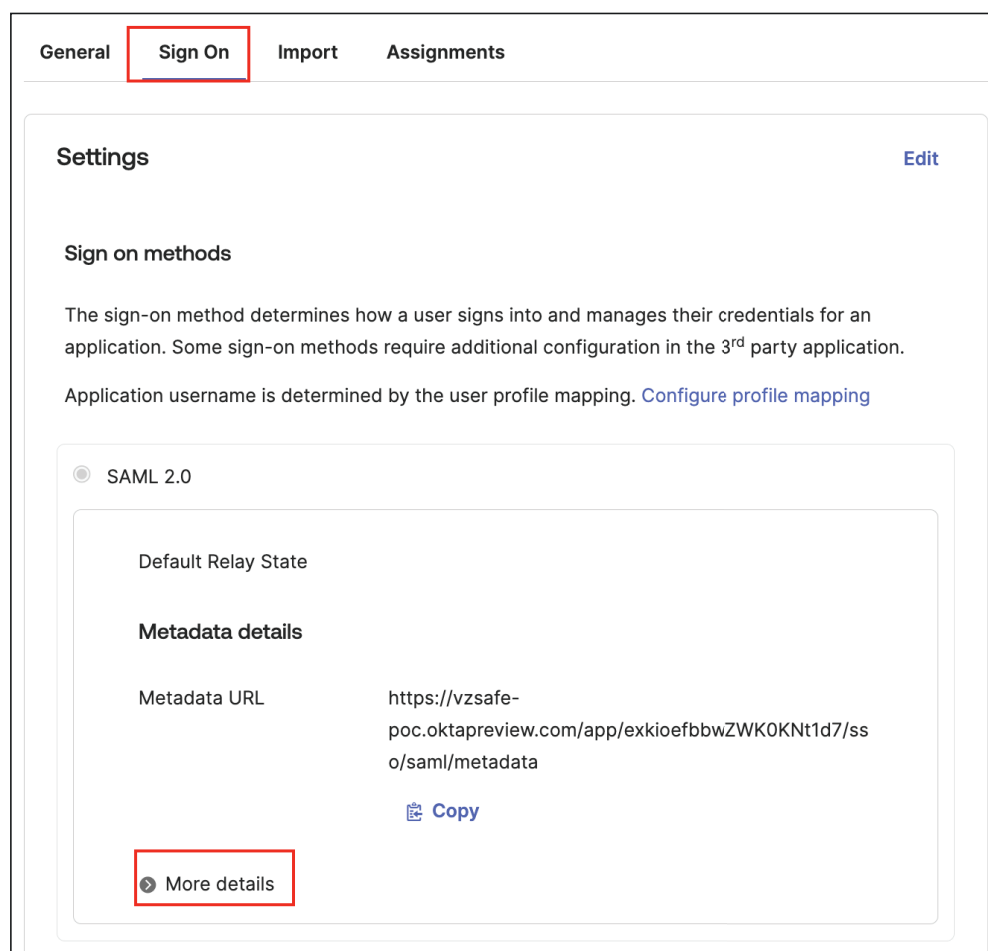
- Section header: **3 Help Okta Support understand how you configured this application**
- Question: **Are you a customer or partner?**
 - ☒ I'm an Okta customer adding an internal app (highlighted with a red box)
 - ☐ I'm a software vendor. I'd like to integrate my app with Okta
- Information box: **The optional questions below assist Okta Support in understanding your app integration.**
- Section: **App type ?**
 - ☒ This is an internal app that we have created
- Buttons: **Previous** and **Finish**

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.

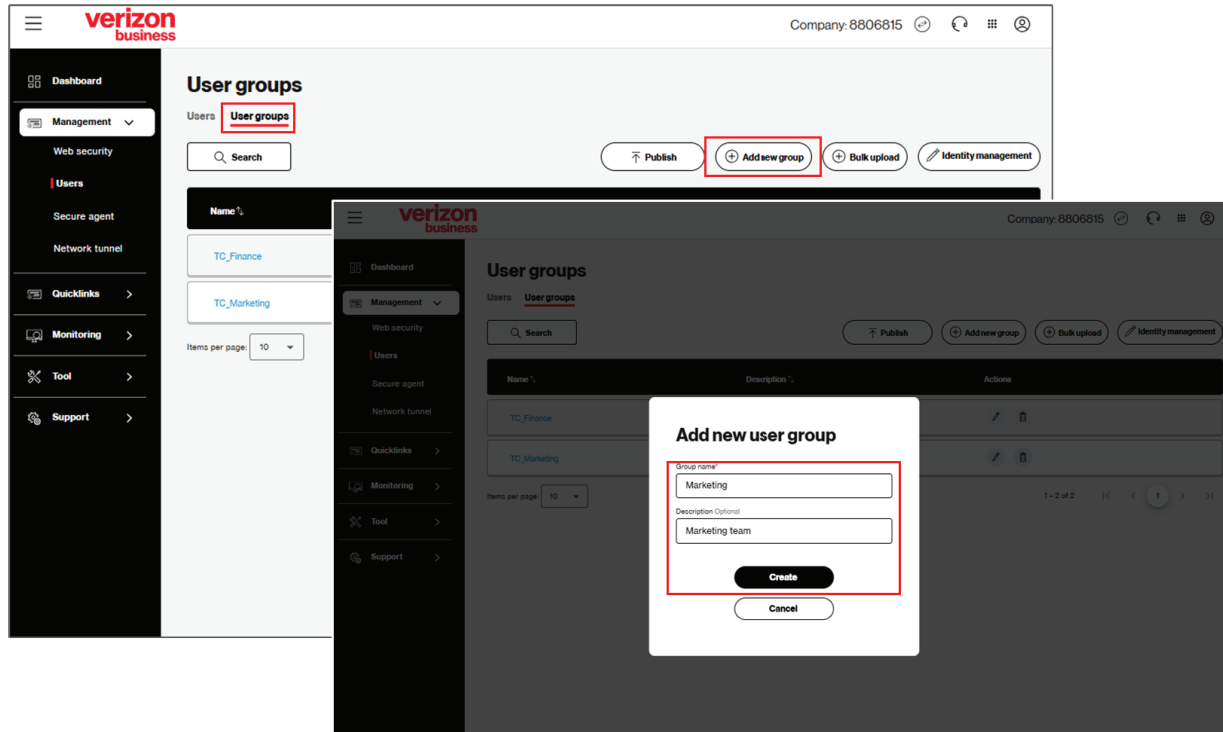
The image displays two browser tabs side-by-side, illustrating the process of configuring a Trusted Connection using Okta settings.

Okta Browser Tab (Left): The "Sign On" tab is active. Under "SAML 2.0" settings, the "Sign on URL" and "Issuer" fields are highlighted with red boxes. The "Sign on URL" is `https://trial-9254673.okta.com/app/exkixnmvuiPiPyUu697/sso/saml/metadata` and the "Issuer" is `http://www.okta.com/exkixnmvuiPiPyUu697`. Both fields have a "Copy" button. The "Signing Certificate" section shows a "Download" button.

Trusted Connection Browser Tab (Right): The "Define settings (Entra ID)" page is shown. The "Single Sign-on URL" field is populated with the URL copied from the Okta "Sign on URL" field. The "Identity provider entity ID" field is populated with the URL copied from the Okta "Issuer" field. The "Identity provider certificate" field is empty, and the "+Add new" button is highlighted with a red circle. The "LDAP Interface" section shows "Only select if your identity provider supports it." with "Yes" selected.

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

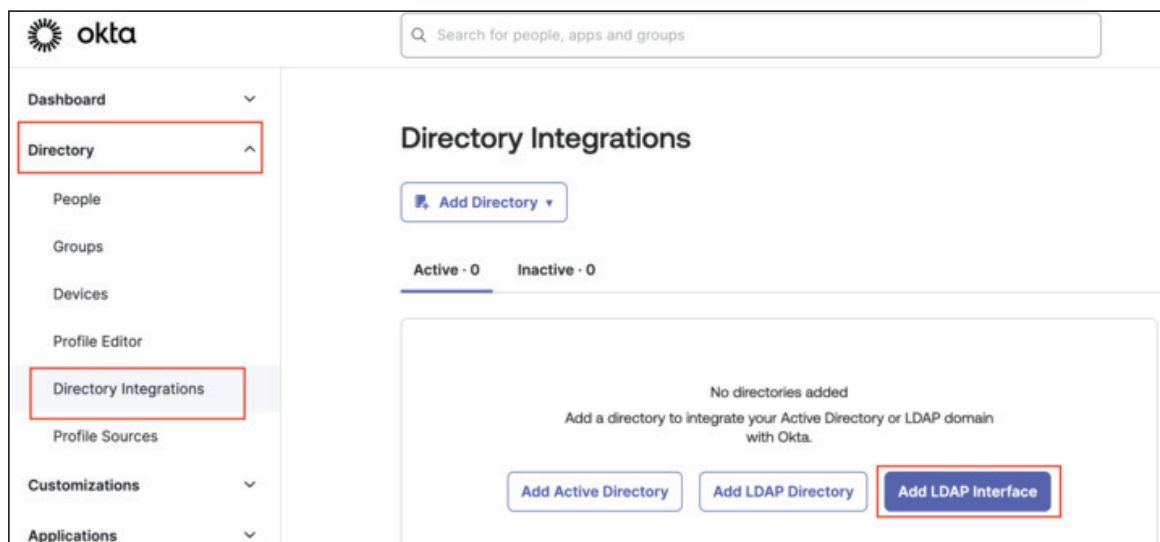
Finally, you must create User Groups in Trusted Connection that match the identical User Groups in Entra ID. Navigate the Management > Users on the left side of the screen. Select **“User Groups”** and press the **“(+) Add new group”** button to add your groups, one at a time.



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.

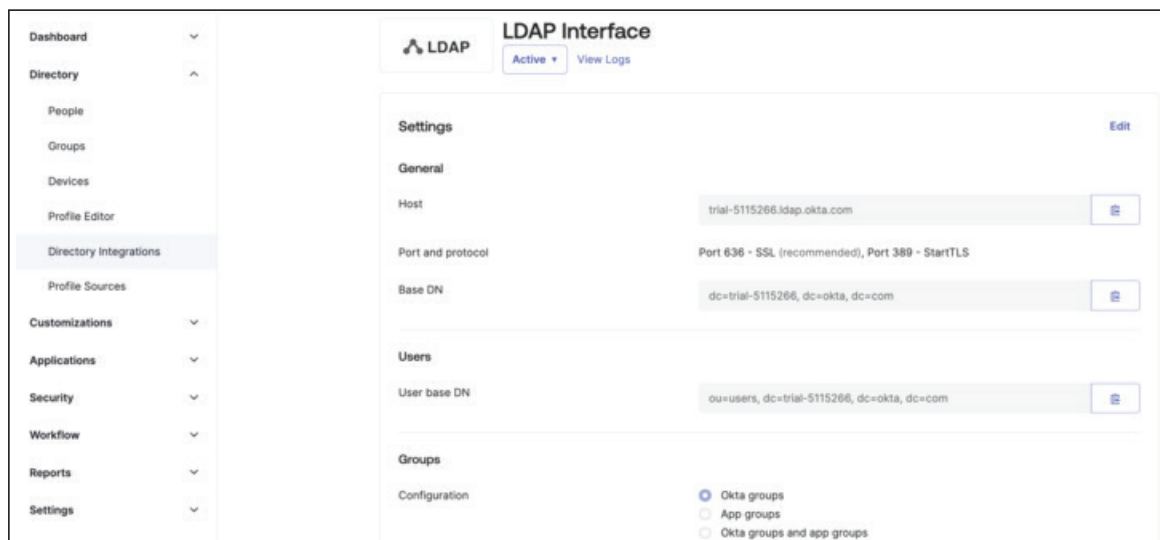
Step 1: First log into the OTKA dashboard to enable the LDAP interface of your Okta tenant by choosing Directory in the Menu on the left side of the screen. Then click on “**Directory Integrations**”, then click on “**Add LDAP Interface**”.



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

Note

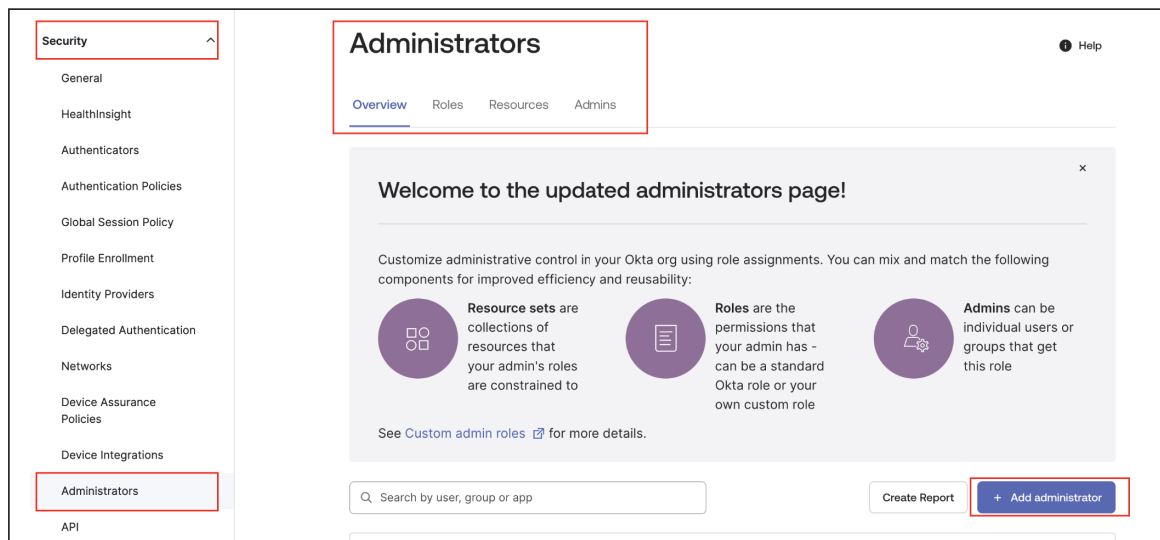
The values shown below are samples only. The actual attributes values will be different for each Okta instance.



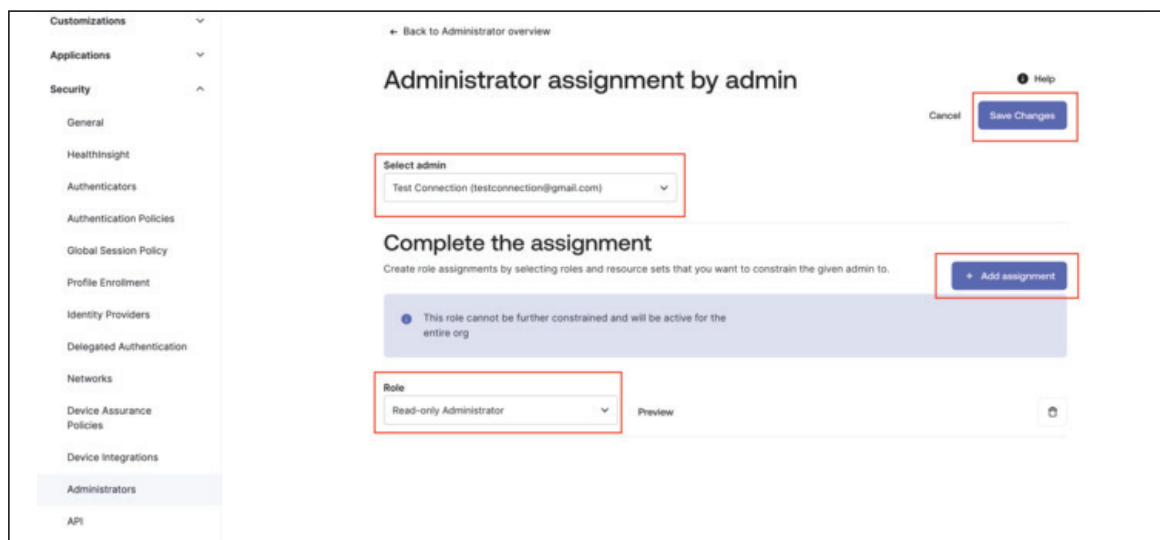
Step 3: Create a service account user for Bind authentication with minimum read-only administrator privileges.

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.

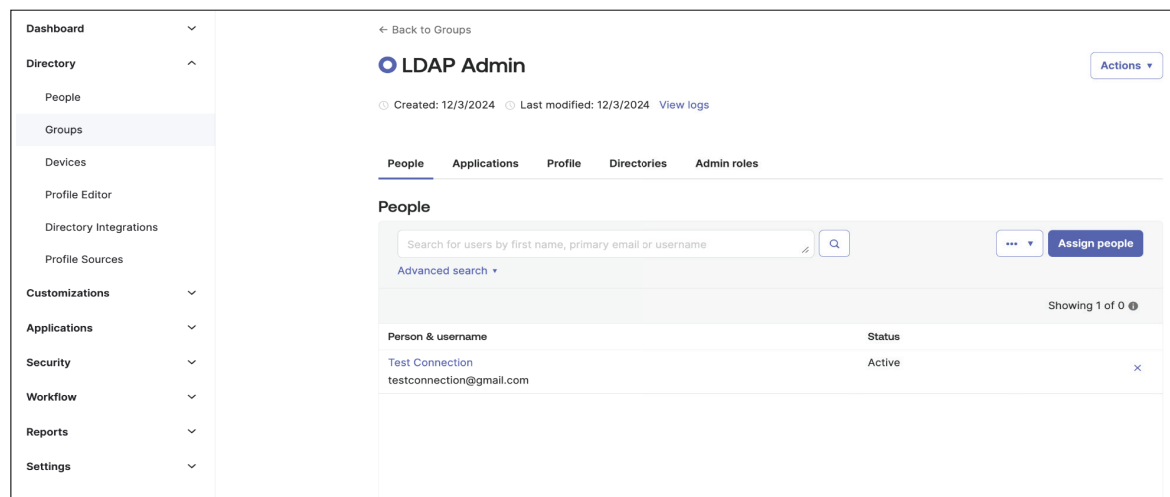
Step 3a: After the user has been created, the next step is to assign them the correct privileges to allow the proper authentication processes to work. Follow the Dropdown Menu on the left side of the screen and click on Security, then Administrators. Once in the Administrator Overview screen, Click on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

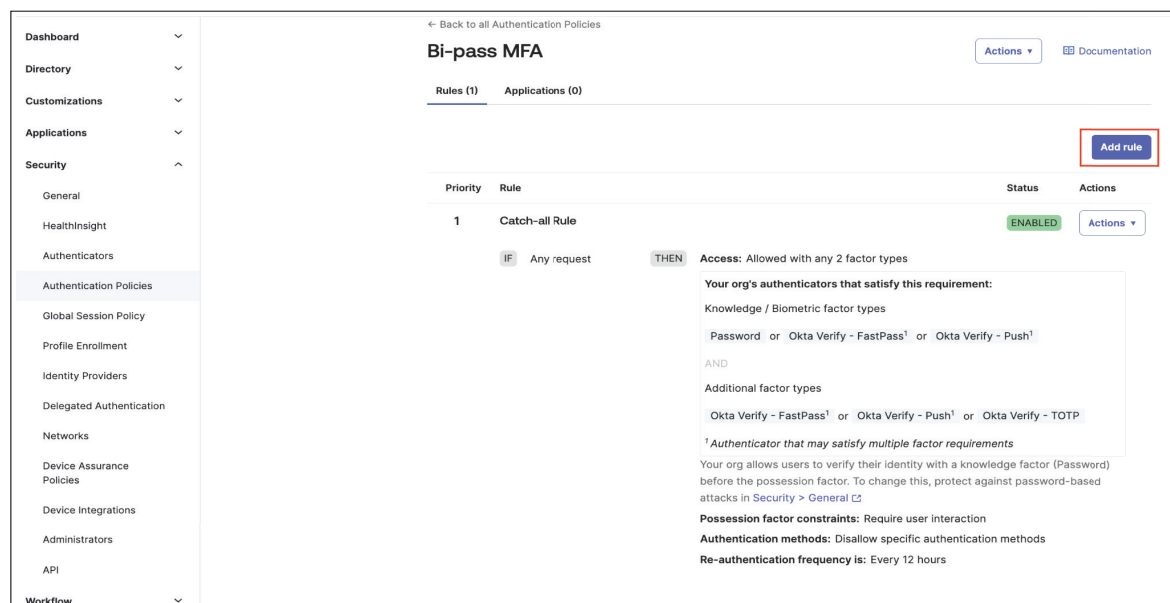


Step 4: Add the service admin account that was created in the previous steps to a specific group that will be used to set the policies to By-pass MFA and set authentication policies to authenticate using LDAP instead. This allows this special user to authenticate against the LDAP data. Once the group 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.



The screenshot shows the Okta 'LDAP Admin' page. On the left is a navigation menu with options like Dashboard, Directory, Groups, Devices, Profile Editor, Directory Integrations, Profile Sources, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'LDAP Admin' and includes a 'Back to Groups' link and an 'Actions' button. Below this, there are tabs for 'People', 'Applications', 'Profile', 'Directories', and 'Admin roles'. The 'People' tab is active, showing a search bar and an 'Assign people' button. A table below shows one user assigned: 'Test Connection' with email 'testconnection@gmail.com' and status '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”**.



The screenshot shows the Okta 'Authentication Policies' screen. The left navigation menu is expanded to 'Security' > 'Authentication Policies'. The main content area is titled 'Bi-pass MFA' and includes a 'Back to all Authentication Policies' link and 'Actions' and 'Documentation' buttons. Below this, there are tabs for 'Rules (1)' and 'Applications (0)'. The 'Rules (1)' tab is active, showing a table with one rule: 'Catch-all Rule' with priority '1' and status 'ENABLED'. The rule details are expanded, showing the 'IF' condition as 'Any request' and the 'THEN' action as 'Access: Allowed with any 2 factor types'. The rule configuration includes a list of authenticators: 'Knowledge / Biometric factor types', 'Password', 'Okta Verify - FastPass¹', and 'Okta Verify - Push¹'. It also shows 'Additional factor types' as 'Okta Verify - FastPass¹', 'Okta Verify - Push¹', and 'Okta Verify - TOTP'. A footnote explains that the rule allows users to verify their identity with a knowledge factor (Password) before the possession factor. The rule also specifies 'Possession factor constraints: Require user interaction', 'Authentication methods: Disallow specific authentication methods', and '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:

IF

IF User's user type is:

AND User's group membership includes:
☒ LDAP Admin

And none of the following groups:

[Go to Groups](#)

AND User is:

AND Device state is: ☒ Any
☐ Registered
[Setup Okta Verify as Authenticator](#)

AND Device platform is:

AND User's IP is:

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:
 Your org's authenticators that satisfy this requirement:

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 [Documentation](#)

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.

Add policy

1 Default Policy

Default Policy

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

Assigned to groups: [Everyone](#)

Add rule

Priority	Rule name	Access	Status	Actions
1	Default Rule	Allowed	Active	Info Edit

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 Authentication

Exclude users

Test Connection (testconnection@gmail.com) x

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](#)

Update rule

Cancel

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 [Documentation](#)

Setup **Enrollment**

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.

Add a policy

1 Default Policy Active [Actions](#)

Default Policy

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](#)

Add rule

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:

Exclude users:

IF: User's IP is

Manage configuration for [Networks](#)

THEN: Enrollment is

☒ Allowed if required authenticators are missing
☐ Deny enrollment of SSO authenticators
☐ Deny enrollment of all authenticators

Create rule [Cancel](#)

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@CQT9XWVJW ~ % 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 *
FQDN

Server Address *
trial-5115266.ldap.okta.com

VPN name *
testpr778382b-Enterprise

Port *
636

Bind DN *
uid=testconnection@gmail.com,dc=trial-51152

Bind password *

Domain name *
okta

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

Group Object Class *
groupofUniqueNames

Group Name *
cn

Group Member *
memberOf

User Object Class *
inetOrgPerson

Username *
uid

Enable SSL ☒

SSL mode *
LDAPS

CA certificate *
default

+ Add new

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.

Test Connection

Save

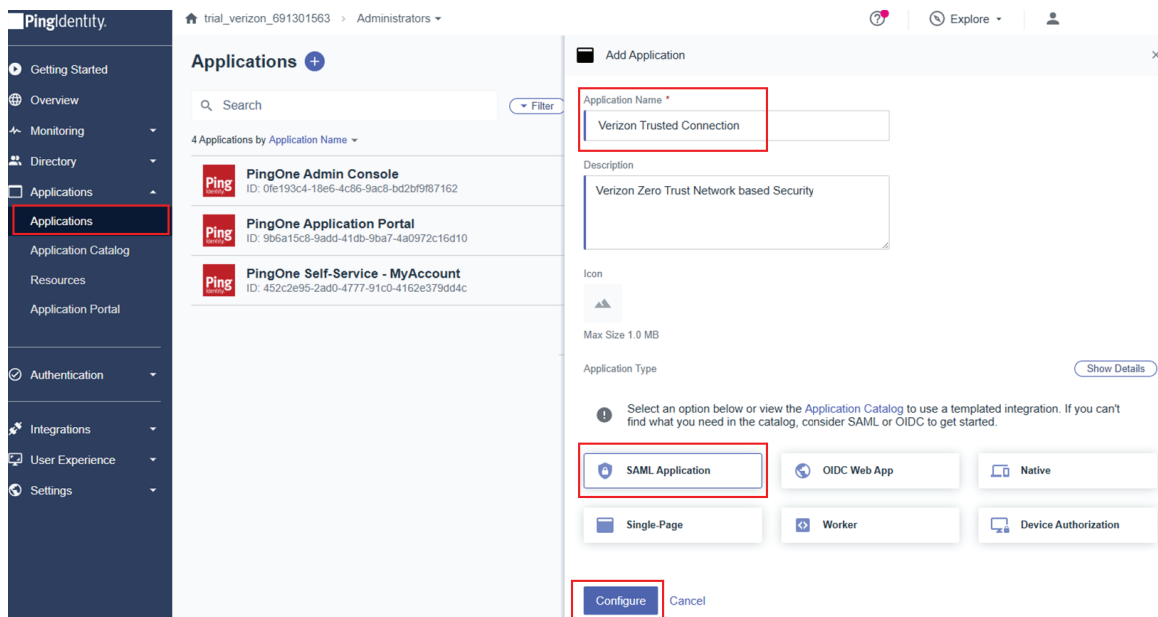
Cancel

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 portal.

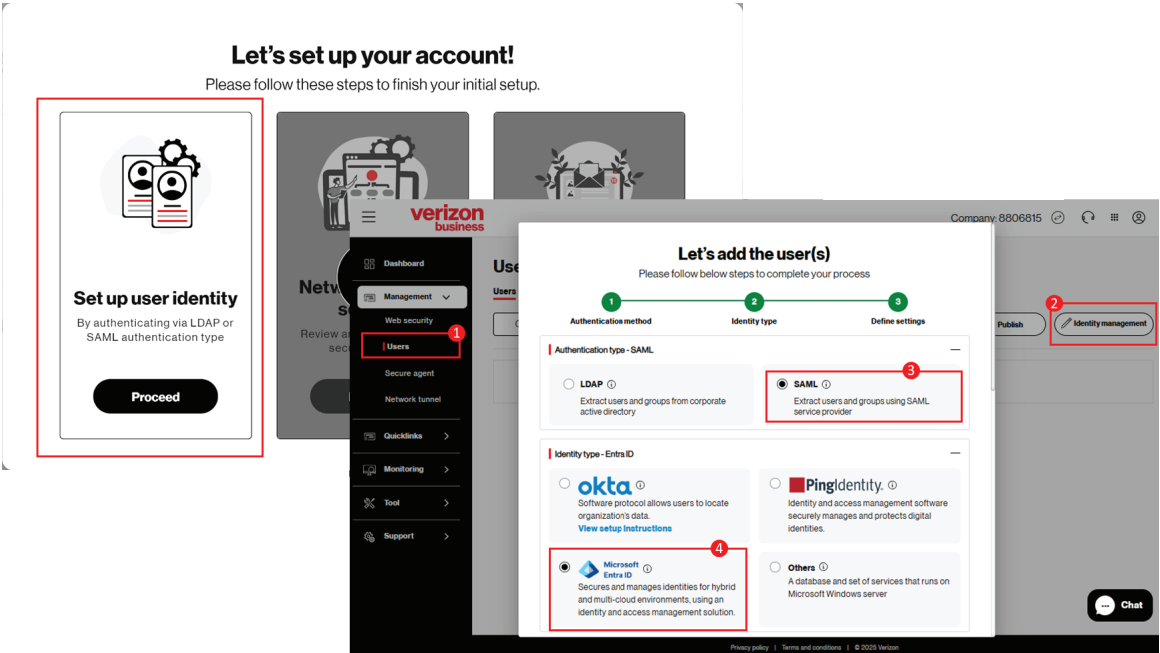
Step 1: After logging into the Ping Portal, create an application in Ping by selecting Applications, enter Application Name (as Verizon Trusted Connection), select SAML and click on **“Configure”**.



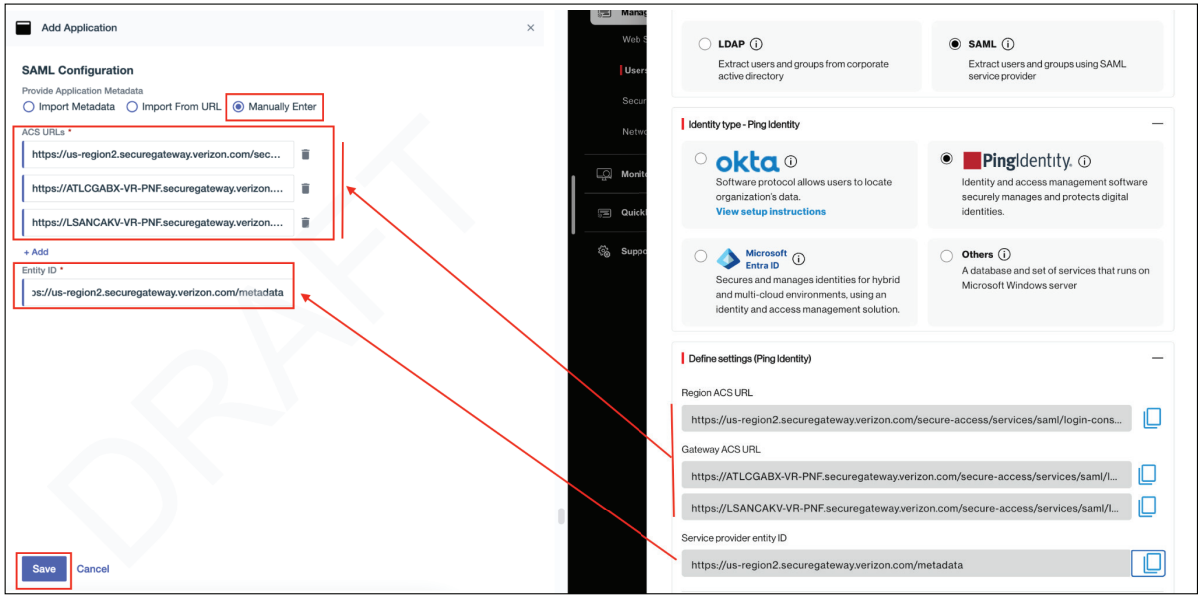
For the next step, you will need to open a browser for Trusted Connection at trustedconnection.verizon.com.

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

The screenshot shows the configuration page for an application named "TestConnection" (ID: feaf4751-066f-4a19-8fde-76739dfb5776). The "Attribute Mappings" tab is selected. A toggle switch at the top right is turned on. Below the tabs, a message states: "These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See [Mapping attributes](#)." A pencil icon is visible next to this message. A warning box contains the text: "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." Below this, a mapping is shown between "saml_subject" (TestConnection attribute) and "User ID" (PingOne attribute), marked as "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"**.

The screenshot shows the "Edit Attribute Mappings" dialog box for the "TestConnection" application. A warning message is displayed at the top. Below it, the "Attribute Mapping" section has a "+ Add" button. The mapping table is as follows:

Attributes	PingOne Mappings	Required
saml_subject	User ID	☒
groupname	Group Names	☐

The "groupname" row is highlighted with a red box. At the bottom, there are "Save" and "Cancel" buttons, with the "Save" button also highlighted by a red box.

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

The screenshot shows the PingIdentity interface. On the left is a navigation menu with 'Applications' selected. The main area displays a list of applications. 'Verizon Trusted Connection' (ID: 9956a5f2-0541-4a3a-9aad-f005d4e75fd6) is highlighted with a red box. To its right, the application details panel is open, showing the 'Access' tab (also highlighted with a red box). A pencil icon in the top right of the details panel is also highlighted with a red box.

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

The screenshot shows the 'Edit Access' page for the 'Verizon Trusted Connection' application. The 'Application Portal Display' section has a checked checkbox for 'Display this application in the Application Portal'. The 'Admin Only Access' section has an unchecked checkbox for 'Must have admin role'. The 'Group Membership Policy' section has a radio button selected for 'User is a member of any applied group'. Below this, a table lists groups to be assigned:

Groups	Applied Groups
TC_Finance	☒
TC_Human Resources	☒
TC_Information Technology	☐
TC_Marketing	☐

The 'Save' button at the bottom is highlighted with a red box.

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.

The screenshot shows the 'TestConnection' configuration page for a SAML application. The 'Configuration' tab is active. On the left, under 'Connection Details', the 'Single Signon Service' URL and 'Issuer ID' are highlighted with red boxes. Red arrows point from these boxes to the 'Single Sign-on URL' and 'Identity provider entity ID' fields on the right. The 'Identity provider certificate' field has a '+Add new' button highlighted with a red box. The 'Group attribute' field contains the value 'groupname'. The 'Save' button is also highlighted with a red box.

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.

The screenshot shows the 'User groups' management page in the Verizon Business Management console. The 'Add new group' button is highlighted with a red box. A modal dialog titled 'Add new user group' is open, showing the 'Group name' field with the value 'Marketing' and the 'Description Optional' field with the value 'Marketing team'. The 'Create' button is highlighted with a red box.

Windows AD/OpenLDAP integration for LDAP authentication

The OpenLDAP Software suite includes:

- [lload](#) - 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 *	Server Address *
FQDN	bh-ldap.arcam.com
VPN name *	Port *
testpr778111a-Enterprise	636
Bind DN *	Bind password *
cn=Administrator,cn=users,dc=bh-ldap,dc=arc	*****
Domain name *	Base DN *
arcam.com	cn=users,dc=bh-ldap,dc=arcam,dc=com
Group Object Class *	Group Name *
top	cn
Group Member *	User Object Class *
memberof	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

+ Add new

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.

Test Connection

SaveCancel

Appendix

LDAP and SAML explained

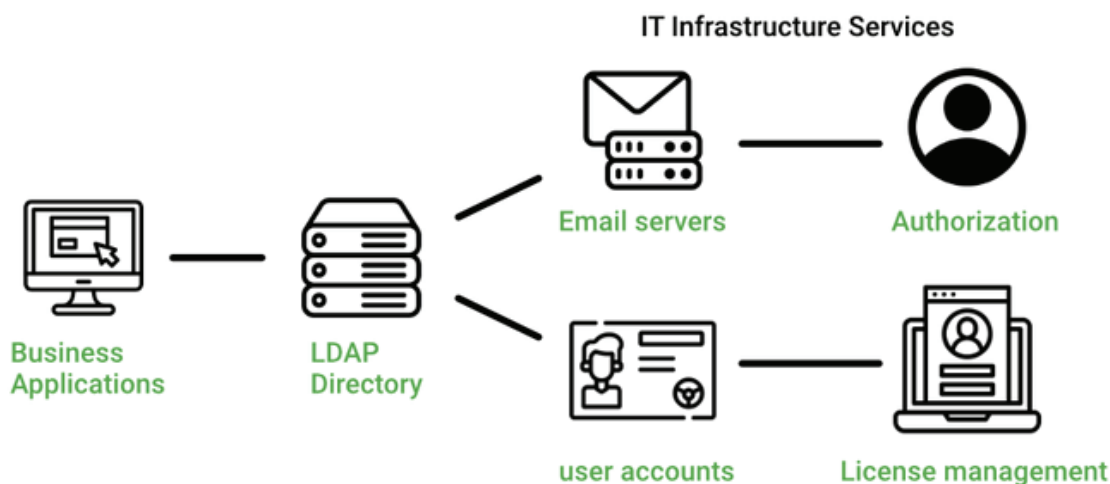
Trusted Connection leverages an organization's own Identity Management Platform (IDM). These systems typically use SAML and LDAP for their authentication protocols, as they are commonly used protocols for the access control and management of large groups of users. Each of these protocols serve somewhat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

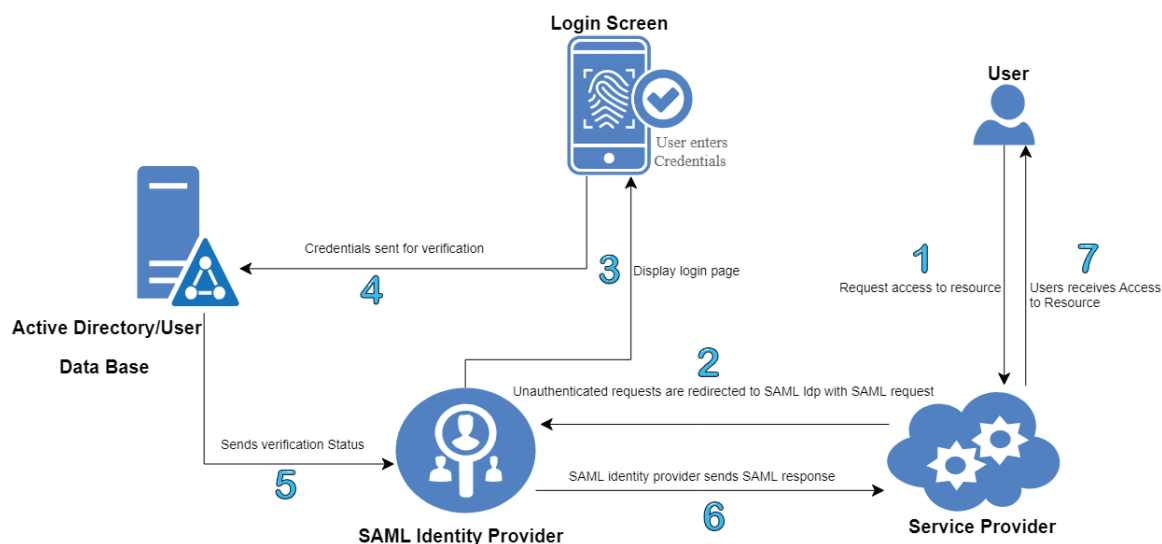


Security Assertion Markup Language (SAML)*

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.

