

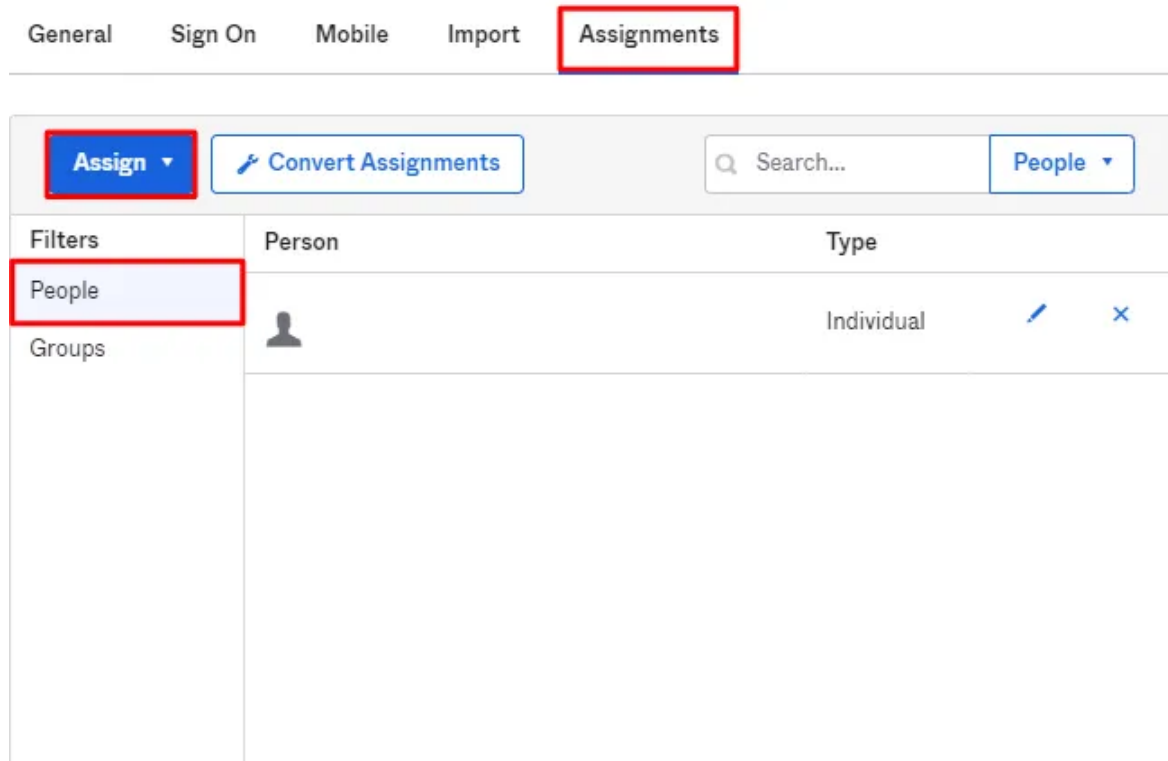
POC on jenkins authentication using okta

Issue:

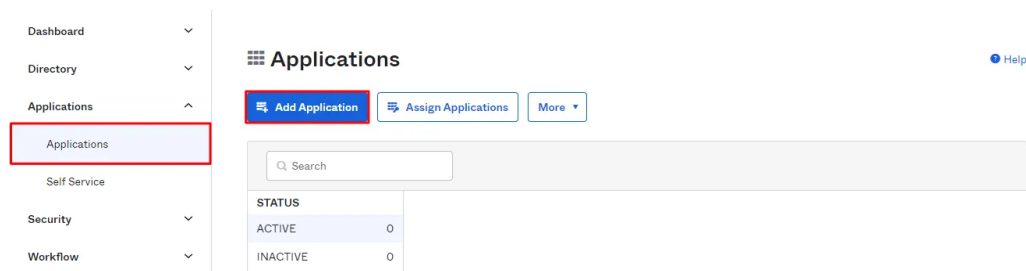
How do I setup OKTA as Identity Provider in Jenkins

Solution:

1. Download SAML plugin in jenkins.
2. Now move to the Okta and do the following setup:
 - a) Create users for the jenkins authentication
 - b) Create groups like Jenkins-admin and Jenkins-users
 - c) Assign user to the respective groups



- d) Now goto the applications and create a new application from app integration and select SAML 2.0 from it.



Create a New Application Integration

Platform

Web

Sign on method

☐ Secure Web Authentication (SWA)

Uses credentials to sign in. This integration works with most apps.

☒ SAML 2.0

Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

☐ OpenID Connect

Uses the OpenID Connect protocol to log users into an app you've built.

Create

Cancel

e) Fill the app Name as Jenkins and leave the rest as default and click next

f) Now fill the required fields as shown in the picture below:

GENERAL

Single sign on URL ?

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Show Advanced Settings](#)

g) Define the user attributes as:

1. Name: DisplayName

Name format: unspecified

Value: String.join(" ",user.firstName,user.lastName)

2. Name: Email
Name format: unspecified
Value: user.email

- h) Define the group attributes as:
Name: Group
Name format: basic
Filter: Match regex (fill the regex value as “.*”)
Click next.
- i) Now select I am a customer and adding an internal app.
Now check the box saying “this is an internal app” in App type.
Click Finish.
- j) Now go to the assignments tab and assign the groups we have created to the application.
- k) Now goto the signon tab and scroll down to “Identity provider metadata”
Open it in a new tab and copy the XML from there.

General **Sign On** Import People Groups

Settings


Edit

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.

SAML 2.0

Default Relay State

SAML Library Version Current



SAML 2.0 is not configured until you complete the setup instructions.
[View Setup Instructions](#)
[Identity Provider metadata](#) is available if this application supports dynamic configuration.

- l) Now go back to the jenkins and goto manage jenkins.
m) Click on configure global security

n) Now choose Security Realm as SAML 2.0.

Now fill the required fields as:

● SAML 2.0

SAML Identity Provider Settings

IdP Metadata

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exka9pfgylWau38jE0h7"><md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="signing"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data>
<ds:X509Certificate>MIIDpDCCAoygAwIBAgIAGAVugnnNQMA0GCsQGSIb3DQEBECwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FueiEZYW5jaXNjbzENMAAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCMRldi00MDY0NDkxHDAABgkqhkiG9w0BCQEW
DWluZm9Ab2t0YS5jb20wHhcNMjcwNDI0MTUzODUwWWhcNMjcwNDI0MTUzODUwWjCBKjELMAkGA1UE
BhMCVVMxEzARBgNVBAgMCkNhbm3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTALBgNV
BAoMBE9rdGEzFDASBgNVBAcMC1NTT1Byb3ZpZGVyMRMwEQYDVQQDDApkZXlYNDANQ2Q5MRwwGgYJ
KoZlhcNAQKBG91pbmZvQ9rdGEuY29lMIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEA
q4nipy0szAsX20uRtNCwkKfthE2ct08QX2dN9ikG8kn0oJyod0GyeNsNeTG6QEIKtwzSe/BfcR1
qFrWPyP/bVhbgMsjldi8kAgm6n+J8vyA3Y12viDI7xo1u4LU56u+H2V72l/Eb7oJEavQIE0ICZM
MFJzDj1Gy+RvPiG5HZCELEdrFY0vvHUF8o4mVcBxluGm2l5ip++psSzxgdkNE9AqQqGd5KLFzD+q
K/LFwe7s9A+k4hf+m9AgVcmmdC3Hny/pAD82qDQTso6uAm0PFnyUEdOXF6tR7pDxWcabcphw1
dsGfOwL.CimPG98zsGEnr1JIY/4b5i4X6Y8GnWIDQAABMA0GCsQGSIb3DQEBECwUAA4IBAQBLYNCK
TPN/nHmtu/R0Ww5fMyblPgILdmMKCq1qCuMPIVZPHvGgwUFcUutmacEVfaCNUx2Qng1zQ9km2SpP
```

Display Name Attribute

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

Group Attribute

Group

Maximum Authentication Lifetime

86400

Username Attribute

Username Case Conversion

None

☐ Use Encryption ?

[Service Provider Metadata](#) which may be required to configure your Identity Provider (based on last saved settings).

Validate the IDP and after you see success.

Copy the value of the display name and paste it in the Username attribute.

Now in the Display name fill the custom attribute we have defined above ie
"DisplayName"

Similarly fill the Group attribute as custom attribute ie "Group"

Now check the advance configuration box and fill the SP Entity ID as "Jenkins-users"

Now in Authorization click on anyone can do anything for safety and setup purpose
because after this admin user cannot get logged in.

o) Now log out from admin user and click on login and you will get a signon page, fill your
username and password of Okta and you will get logged in to the jenkins.

p) Now go to the authorization and set it as per your need.

q) Now get the sign in link in the General tab as Embedded link and share it with the users
for sign in.