Single Sign On

Setup Guide

Version 1.0

Document Number: SSOSG 100.005

Document Title: Single Sign On Setup Guide
Document Release Date: October 2023
Document Number: SSOSG 100.005

Published by:
Research & Development
meshIQ
88 Sunnyside Blvd, Suite 101
Plainview, NY 11803

Confidentiality Statement: The information within this media is proprietary in nature and is the sole property of meshIQ. All products and information developed by meshIQ are intended for limited distribution to authorized meshIQ employees, licensed clients, and authorized users. This information (including software, electronic and printed media) is not to be copied or distributed in any form without the expressed written permission from meshIQ.

Contents

Chapter 1: Introduction

1.1 What is Single Sign On (SSO)?

Single sign-on (SSO) is an authentication method that allows users to securely sign on to several software systems with one set of credentials.

Single Sign-On requires two entities to be defined:

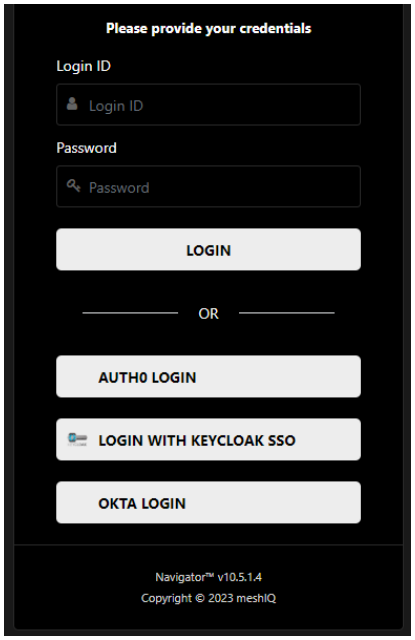
- Service Provider: This is the provider of the service, or application, to which users are signing on. (In this case, the provider is meshIQ.)
- Identity Provider: This is the provider that is responsible for authenticating users for the sign-on process. In this document, Identity Providers are Keycloak, Okta, Auth0, and Ping Identity.

The name of the XML configuration file that stores settings for these entities is as follows:

- The xray_samlsso.xml configuration file stores XRay SSO configuration settings.
- The apwmq_samlsso.xml configuration file stores Navigator SSO configuration settings.

Multiple Identity Providers

A single login page can include multiple buttons, so that users can choose which identity providers they want to use to sign on. When this is the case, the Tomcat samlsso configuration file includes more than one <config> element; each one represents a different button on the login page.



Simplified configuration file example:

```
<configs>
        <config>
            [Name, description, button, and other configuration for
    Auth0 SSO]
            <position>1</position>
        </config>

        <config>
            [Name, description, button, and other configuration for
    Keycloak SSO]
            <position>2</position>
        </config>

        <config>
            [Name, description, button, and other configuration for
    Okta SSO]
            <position>3</position>
        </config>
    </configs>
```

The image above shows a login page with a button for three identity providers: Auth0, Keycloak, and Okta.

1.2 How this Guide is Organized

Chapter 1:	Introduction and document information
Chapter 2:	Contains setup and configuration information for the Keycloak identity provider.
Chapter 3:	Contains setup and configuration information for the Okta identity provider.
Chapter 4:	Contains setup and configuration information for the Auth0 identity provider.
Chapter 5:	Contains setup and configuration information for the Ping Identity provider.
Chapter 6:	Contains instructions for where to place the SSO configuration file and how to point to it.

1.3 History of this Document

Table 1 History of this Document

Release Date	Document Number	Product Version	Summary
October 2023	100.005	Navigator 10.3 and later; XRay 1.4 and later	Initial public release.

1.3.1 User Feedback

meshIQ encourages all users and administrators to submit comments, suggestions, corrections, and recommendations for improvement of all documentation. Please send your comments via e-mail to: support@meshiq.com. You will receive a response, along with status of any proposed change, update, or correction.

1.4 Release Notes

See the online release notes in the meshIQ Resource Center at *https://customers.meshiq.com/hc/en-us*.

1.5 Intended Audience

This guide is intended for administrators.

1.6 Technical Support

If you need additional technical support, you can contact meshIQ by telephone or by e-mail. To contact technical support by telephone, call 800-963-9822 ext. 1, if you are calling from outside the United States dial 001-516-801-2100. To contact meshIQ technical support by e-mail, send a message to *mysupport@meshiq.com.* To access the meshIQ automated support system (user ID and password required), go to *https://mysupport.meshiq.com/*. Contact your local administrator for further information.

Chapter 2: Keycloak (XRay Example)

2.1 Installation

https://hub.docker.com/r/jboss/keycloak

https://github.com/keycloak/keycloak-containers/blob/14.0.0/server/README.md

download image of Keycloak (latest version)

```
docker pull jboss/keycloak
```

Start keycloak server instance.

```
docker run --name keycloak01 --restart unless-stopped -e KEYCLOAK_USER=admin -e KEYCLOAK_PASSWORD=admin -p 8880:8080 -d jboss/keycloak
```

Start keycloak server instance.

```
docker ps -a
docker logs keycloak01
```

Upgrade process:

If there is a new version of Keycloak, stop the current version and remove it.

```
docker stop keycloak01
docker rm keycloak01
```

To install the new version, repeat the installation commands above.

2.2 Keycloak Identity Provider Configuration

After installing Keycloak, the next step is to set it up as an Identity Provider. In this document, Keycloak is the first of three Identity Providers that will be covered. Okta and Auth0 are discussed in later chapters.

Access the Keycloak Administration Console.

- If you are running Keycloak locally, open a browser and go to http://localhost:8880/auth/admin/.
- Otherwise, go to http://[*ip address*]:[*port*]/.

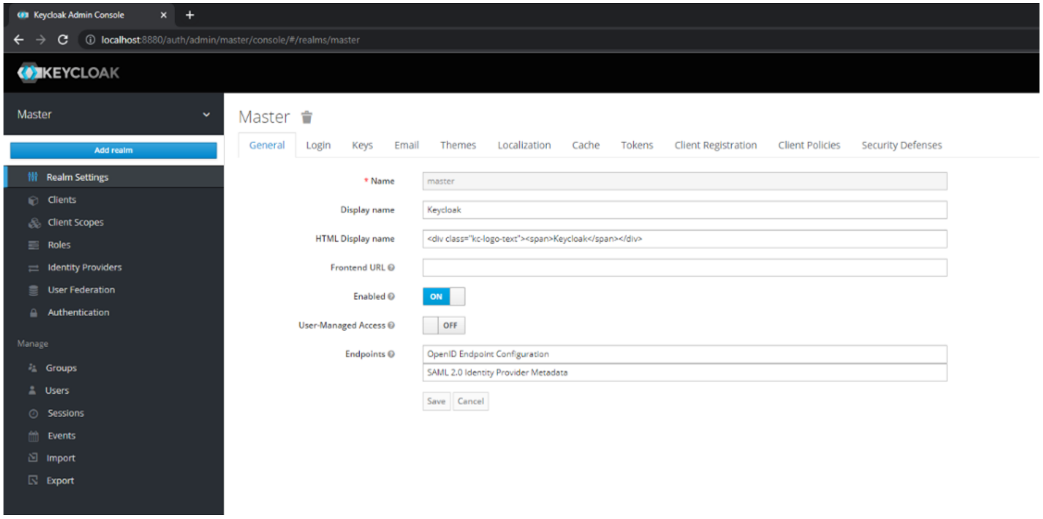
You will be redirected to the Keycloak login page.

Click **Administration Console**.

Log in with the admin username and password you created in the previous section.

The Keycloak Admin Console opens, as shown below. Use the following steps to set up a realm and client, export the Client Signing Key, add client roles, create groups, and create users.

1. Create a new Realm (For example "Nastel").
   a. Move the mouse over ("hover" over) the current realm name (probably "Master").



* Name: master

Display name: Keycloak

HTML Display name: <div class="kc-logo-text"><span>Keycloak</span></div>

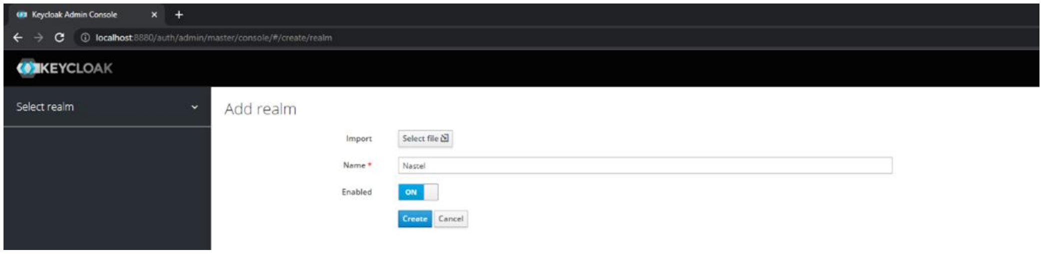
Frontend URL:

Enabled: ON

User-Managed Access: OFF

Endpoints: OpenID Endpoint Configuration; SAML 2.0 Identity Provider Metadata

   b. Click **Add realm**.
   c. Enter the name of the new realm ("Nastel").



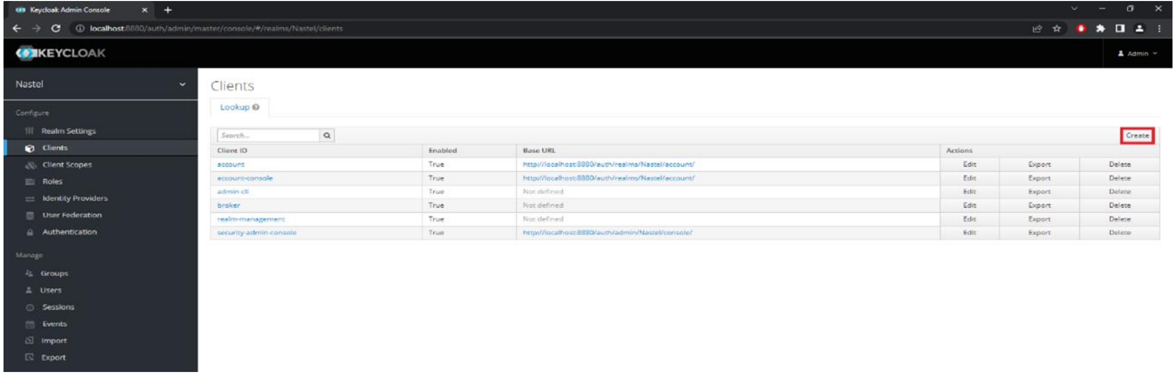
Import: Select file

Name *: Nastel

Enabled: ON

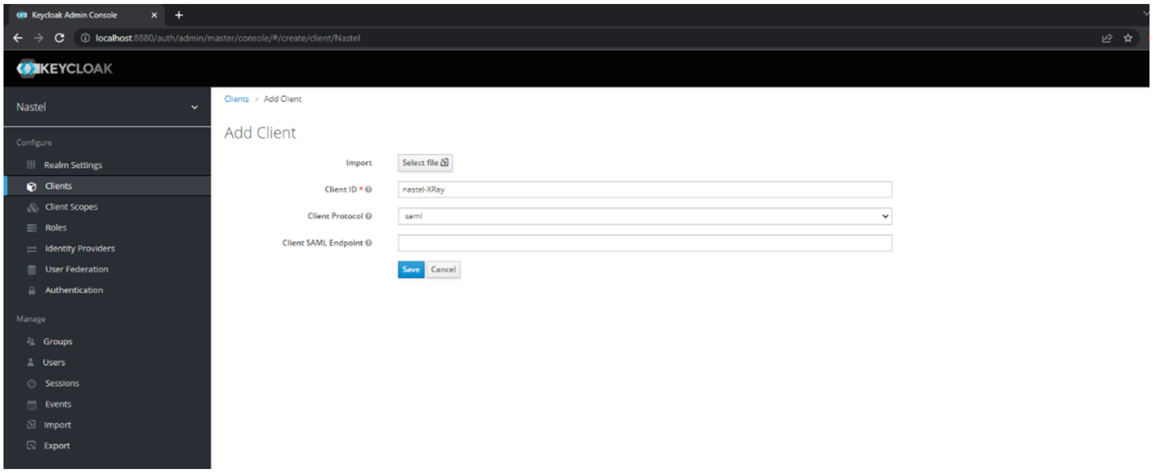
   d. Click **Create**.
2. Create a new Client (for example, "nastel-XRay").
   a. Click **Clients** on the Configure menu on the left.

b. Click **Create** in the upper-right corner of the table.



Client ID	Enabled	Base URL	Actions		
account	True	http://localhost:8880/auth/realms/Nastel/account/	Edit	Export	Delete
account-console	True	http://localhost:8880/auth/realms/Nastel/account/	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	http://localhost:8880/auth/admin/Nastel/console/	Edit	Export	Delete

c. Enter a **Client ID** ("nastel-XRay") and select **saml** from the **Client Protocol** list.



Import: Select file

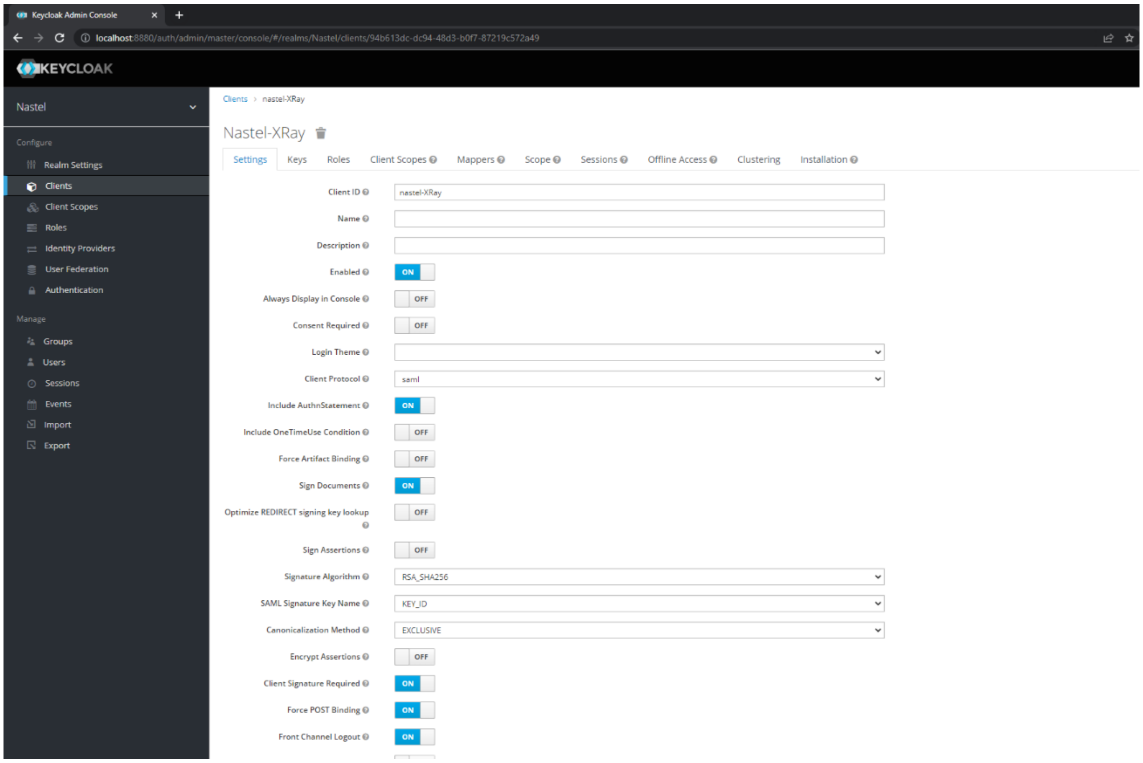
Client ID *: nastel-XRay

Client Protocol: saml

Client SAML Endpoint:

d. Click **Save**.

e. Enter "*" in the **Valid Redirect URIs** field.



Client ID: nastel-XRay

Name:

Description:

Enabled: ON

Always Display in Console: OFF

Consent Required: OFF

Login Theme:

Client Protocol: saml

Include AuthnStatement: ON

Include OneTimeUse Condition: OFF

Force Artifact Binding: OFF

Sign Documents: ON

Optimize REDIRECT signing key lookup: OFF

Sign Assertions: OFF

Signature Algorithm: RSA_SHA256

SAML Signature Key Name: KEY_ID

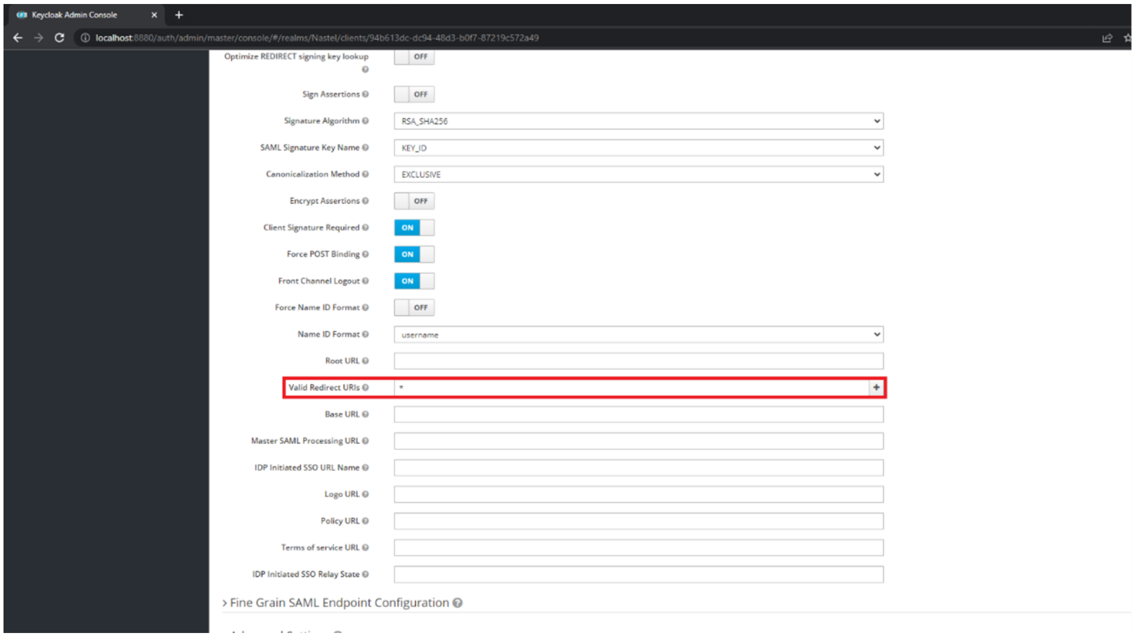
Canonicalization Method: EXCLUSIVE

Encrypt Assertions: OFF

Client Signature Required: ON

Force POST Binding: ON

Front Channel Logout: ON


Keycloak Admin Console
localhost:8880/auth/admin/master/console/#/realms/Nastel/clients/94b613dc-dc94-48d3-b0f7-87219c572a49

Optimize REDIRECT signing key lookup: OFF

Sign Assertions: OFF

Signature Algorithm: RSA_SHA256

SAML Signature Key Name: KEY_ID

Canonicalization Method: EXCLUSIVE

Encrypt Assertions: OFF

Client Signature Required: ON

Force POST Binding: ON

Front Channel Logout: ON

Force Name ID Format: OFF

Name ID Format: username

Root URL:

Valid Redirect URIs: *

Base URL:

Master SAML Processing URL:

IDP Initiated SSO URL Name:

Logo URL:

Policy URL:

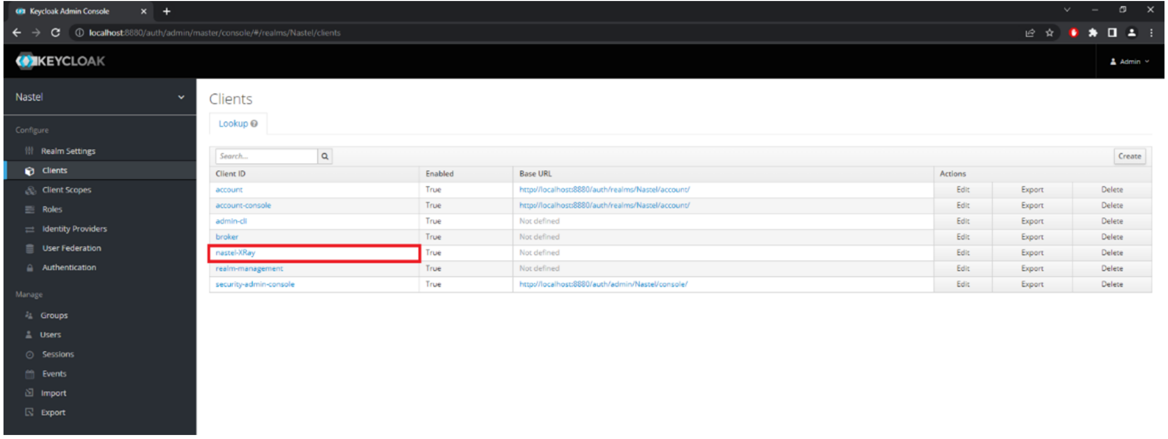
Terms of service URL:

IDP Initiated SSO Relay State:

› Fine Grain SAML Endpoint Configuration

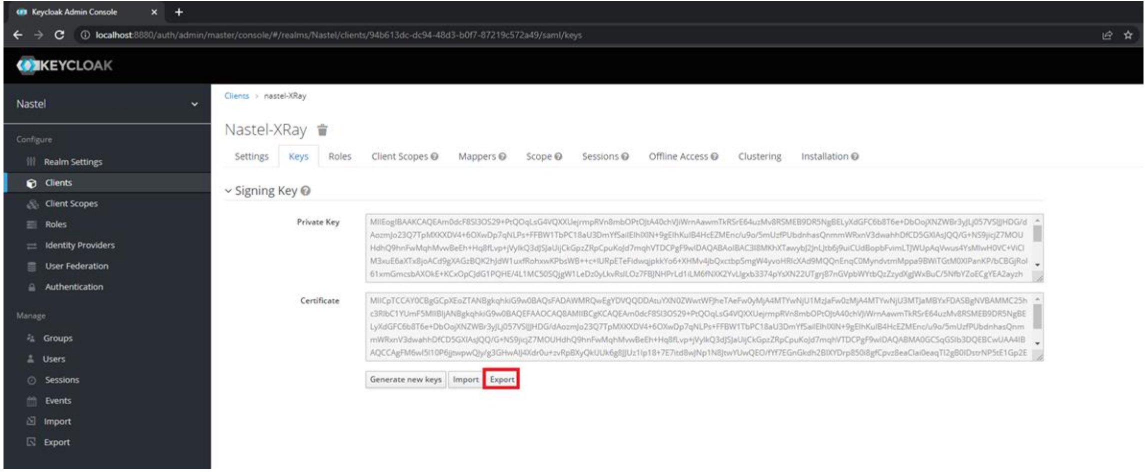
f. Click **Save**.

3. Export the Client Signing Key:
   a. Click **Clients** on the Configure menu on the left.
   b. Open the recently created Client (“nastel-XRay”).



Client ID	Enabled	Base URL	Actions		
account	True	http://localhost:8880/auth/realms/Nastel/account/	Edit	Export	Delete
account-console	True	http://localhost:8880/auth/realms/Nastel/account/	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
nastel-XRay	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	http://localhost:8880/auth/admin/Nastel/console/	Edit	Export	Delete

   c. Open the **Keys** tab.
   d. Click **Export**.



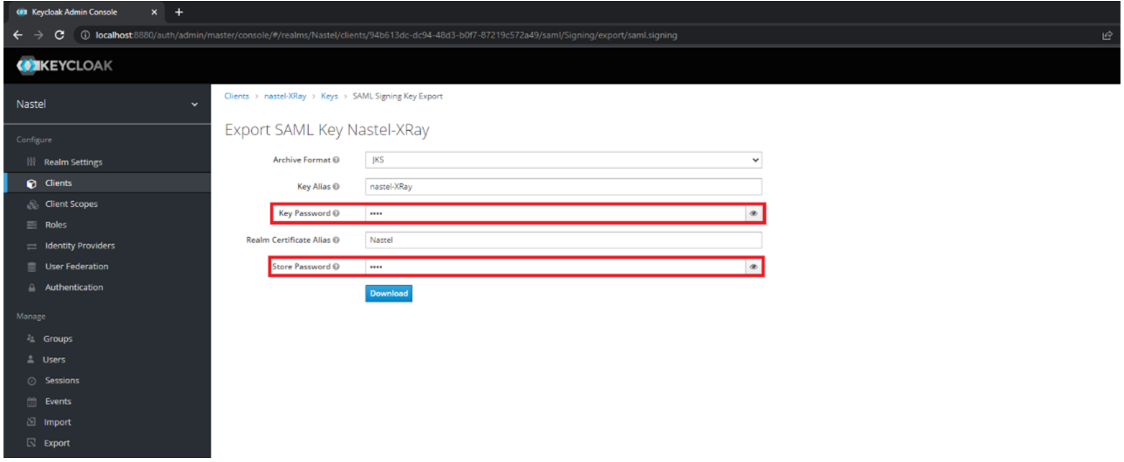
Private Key

MIIEogIBAAKCAQEAm0dcF8SI3OS29+PtQOqLsG4VQXXUejrmpRVn8mbOPtOJtA40chVJiWrnAawmTkRSrE64uzMv8RSMEB9DR5NgBELyXdGFC6b8T6e+DbOojXNZWBr3yJLj057VSIJJHDG/d
AozmJo23Q7TpMXKXDV4+6OXwDp7qNLPs+FFBW1TbPC18aU3DmYfSailElhIXIN+9gElhKuIB4HcEZMEnc/u9o/5mUzfPUbdnhasQnmmWRxnV3dwahhDfCD5GXIAsJQQ/G+NS9jicjZ7MOU
HdhQ9hnFwMqhMvwBeEh+Hq8fLvp+jVylkQ3dJSJaUijCkGpzZRpCpuKoJd7mqhVTDCPgF9wIDAQABAoIBAC3I8MKhXTawybJ2JnLJtb6j9uiCUdBopbFvimLTJWUpAqVwus4YsMIwH0VC+ViCI
M3xuE6aXTx8joACd9gXAGzBQK2hJdW1uxfRohxwKPbsWB++c+IURpETeFidwqjpkkYo6+XHMv4jbQxctbpSmgW4yvoHRIcXAd9MQQnEnqC0MyndvtmMppa9BWiTGtM0XIPanKP/bCBGjRol
61xmGmcsbAXOkE+KCxOpCJdG1PQHE/4L1MC50SQjgW1LeDz0yLkvRsILOz7FBJNHPrLd1iLM6fNXK2YvLlgxb3374pYsXN22UTgrj87nGVpbWYtbQzZzydXgJWxBuC/5NfbYZoECgYEA2ayzh

Certificate

MIICpTCCAY0CBgGCpXEoZTANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDDAtuYXN0ZWwtWFJheTAeFw0yMjA4MTYwNjU1MzJaFw0zMjA4MTYwNjU3MTJaMBYxFDASBgNVBAMMC25h
c3RlbC1YUmF5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAm0dcF8SI3OS29+PtQOqLsG4VQXXUejrmpRVn8mbOPtOJtA40chVJiWrnAawmTkRSrE64uzMv8RSMEB9DR5NgBE
LyXdGFC6b8T6e+DbOojXNZWBr3yJLj057VSIJJHDG/dAozmJo23Q7TpMXKXDV4+6OXwDp7qNLPs+FFBW1TbPC18aU3DmYfSailElhIXIN+9gElhKuIB4HcEZMEnc/u9o/5mUzfPUbdnhasQnm
mWRxnV3dwahhDfCD5GXIAsJQQ/G+NS9jicjZ7MOUHdhQ9hnFwMqhMvwBeEh+Hq8fLvp+jVylkQ3dJSJaUijCkGpzZRpCpuKoJd7mqhVTDCPgF9wIDAQABMA0GCSqGSIb3DQEBCwUAA4IB
AQCCAgFM6wI5I10P6jjtwpwQJy/g3GHwAIJ4Xdr0u+zvRpBXyQkUUk6g8JJUz1Ip18+7E7itd8wJNp1N8JtwYUwQEO/fYf7EGnGkdh2BIXYDrp850i8gfCpvz8eaClai0eaqTI2gB0IDstrNP5tE1Gp2E

e. Add a **Key Password** and a **Store Password**.


Keycloak Admin Console
localhost:8880/auth/admin/master/console/#/realms/Nastel/clients/94b613dc-dc94-48d3-b0f7-87219c572a49/saml/Signing/export/saml.signing
KEYCLOAK
Nastel
Configure
Realm Settings
Clients
Client Scopes
Roles
Identity Providers
User Federation
Authentication
Manage
Groups
Users
Sessions
Events
Import
Export
Clients › nastel-XRay › Keys › SAML Signing Key Export

Export SAML Key Nastel-XRay

Archive Format: JKS

Key Alias: nastel-XRay

Key Password: ••••

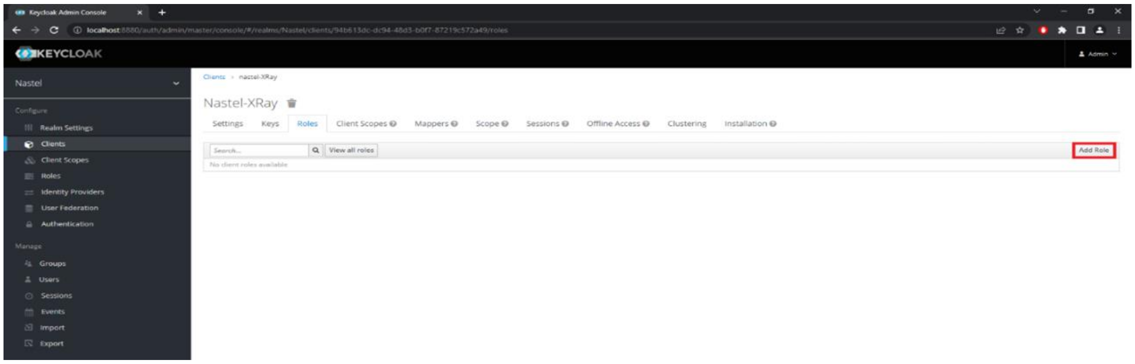
Realm Certificate Alias: Nastel

Store Password: ••••

Download

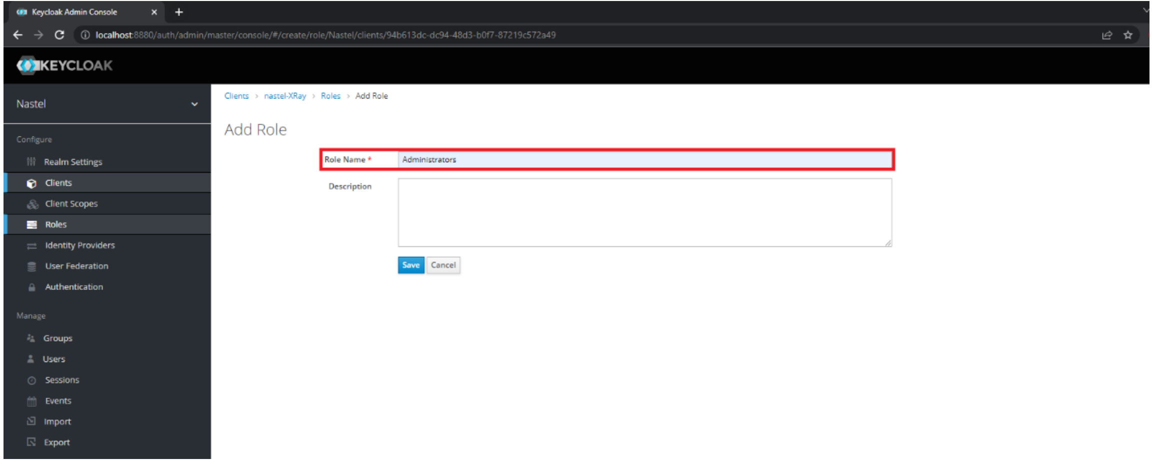
f. Click **Download**.

4. Add Client Roles. Roles names should correspond to Team names in XRay.
    a. Click **Clients** on the Configure menu on the left.
    b. Open the Client you created in step 2 (“nastel-XRay”).
    c. Open the **Roles** tab.
    d. Click **Add Role**.



No client roles available

e. Enter a **Role Name** (for example, “Administrators”).



Add Role

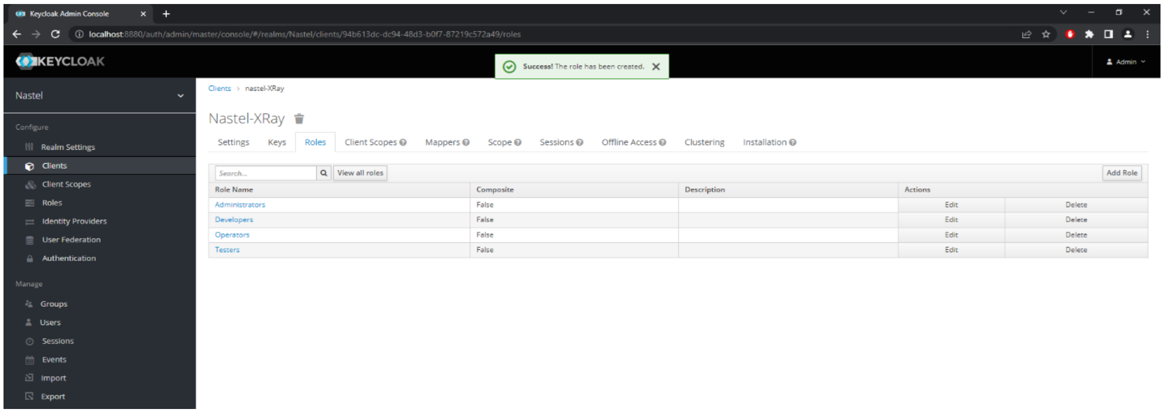
Role Name *: Administrators

Description:

Save Cancel

f. Click **Save**.

g. Repeat steps a-f for other Roles. Create a Role for each XRay Team, with the same name as the Team.

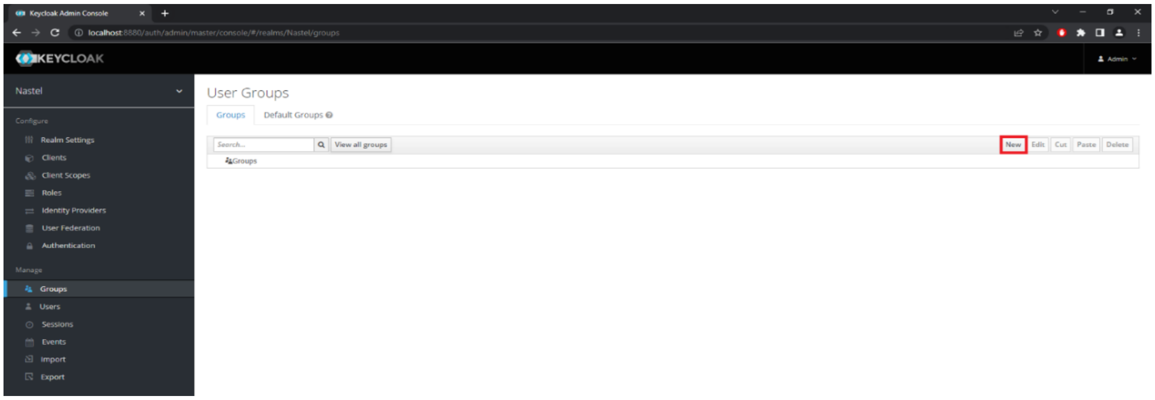


localhost:8880/auth/admin/master/console/#/realms/Nastel/clients/94b613dc-dc94-48d3-b0f7-87219c572a49/roles

Success! The role has been created.

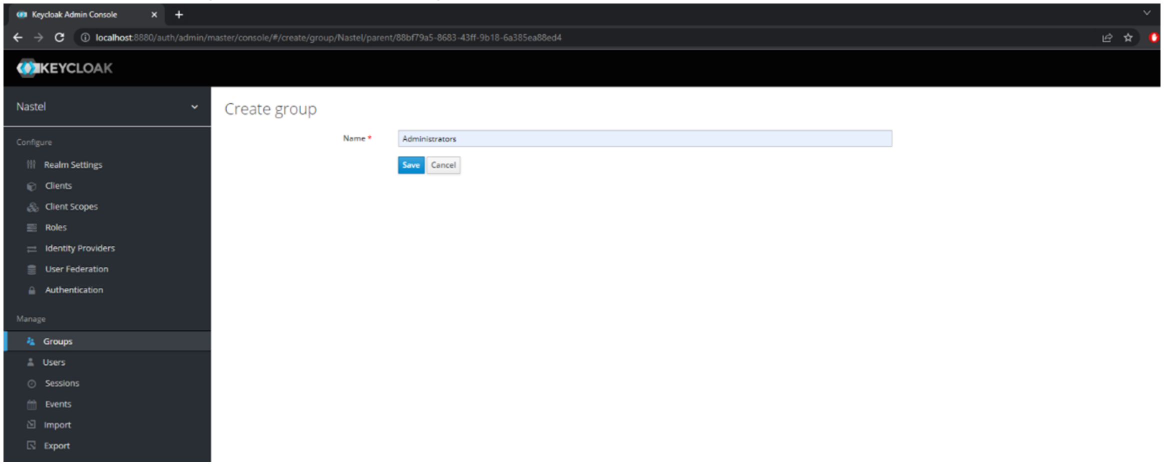
Role Name	Composite	Description	Actions	
Administrators	False		Edit	Delete
Developers	False		Edit	Delete
Operators	False		Edit	Delete
Testers	False		Edit	Delete

5. Create Groups. Group names should also correspond to Team names in XRay. Create a Group for each XRay Team, with the same name as the Team.
   a. Click **Groups** on the Manage menu on the left.
   b. Click **New**.



localhost:8880/auth/admin/master/console/#/realms/Nastel/groups

   c. Enter a **Name** (“Administrators”).

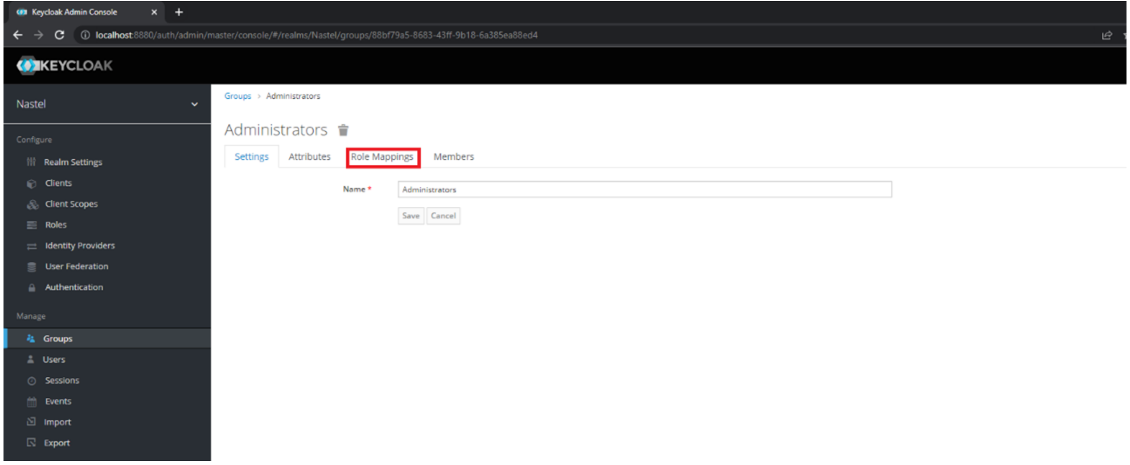


localhost:8880/auth/admin/master/console/#/create/group/Nastel/parent/88bf79a5-8683-43ff-9b18-6a385ea88ed4

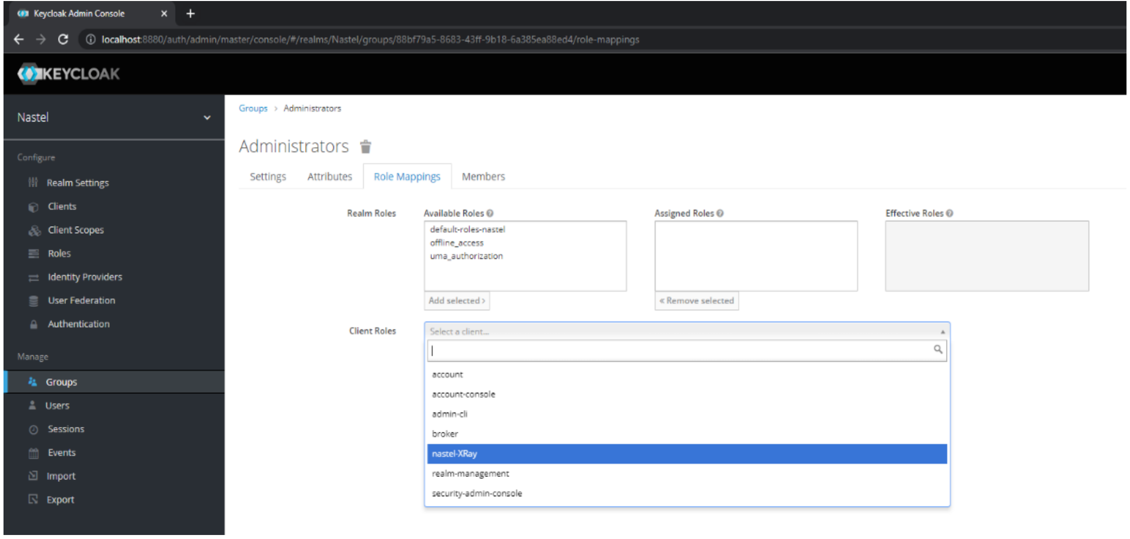
Name * Administrators

   d. Click **Save**.

e. Open the **Role Mappings** tab.



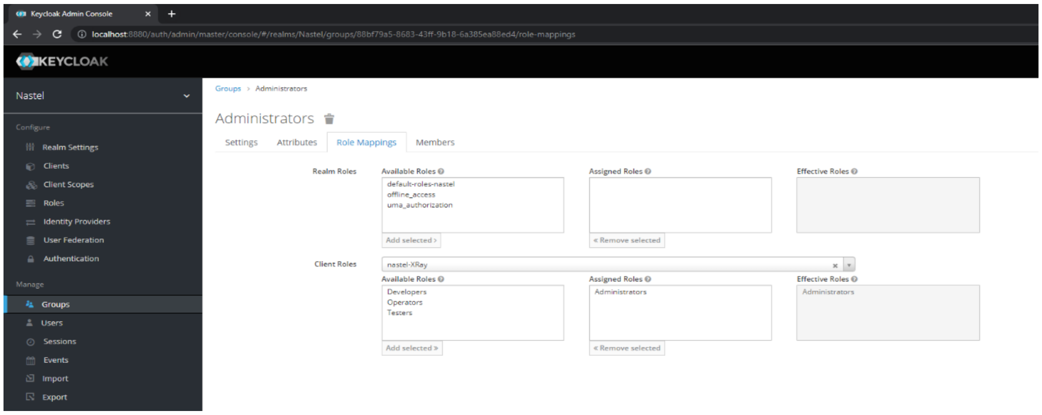
f. Select the Client you created (“nastel-XRay”) from the list of **Client Roles**.



g. Add Roles:

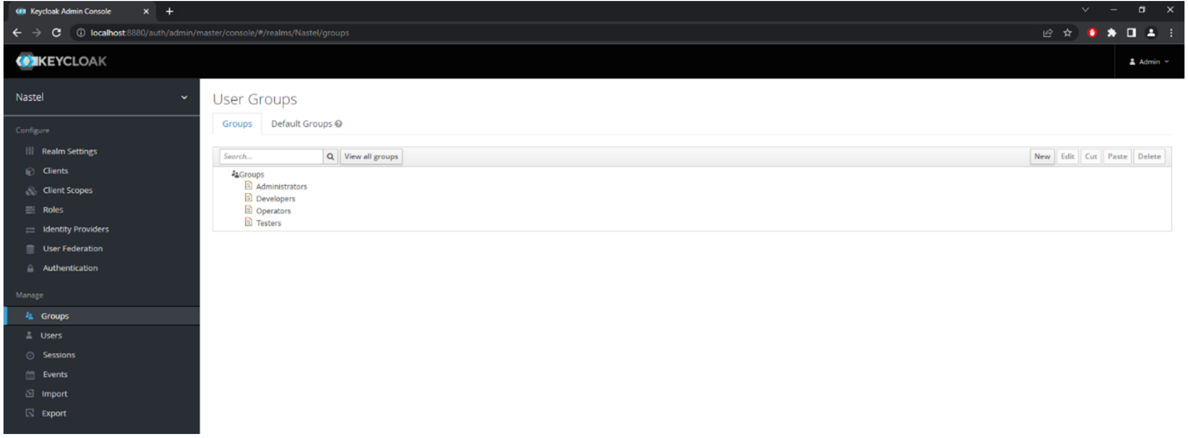
i. Select one or more roles from the list of **Available Roles**.

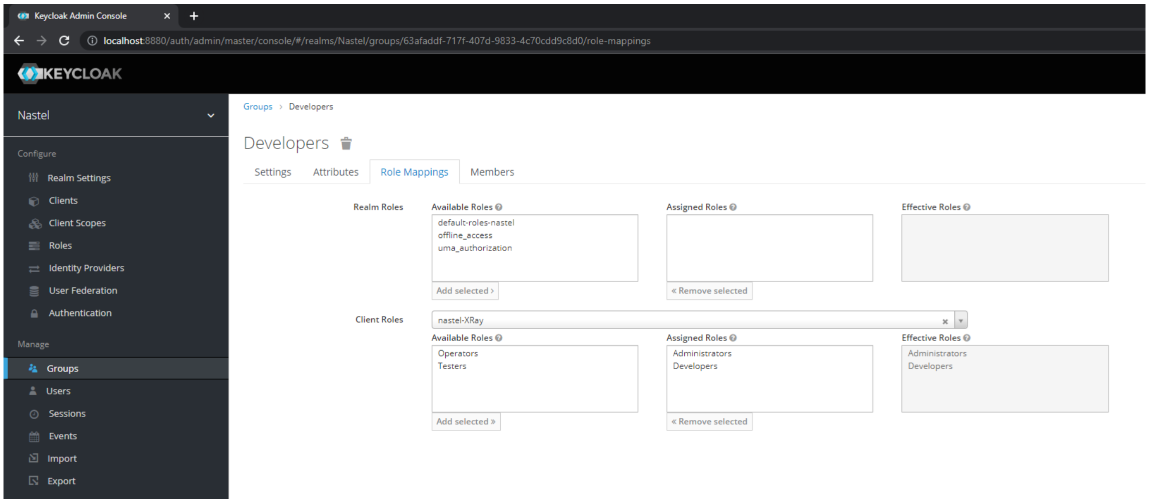
ii. Click **Add selected**.



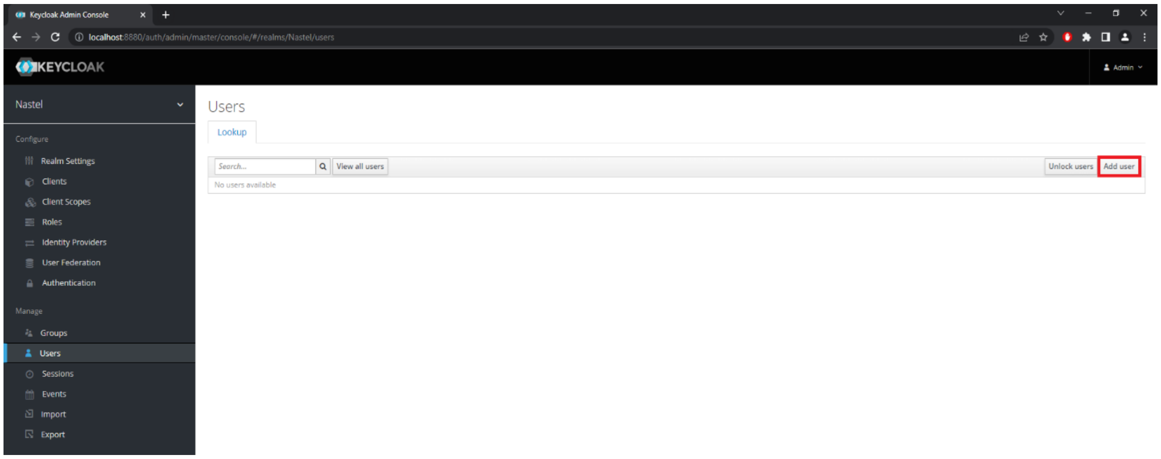
h. Repeat steps a-g for other Groups. Groups names should also correspond to team names in XRay. If the group you’re adding corresponds to an XRay team that itself belongs to another XRay team, then add both roles in Keycloak. For example, if the Developers team belongs to the Administrators team, then when you are creating the Developers group in step 5g, add both Roles:

Developers and Administrators.



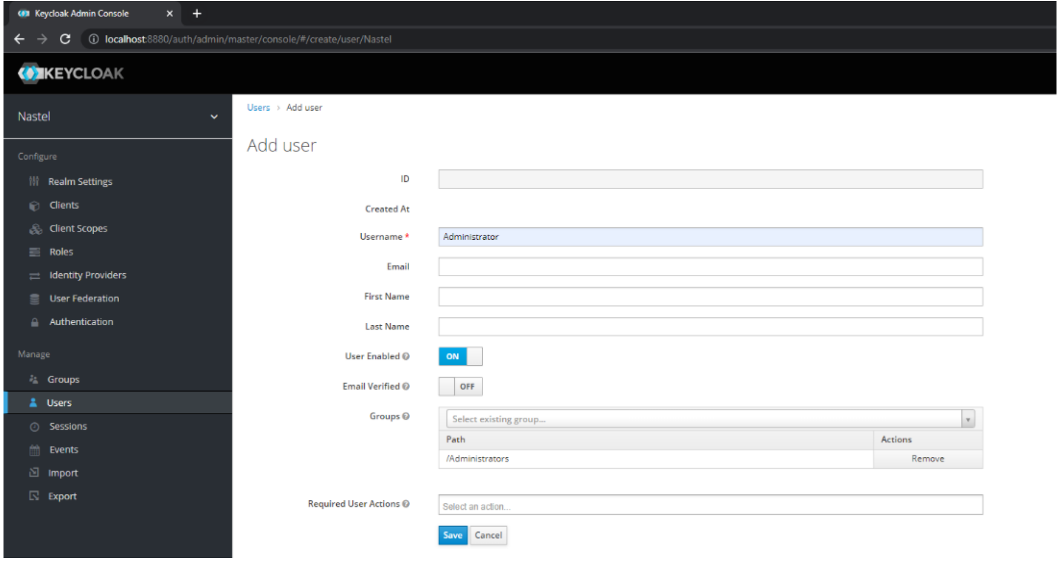


6. Create Users.
   a. Click **Users** on the Manage menu on the left.
   b. Click **Add user**.



   c. Enter a **Username** and use the **Groups** list to add all the Teams the user belongs to in XRay. To add groups:
      i. Click **Select existing groups**....
      ii. Start typing the name of the group (names are case-sensitive).

iii. Select the group from the list.



Add user

ID

Created At

Username * Administrator

Email

First Name

Last Name

User Enabled: ON

Email Verified: OFF

Groups: Select existing group...

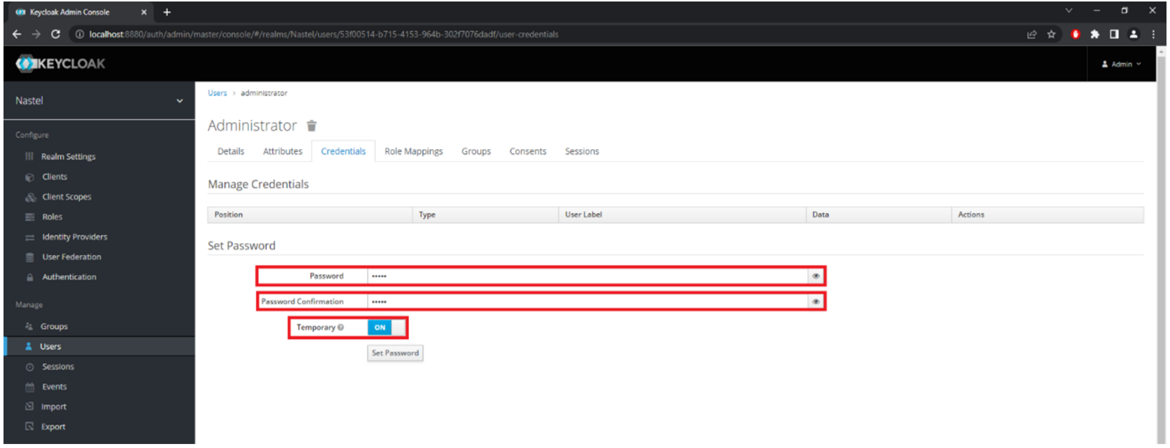
Path	Actions
/Administrators	Remove

Required User Actions: Select an action...

d. Click **Save**.

e. Open the **Credentials** tab.

f. Enter the user's password in both the **Password** and **Password Confirmation** fields. By default, the Temporary setting is on. If it is left on, the user will need to change the password after the first login.



Administrator

Manage Credentials

Position	Type	User Label	Data	Actions

Set Password

Password •••••

Password Confirmation •••••

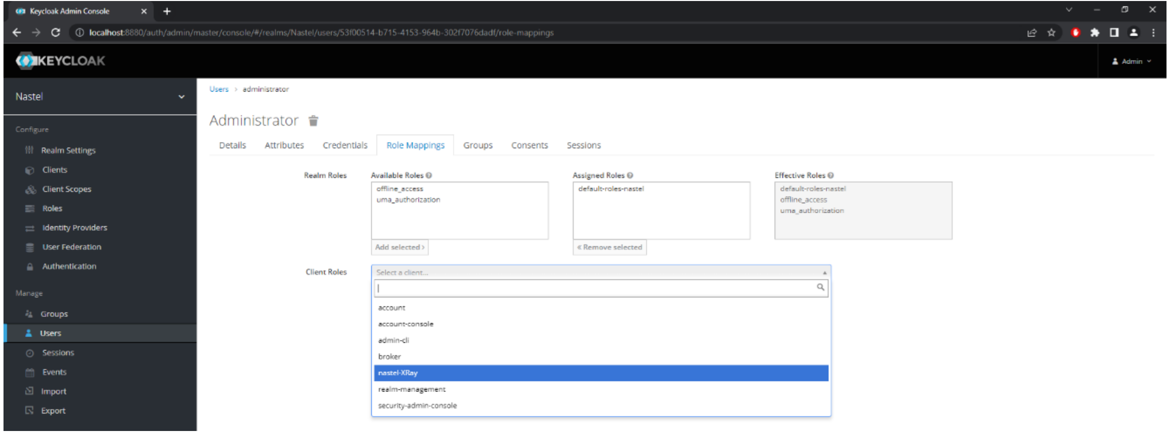
Temporary: ON

g. Click **Set Password**. A confirmation message is displayed.

h. Click **Set Password** on the message to confirm it.

i. Open the **Role Mappings** tab.

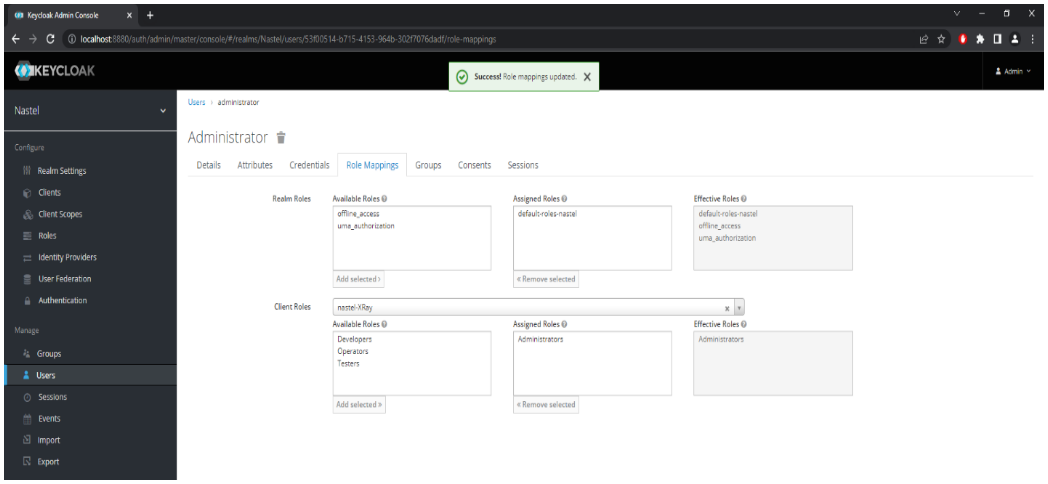
j. Select the Client you created ("nastel-XRay") from the **Client Roles** list.



k. Add roles:

iv. Select one or more roles from the list of **Available Roles**.

v. Click **Add selected**.



l. If a user belongs to an XRay team that itself belongs to another XRay team, then add both roles in Keycloak. For example, if the user belongs to the XRay Developers team, which belongs to the XRay Administrators team, then when you are creating the user in step 6k, add both Roles: Developers and Administrators.

2.3 Important Configuration Parameters

2.3.1 For Service Providers

spEntityId – Specify the Client name.

spCert > *keyStoreFile* – Specify the absolute path to the Client Signing Key file (from step 3 in Keycloak Identity Provider Configuration).

spCert > StorePassword – Specify Store Password, if set.

spCert > *keyAlias* – Specify the Key Alias. If not changed, it should be the same as the Client name.

spCert > keyPassword – Specify the Key Password, if set.

2.3.2 For Identity Providers

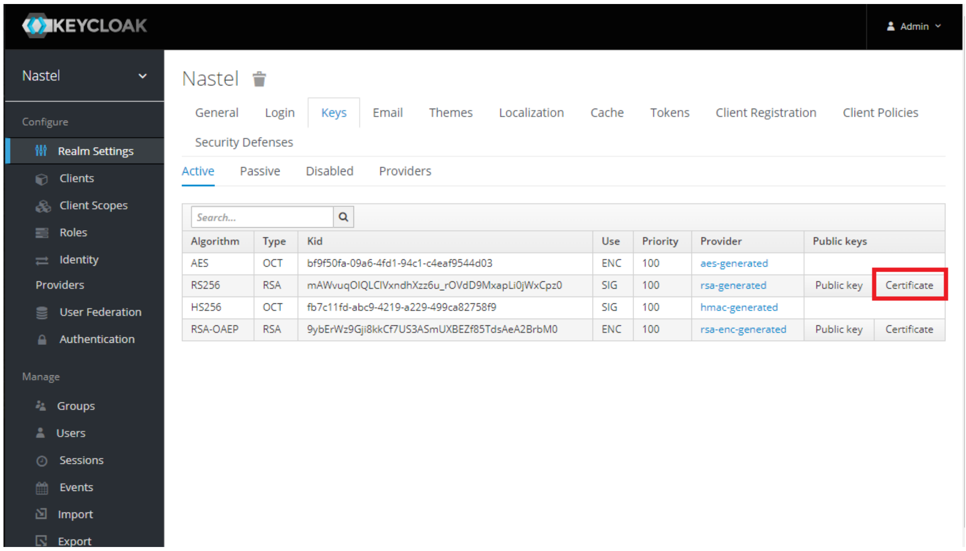
IdpEntityId, *idpSsoServiceUrl*, *idpArtifactResolveServiceUrl* and *idpSloServiceUrl*

2.3.2.1 Keycloak

In all URLs, it's important to specify the correct IP address (where Keycloak runs) and the Realm name.

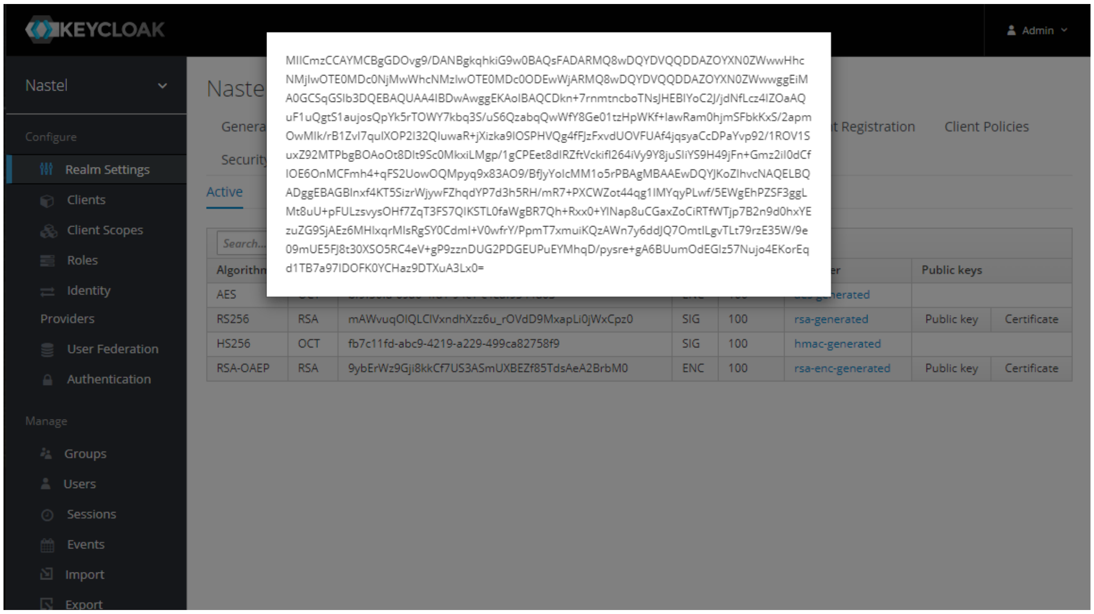
idpSignCert – To locate the Realm Key Certificate:

1. Make sure Nastel is selected in the Realm list.
2. Go to Realm Settings.
3. On the **Keys** tab, look for the record with "rsa-generated" in the **Provider** column.
4. Click **Certificate** to view it.



Algorithm	Type	Kid	Use	Priority	Provider	Public keys	
AES	OCT	bf9f50fa-09a6-4fd1-94c1-c4eaf9544d03	ENC	100	aes-generated		
RS256	RSA	mAWvuqOIQLClVxndhXzz6u_rOVdD9MxapLi0jWxCpz0	SIG	100	rsa-generated	Public key	Certificate
HS256	OCT	fb7c11fd-abc9-4219-a229-499ca82758f9	SIG	100	hmac-generated		
RSA-OAEP	RSA	9ybErWz9Gji8kkCf7US3ASmUXBEZf85TdsAeA2BrbM0	ENC	100	rsa-enc-generated	Public key	Certificate

The certificate is displayed on-screen.



```
MIICmzCCAYMCBgGDOvg9/DANBgkqhkiG9w0BAQsFADARMQ8wDQYDVQQDDAZOYXN0ZWwwHhc
NMjIwOTE0MDc0NjMwWhcNMzIwOTE0MDc0ODEwWjARMQ8wDQYDVQQDDAZOYXN0ZWwwggEiM
A0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCDkn+7rnmtncboTNsJHEBIYoC2J/jdNfLcz4IZOaAQ
uF1uQgtS1aujosQpYk5rTOWY7kbq3S/uS6QzabqQwWfY8Ge01tzHpWKf+lawRam0hjmSFbkKxS/2apm
OwMIk/rB1ZvI7quIXOP2I32QIuwaR+jXizka9IOSPHVQg4fFJzFxvdUOVFUAf4jqsyaCcDPaYvp92/1ROV1S
uxZ92MTPbgBOAoOt8DIt9Sc0MkxiLMgp/1gCPEet8dIRZftVckifI264iVy9Y8juSIiYS9H49jFn+Gmz2iI0dCf
IOE6OnMCFmh4+qFS2UowOQMpyq9x83AO9/BfJyYoIcMM1o5rPBAgMBAAEwDQYJKoZIhvcNAQELBQ
ADggEBAGBInxf4KT5SizrWjywFZhqdYP7d3h5RH/mR7+PXCWZot44qg1IMYqyPLwf/5EWgEhPZSF3ggL
Mt8uU+pFULzsvysOHf7ZqT3FS7QIKSTL0faWgBR7Qh+Rxx0+YINap8uCGaxZoCiRTfWTjp7B2n9d0hxYE
zuZG9SjAEz6MHIxqrMIsRgSY0CdmI+V0wfrY/PpmT7xmuiKQzAWn7y6ddJQ7OmtILgvTLt79rzE35W/9e
09mUE5FJ8t30XSO5RC4eV+gP9zznDUG2PDGEUPuEYMhqD/pysre+gA6BUumOdEGIz57Nujo4EKorEq
d1TB7a97IDOFK0YCHaz9DTXuA3Lx0=
```

Algorithn					er	Public keys	
AES					erated		
RS256	RSA	mAWvuqOIQLCIVxndhXzz6u_rOVdD9MxapLi0jWxCpz0	SIG	100	rsa-generated	Public key	Certificate
HS256	OCT	fb7c11fd-abc9-4219-a229-499ca82758f9	SIG	100	hmac-generated		
RSA-OAEP	RSA	9ybErWz9Gji8kkCf7US3ASmUXBEZf85TdsAeA2BrbM0	ENC	100	rsa-enc-generated	Public key	Certificate

2.4 Sample xray_samlsso.xml file using Keycloak

```
<?xml version="1.0"?>
<!-- SAML SSO handlers configurations -->
<configs>
<!-- SAML SSO handler configuration -->
<config>
<!-- Position, User defined -->
<position>2</position>
<!-- Unique name to select required handler, User defined -->
<name>test</name>
<!-- Description to show on link or button, User defined -->
<descr>Login via Test1 SSO</descr>
<!-- Button or link text (name), User defined -->
<buttonText>Login via Test1 SSO</buttonText>
<!-- Button icon (path or base64), User defined -->
<buttonIcon>data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAYAAAAfFcSJAAAADUlE
QVR42mP8/5+hHgAHggJ/PchI7wAAAABJRU5ErkJggg==</buttonIcon>
<!-- Color code for button background(#FFFFFF-white #000000-black), User defined -->
<buttonBackgroundColor>#FFFFFF</buttonBackgroundColor>
<!-- Color code for button text(#FFFFFF-white #000000-black), User defined -->
<buttonTextColor>#000000</buttonTextColor>
<!-- Service Provider client ID, issuer on authentication request, User defined (must be same as on IdP) -->
```

```xml
<spEntityId>nastel-XRay</spEntityId>

<!-- Service Provider assertion consumer URL for authentication request. In most cases, this field can be left
empty because it is generated automatically. For situations in which it cannot be generated automatically (for
example, if you are running multiple XRay instances behind load balancer), you will need to fill in this field as
follows:
<xray_host>/xray/servlet/SamlSsoLoginServlet/<xray-sp-entity-id>

 -->

<spAssertionCSUrl></spAssertionCSUrl>

<!-- Service Provider certificate will be used to sign requests or decrypt assertion, User defined (must be same as
on IdP) -->

<spCert>

<type>JKS</type>

<keyStoreFile>E:\nastel\nastel-XRay .jks</keyStoreFile>

<storePassword>test</storePassword>

<keyAlias>nastel-XRay</keyAlias>

<keyPassword>test</keyPassword>

</spCert>

<!-- Identity Provider entityID, From IdP metadata [EntityDescriptor > entityID] -->

<idpEntityId>http://172.16.6.206:8880/auth/realms/Nastel</idpEntityId>

<!-- Identity Provider SSO service URL, From IdP metadata [EntityDescriptor > IDPSSODescriptor >
SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->

<idpSsoServiceUrl>http://172.16.6.206:8880/auth/realms/Nastel/protocol/saml

</idpSsoServiceUrl>

<!-- Identity Provider SSO artifact resolve URL, From IdP metadata [EntityDescriptor > IDPSSODescriptor >
ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"] -->

<idpArtifactResolveServiceUrl>http://172.16.6.206:8880/auth/realms/Nastel/protocol/saml/resolve

</idpArtifactResolveServiceUrl>

<!-- Identity Provider SLO service URL, From IdP metadata [EntityDescriptor > IDPSSODescriptor >
SSingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->

<idpSloServiceUrl>http://172.16.6.206:8880/auth/realms/Nastel/protocol/saml

</idpSloServiceUrl>

<!-- Identity Provider certificate will be used to validate signatures, From IdP metadata [EntityDescriptor >
IDPSSODescriptor > KeyDescriptor use="signing" > KeyInfo > X509Data > X509Certificate] -->

<idpSignCert>MIICmzCCAYMCBgF6gLcmFDANBgkqhkiG9w0BAQsFADARMQ8wDQYDVQQDDAZuYXN0
ZWwwHhcNMjEwNzA3MTEyMzQ0WhcNMzEwNzA3MTEyNTI0WjARMQ8wDQYDVQQDDAZuYXN0ZWw
wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCA+oeUa7u8PkxLHZ6XhPldjCaPUCxg8+6st6
prTK4UEOR+kaIVjJzsZ0cTUS04IoaNhyj+YBdUAxKI/ZWxbQwcK7+nyCtS+quoIB8Sz7gejbi/2/EvwsDgw
2jmYttB/YetzuPPetrp+kOx/nuGs/eGB7IvKbPLz7rKRIzjdrKS0Oh3pLVP9KTT6+gRTTwOWkbG9RotpR
cdEOFATp4ywKA3stTgoIaRSXiCKt4uLjWiCrdNhijIFWKc1/UxFu38tvoFW8XCrTv/EihOikCEYoCfLOFd9
0p9s0eJA0uTMG7llqTdzbvB98x+SlaDZQPlWNcC/PhLwfp+Lg/1ushjtjDTAgMBAAEwDQYJKoZIhvcNAQ
ELBQADggEBAEGwPLd5bdE3y5VkxZjKtMB+J45stQjkpxsu4guv4ZYbpiOzlP8v/WM7QWpyXH1tKP3aA
YwvGCfNNpMaO++9wMSsNvEBu0lQaBZHrooCq6qFoWMG12N/iHdTfdxOhkiH2Aa6RGCGtRw/bUz+Ax
eHhPVmBXl6Igug/ruwMwV4jwlAIvx9WLtKDubdy1fzSZW68sCFeDXrRH4NlkZ3k8WwWC8VAhvnsNJL
+5vSOgL7ocG1OefAuhXm1iFroAjUXt27/HYDWylBpL3FbPVbyNWhSBZcOrS1AUZ14ECdRW6tOGONe3
0zze5xueHWGEWlOjan7e9O45h+SHvI8WsQpwJ0xuU=

</idpSignCert>
```

```
<!-- Service Provider must sign authentication request, User defined -->
<authnRequestSigned>true</authnRequestSigned>
<!-- Service Provider must sign artifact resolve request; User defined -->
<resolveArtifactRequestSigned>true</resolveArtifactRequestSigned>
</config>
</configs>
```

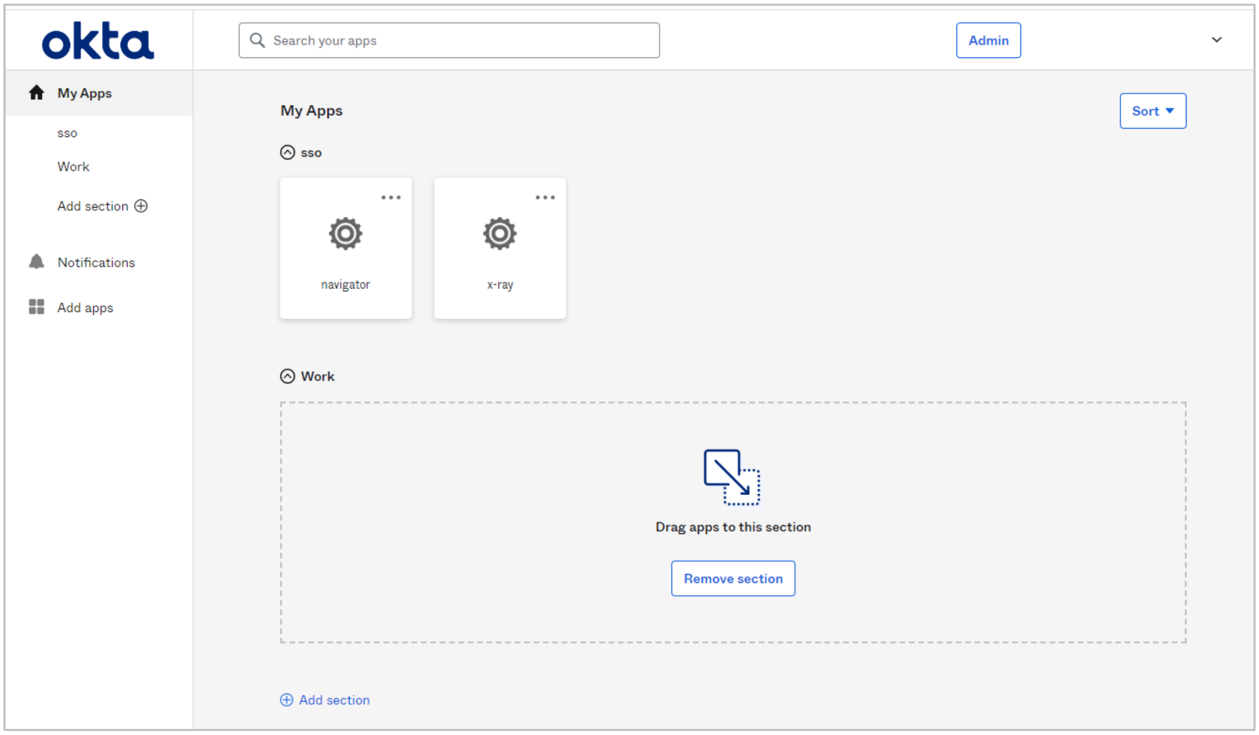
Chapter 3: Okta

The Okta Identity Provider does not require installation. To use Okta, you must complete the following online configuration steps and apply configurations to Tomcat.

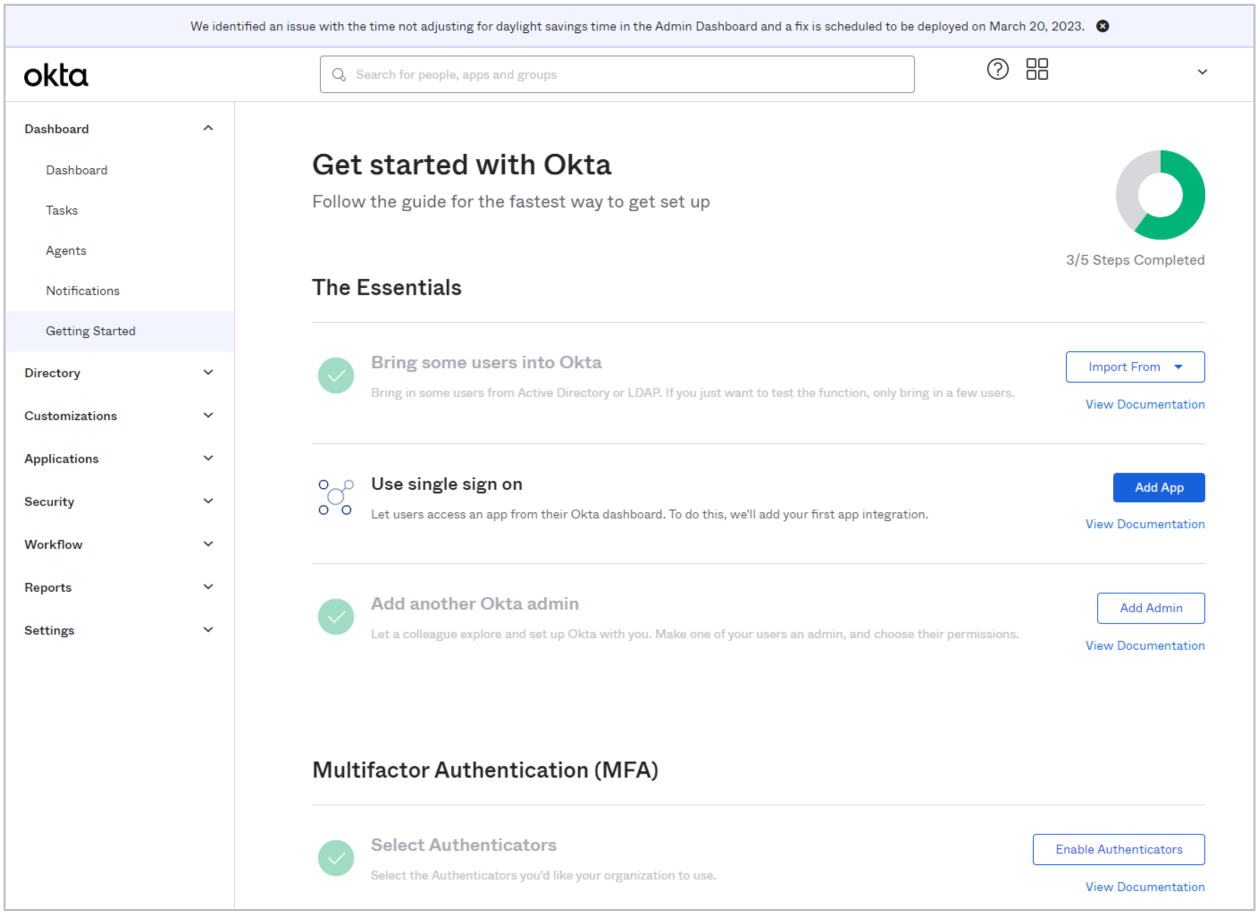
3.1 Okta Identity Provider Configuration (XRay Example)

First, set up the application to which you are providing SSO access through Okta.

1. Log into Okta. The main page is displayed.



2. To access Okta's configuration wizards, click **Admin** in the upper-right corner.


We identified an issue with the time not adjusting for daylight savings time in the Admin Dashboard and a fix is scheduled to be deployed on March 20, 2023.

Get started with Okta

Follow the guide for the fastest way to get set up

3/5 Steps Completed

The Essentials

Bring some users into Okta

Bring in some users from Active Directory or LDAP. If you just want to test the function, only bring in a few users.

Use single sign on

Let users access an app from their Okta dashboard. To do this, we'll add your first app integration.

Add another Okta admin

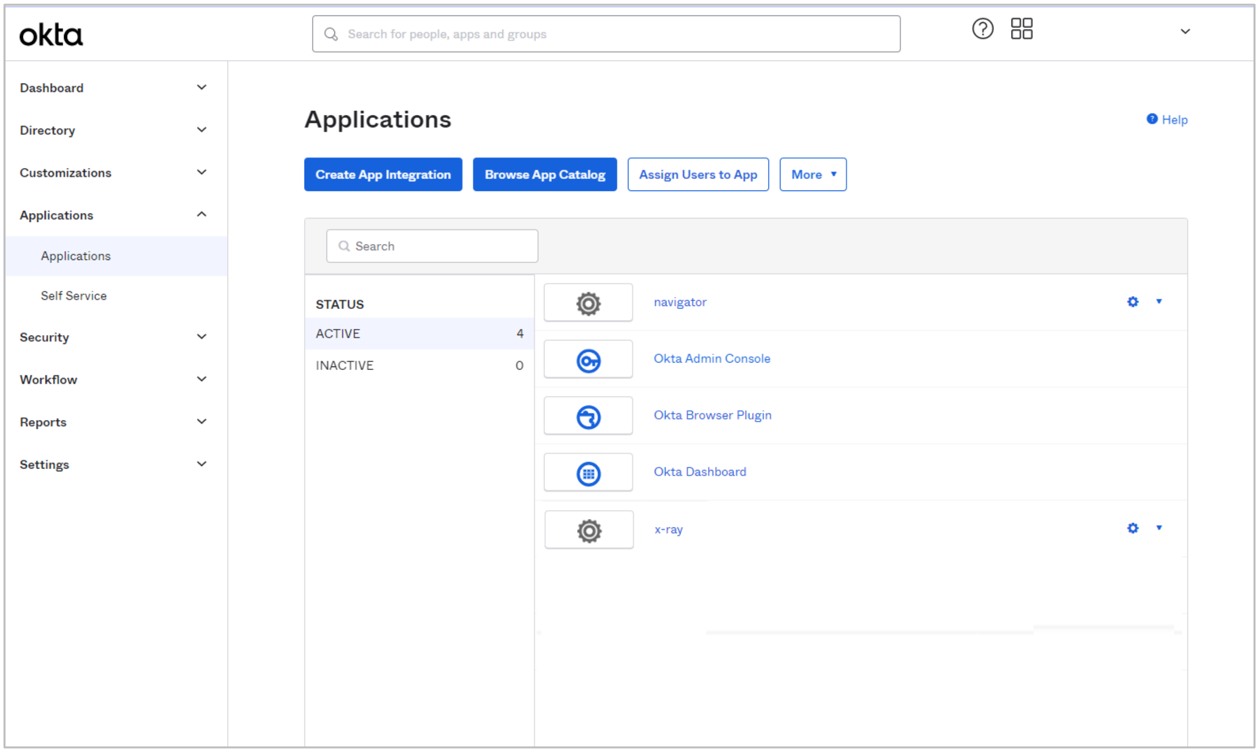
Let a colleague explore and set up Okta with you. Make one of your users an admin, and choose their permissions.

Multifactor Authentication (MFA)

Select Authenticators

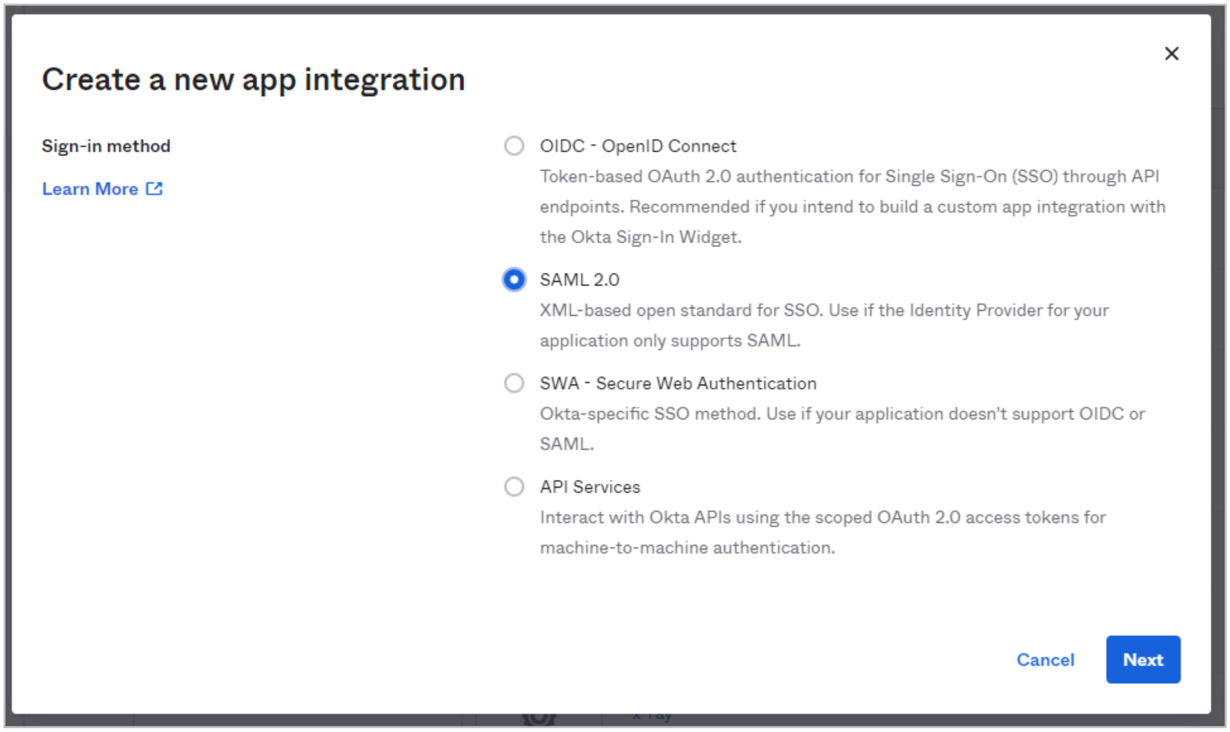
Select the Authenticators you'd like your organization to use.

3. From the left pane, select **Applications** > **Applications**.


Applications

STATUS	
ACTIVE	4
INACTIVE	0

4. Click **Create App Integration**. (Or, if you have already created an app integration, select the one you want to edit and proceed to step 6.)
5. If you chose to create an app integration, the *Create a new app integration* dialog is displayed. Select SAML 2.0 and click **Next**.



Create a new app integration

Sign-in method

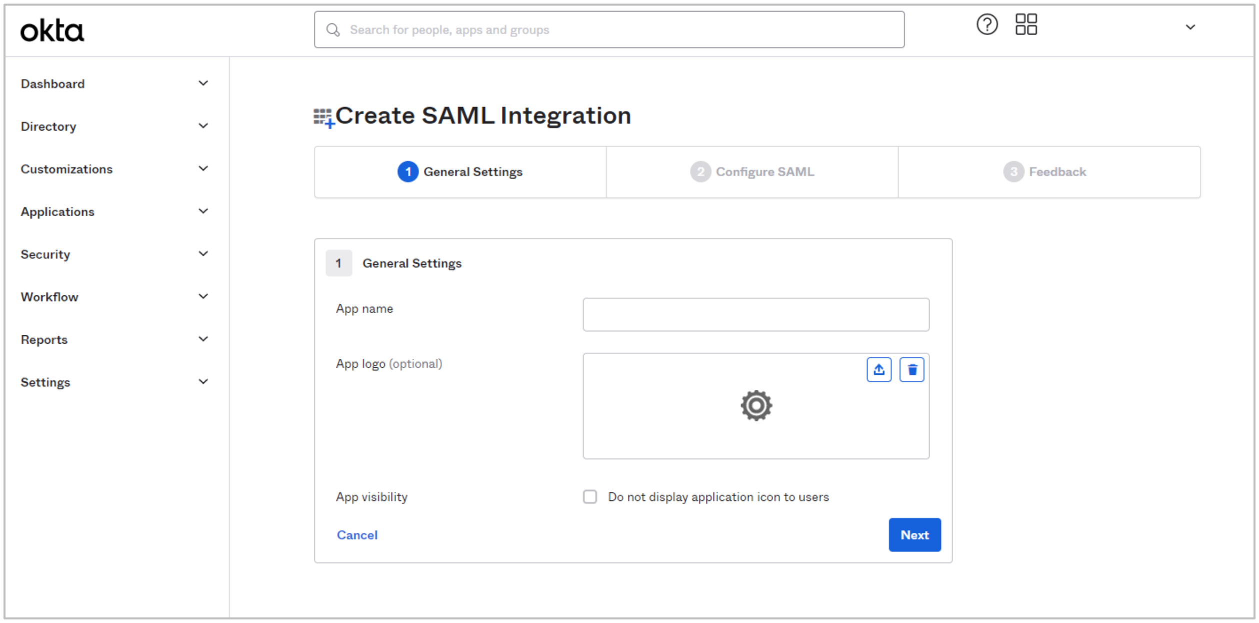
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● 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.

6. In step 1 of the Create SAML Integration process (General Settings), enter the new **App name** and click **Next**.



Create SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

1 General Settings

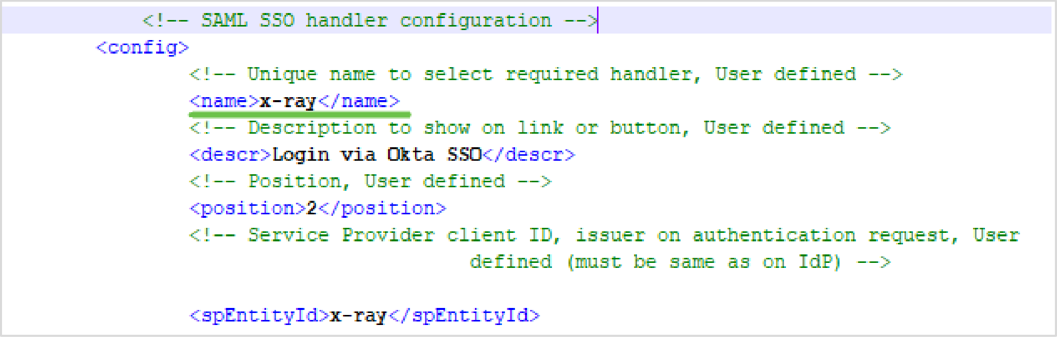
App name

App logo (optional)

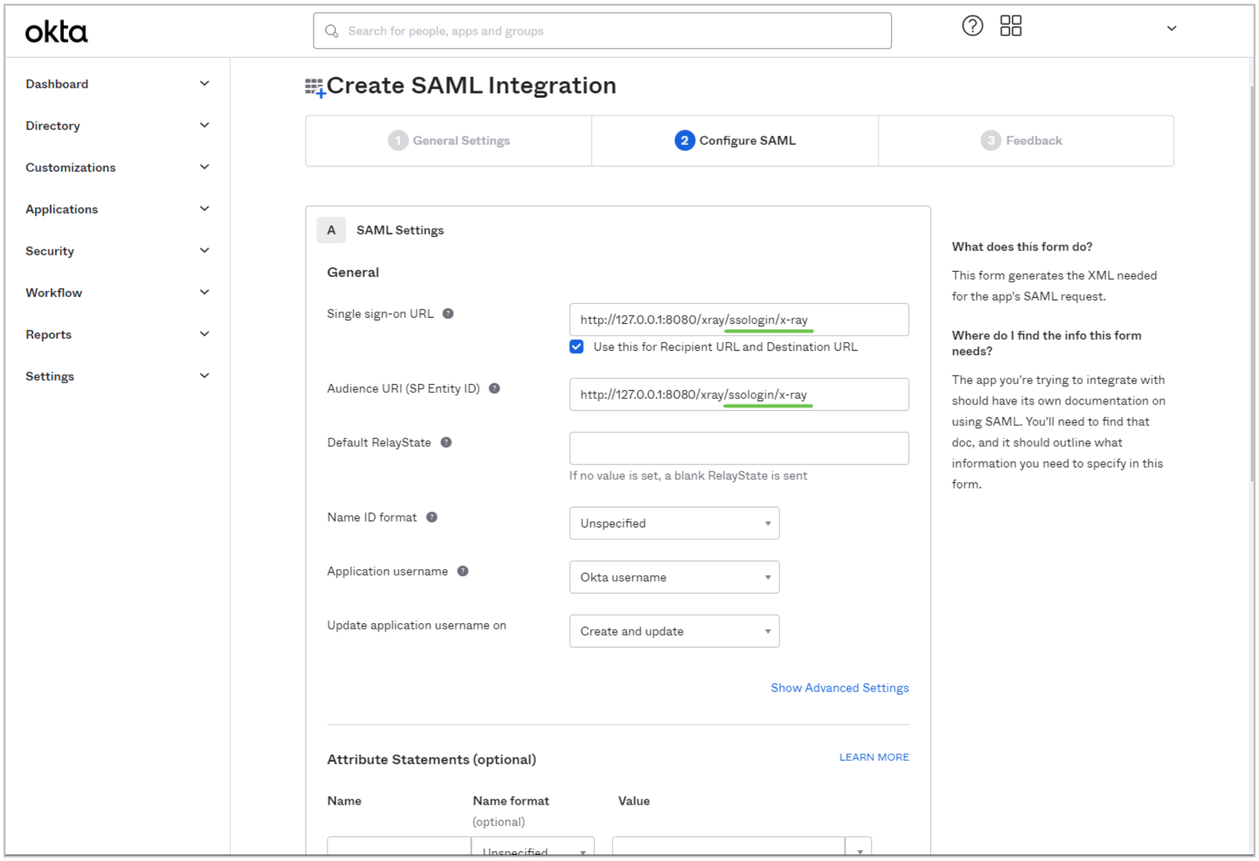
App visibility □ Do not display application icon to users

7. In step 2 (Configure SAML), enter the Single sign-on URL and fill in the **Single sign-on URL** and **Audience URI (SP Entity ID)** fields, making sure that both of these URLs end with /ssologin/{name-of-config}

ssologin is used in the login servlet. {name-of-config} is the value in the <name> parameter in the Tomcat samlsso configuration file. (The name of this file varies based on the application. See *What is Single Sign On (SSO)?* for more information.)



```
        <!-- SAML SSO handler configuration -->
    <config>
        <!-- Unique name to select required handler, User defined -->
        <name>x-ray</name>
        <!-- Description to show on link or button, User defined -->
        <descr>Login via Okta SSO</descr>
        <!-- Position, User defined -->
        <position>2</position>
        <!-- Service Provider client ID, issuer on authentication request, User
                        defined (must be same as on IdP) -->

        <spEntityId>x-ray</spEntityId>
```



Create SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

A SAML Settings

General

Single sign-on URL	http://127.0.0.1:8080/xray/ssologin/x-ray
	☑ Use this for Recipient URL and Destination URL
Audience URI (SP Entity ID)	http://127.0.0.1:8080/xray/ssologin/x-ray
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

Show Advanced Settings

Attribute Statements (optional) LEARN MORE

Name	Name format (optional)	Value
	Unspecified	

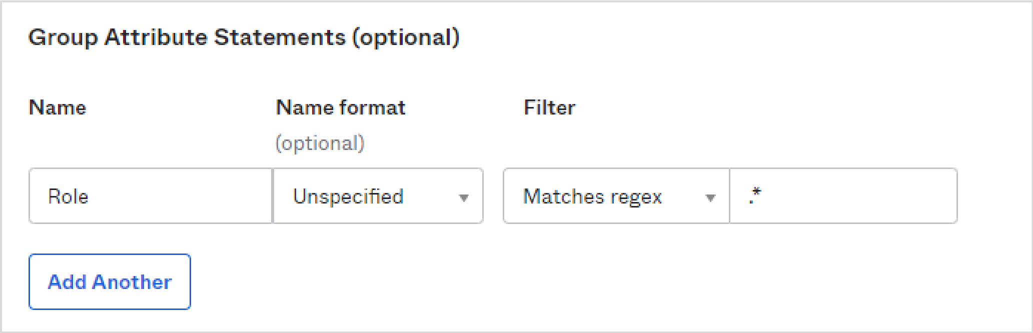
What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

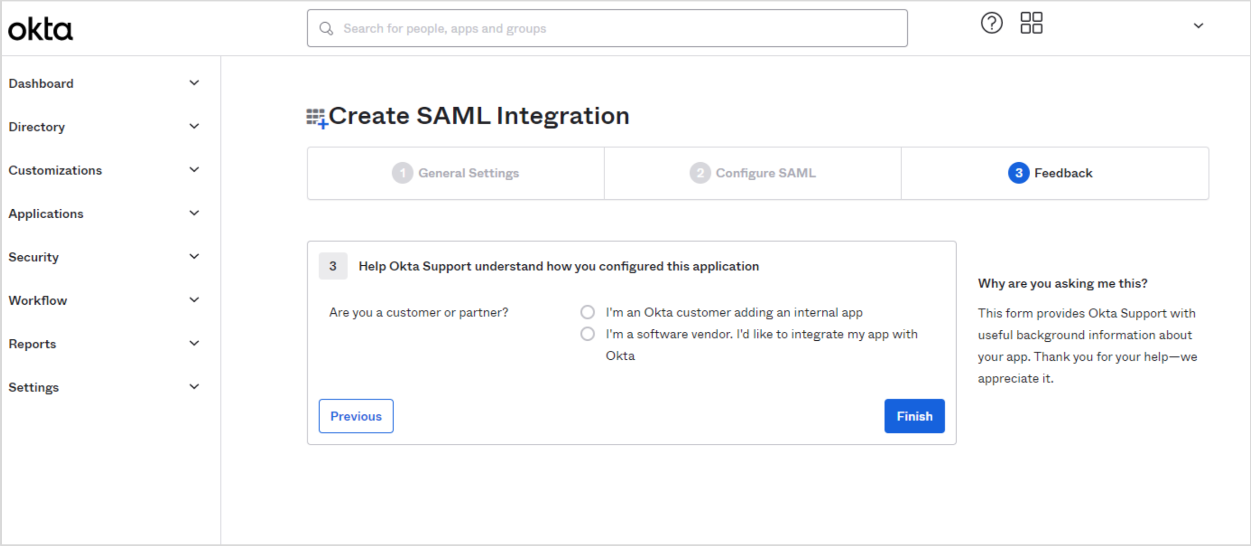
8. On the same page, fill in the **Group Attribute Statements (optional)** section as follows:
   - In the **Name** field, enter "Role".
   - In the **Name format** field, select *Unspecified*.
   - In the **Filter** field, select *Matches Regex*.
   - In the final field, enter the regular expression ".*".



Group Attribute Statements (optional)

Name	Name format (optional)	Filter	
Role	Unspecified	Matches regex	.*

9. Click **Next**.
10. In step 3 (Feedback), select *"I'm a software vendor..."*.



3 Help Okta Support understand how you configured this application

Are you a customer or partner?

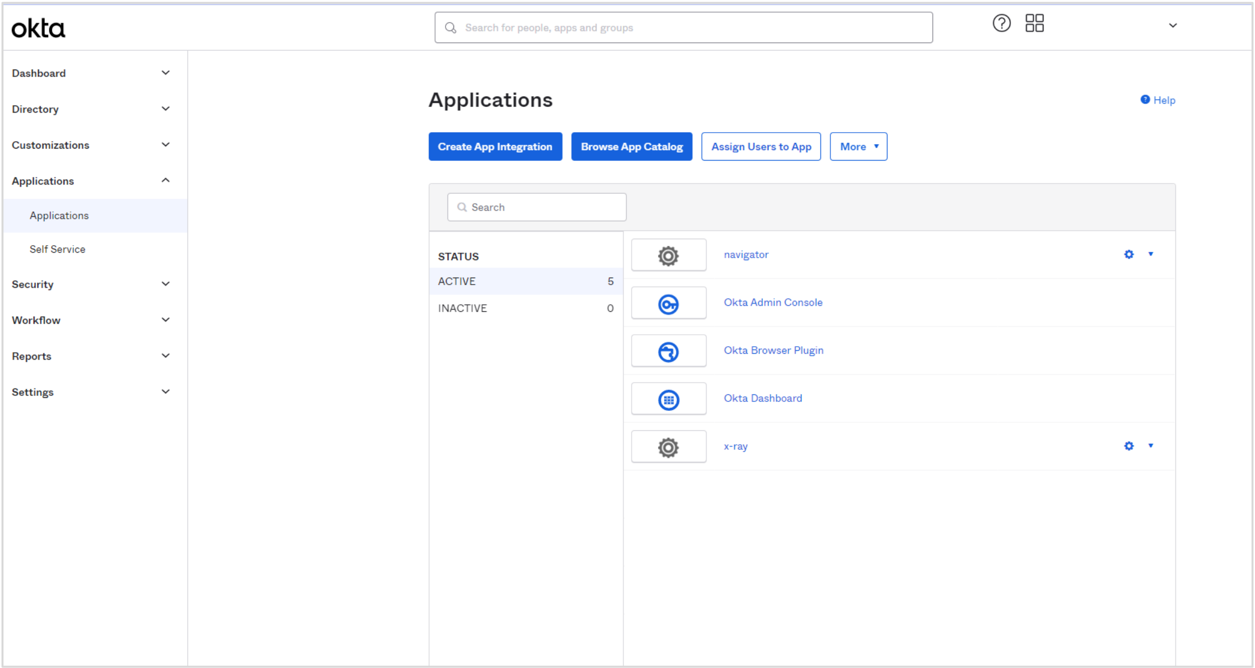
○ I'm an Okta customer adding an internal app
○ I'm a software vendor. I'd like to integrate my app with Okta

Why are you asking me this?

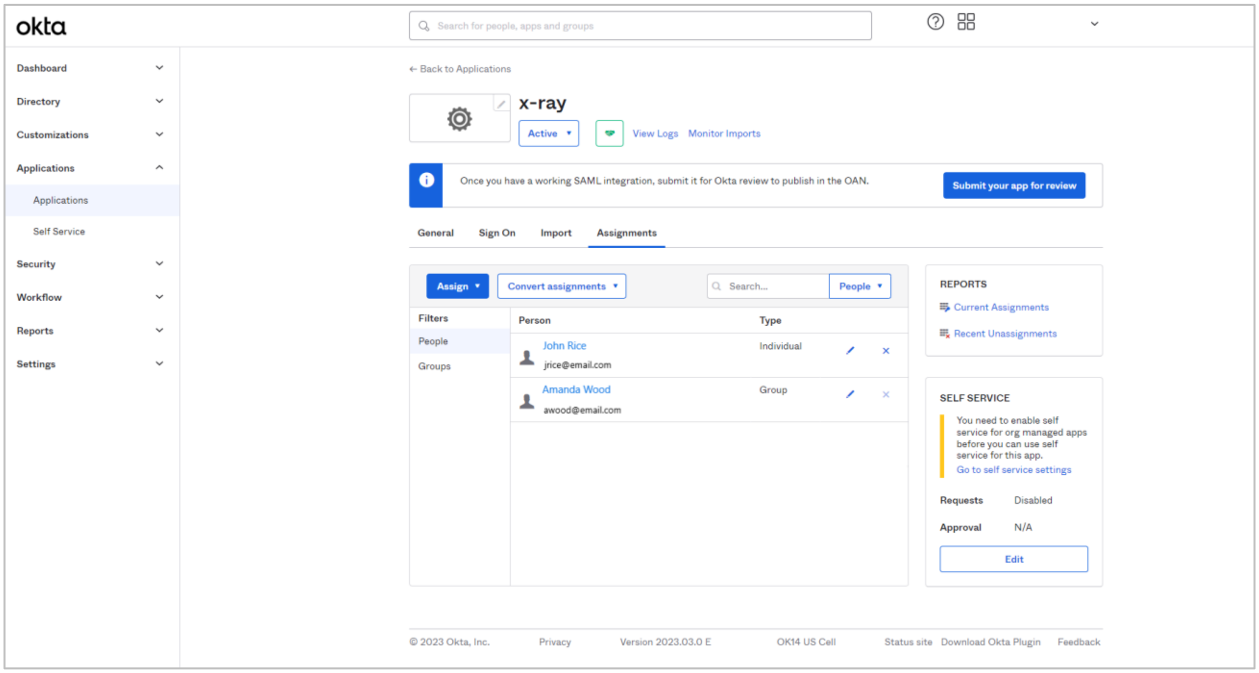
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

11. Click **Finish**.

12. To find the configuration settings that need to be set in the Tomcat samlsso configuration file, first select the application you are setting up from the list of applications:



The **Assignments** tab is displayed:



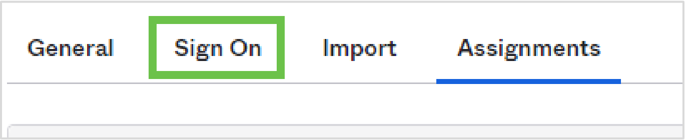
Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

Person	Type
John Rice jrice@email.com	Individual
Amanda Wood awood@email.com	Group

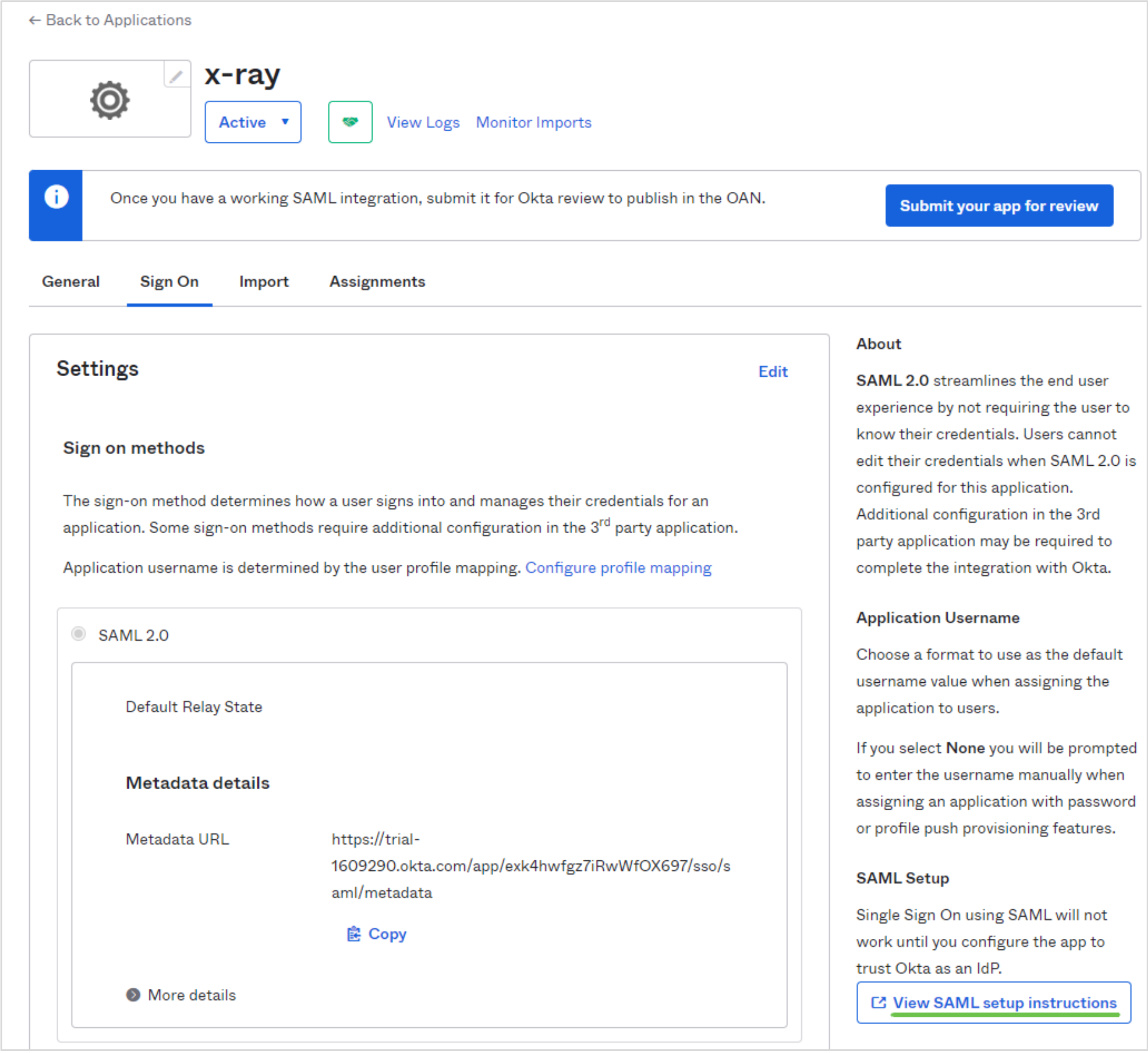
You need to enable self service for org managed apps before you can use self service for this app.
Go to self service settings

Requests	Disabled
Approval	N/A

13. Select the **Sign On** tab.



14. Select the **View SAML setup instructions** link in the lower-right corner.



Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

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-1609290.okta.com/app/exk4hwfgz7iRwWfOX697/sso/saml/metadata

● More details

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

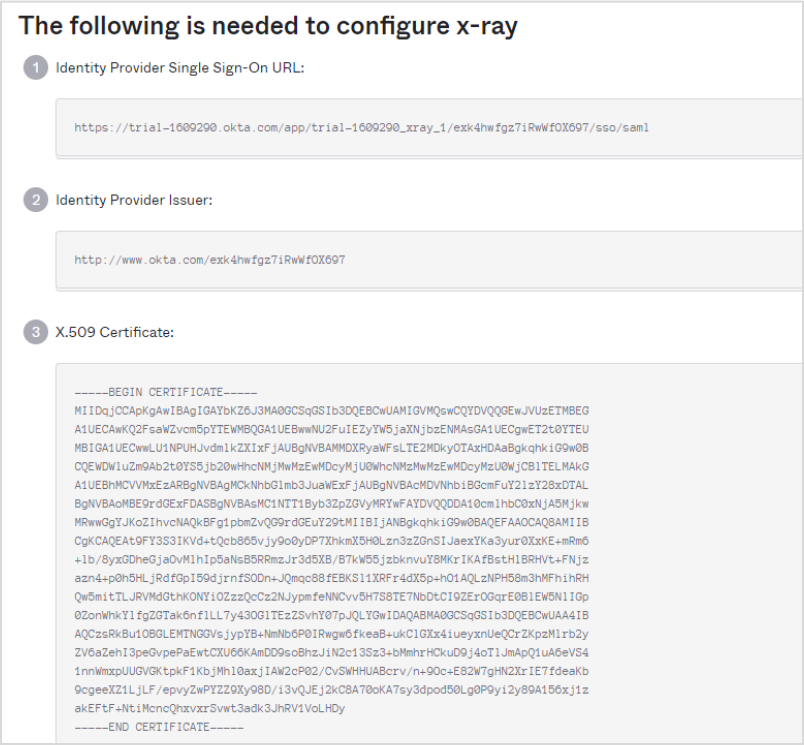
SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

The three fields provided under **The following is needed to configure x-ray** correspond to the xml parameters below. Continue on to the Important Configuration Parameters section below.

Table 2 Okta Parameter Mapping

Okta The following is needed to configure x-ray setup page	XML Parameter
1. Identity Provider Single Sign-On URL	used in idpSsoServiceUrl, idpArtifactResolveServiceUrl and idpSloServiceUrl
2. Identity Provider Issuer	idpEntityId
3. X.509 Certificate	idpSignCert



The following is needed to configure x-ray

1 Identity Provider Single Sign-On URL:

```
https://trial-1609290.okta.com/app/trial-1609290_xray_1/exk4hwfgz7iRwWfOX697/sso/saml
```

2 Identity Provider Issuer:

```
http://www.okta.com/exk4hwfgz7iRwWfOX697
```

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDqjCCApKgAwIBAgIGAYbKZ6J3MA0GCSqGSIb3DQEBCwUAMIGVMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDXRyaWFsLTE2MDkyOTAxHDAaBgkqhkiG9w0B
CQEWDWluZm9Ab2t0YS5jb20wHhcNMjMwMzEwMDcyMjU0WhcNMzMwMzEwMDcyMzU0WjCBlTELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTAL
BgNVBAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRYwFAYDVQQDDA10cmlhbC0xNjA5Mjkw
MRwwGgYJKoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAt9FY3S3IKVd+tQcb865vjy9o0yDP7XhkmX5H0Lzn3zZGnSIJaexYKa3yur0XxKE+mRm6
+lb/8yxGDheGjaOvMlhIp5aNsB5RRmzJr3d5XB/B7kW55jzbknvuY8MKrIKAfBstHlBRHVt+FNjz
azn4+p0h5HLjRdfGpI59djrnfSODn+JQmqc88fEBKSl1XRFr4dX5p+hO1AQLzNPH58m3hMFhihRH
Qw5mitTLJRVMdGthKONYiOZzzQcCz2NJypmfeNNCvv5H7S8TE7NbDtCI9ZErOGqrE0BlEW5NlIGp
0ZonWhkYlfgZGTak6nflLL7y43OGlTEzZSvhY07pJQLYGwIDAQABMA0GCSqGSIb3DQEBCwUAA4IB
AQCzsRkBu1OBGLEMTNGGVsjypYB+NmNb6P0IRwgw6fkeaB+ukClGXx4iueyxnUeQCrZKpzMlrb2y
ZV6aZehI3peGvpePaEwtCXU66KAmDD9soBhzJiN2c13Sz3+bMmhrHCkuD9j4oTlJmApQ1uA6eVS4
1nnWmxpUUGVGKtpkF1KbjMhl0axjIAW2cP02/CvSWHHUABcrv/n+9Oc+E82W7gHN2XrIE7fdeaKb
9cgeeXZ1LjLF/epvyZwPYZZ9Xy98D/i3vQJEj2kC8A70oKA7sy3dpod50Lg0P9yi2y89A156xj1z
akEFtF+NtiMcncQhxvxrSvwt3adk3JhRV1VoLHDy
-----END CERTIFICATE-----
```

3.2 Important Configuration Parameters (XRay Example)

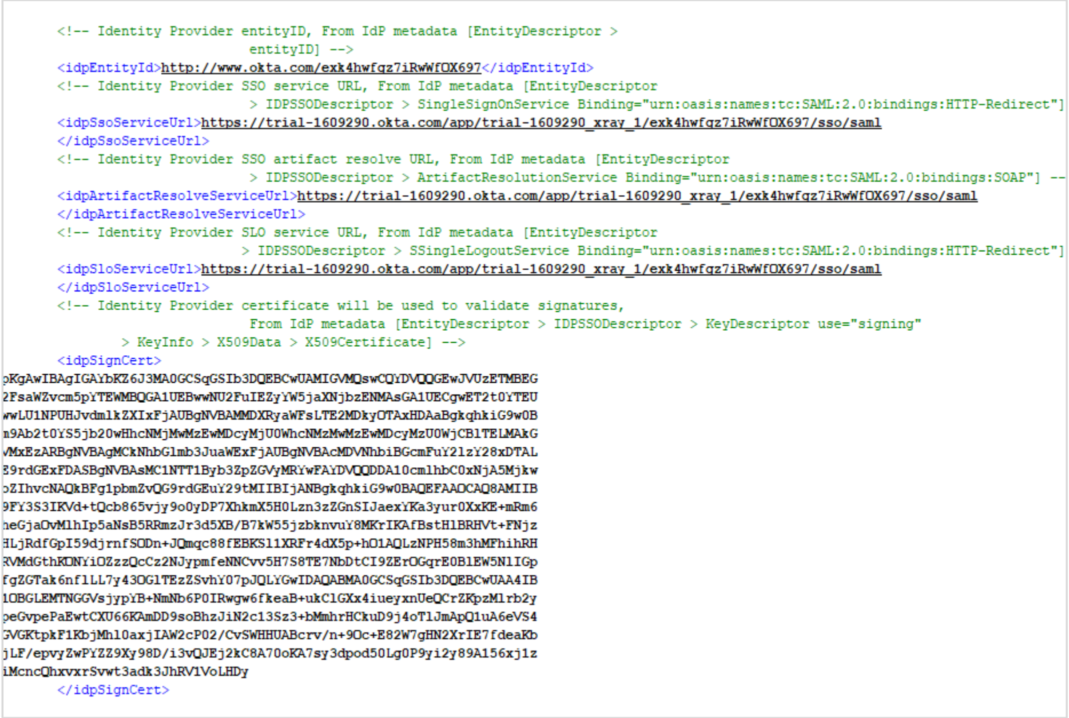
3.2.1 For Service Providers

spEntityId – Specify the name of the service provider. To better keep track of service providers, you might consider using the **App name** from step 1 of the Create SAML Integration process. However, it is not required that these two names be the same.

3.2.2 For Identity Providers

IdpEntityId, *idpSsoServiceUrl*, *idpArtifactResolveServiceUrl* and *idpSloServiceUrl*

Enter the parameters from step 14 of Okta Identity Provider Configuration in the Tomcat samlsso configuration file, as shown below:



```
        <!-- Identity Provider entityID, From IdP metadata [EntityDescriptor >
                                entityID] -->
        <idpEntityId>http://www.okta.com/exk4hwfqz7iRwWfOX697</idpEntityId>
        <!-- Identity Provider SSO service URL, From IdP metadata [EntityDescriptor
                                > IDPSSODescriptor > SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"]
        <idpSsoServiceUrl>https://trial-1609290.okta.com/app/trial-1609290_xray_1/exk4hwfqz7iRwWfOX697/sso/saml
        </idpSsoServiceUrl>
        <!-- Identity Provider SSO artifact resolve URL, From IdP metadata [EntityDescriptor
                                > IDPSSODescriptor > ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"] --
        <idpArtifactResolveServiceUrl>https://trial-1609290.okta.com/app/trial-1609290_xray_1/exk4hwfqz7iRwWfOX697/sso/saml
        </idpArtifactResolveServiceUrl>
        <!-- Identity Provider SLO service URL, From IdP metadata [EntityDescriptor
                               > IDPSSODescriptor > SSingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"]
        <idpSloServiceUrl>https://trial-1609290.okta.com/app/trial-1609290_xray_1/exk4hwfqz7iRwWfOX697/sso/saml
        </idpSloServiceUrl>
        <!-- Identity Provider certificate will be used to validate signatures,
                                From IdP metadata [EntityDescriptor > IDPSSODescriptor > KeyDescriptor use="signing"
                > KeyInfo > X509Data > X509Certificate] -->
        <idpSignCert>
pKgAwIBAgIGAYbKZ6J3MA0GCSqGSIb3DQEBCwUAMIGVMQswCQYDVQQGEwJVUzETMBEG
2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
wwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDXRyaWFsLTE2MDkyOTAxHDAaBgkqhkiG9w0B
n9Ab2t0YS5jb20wHhcNMjMwMzEwMDcyMjU0WhcNMzMwMzEwMDcyMzU0WjCBlTELMAkG
VMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTAL
E9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRYwFAYDVQQDDA10cmlhbC0xNjA5Mjkw
oZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
9FY3S3IKVd+tQcb865vjy9o0yDP7XhkmX5H0Lzn3zZGnSIJaexYKa3yur0XxKE+mRm6
heGjaOvMlhIp5aNsB5RRmzJr3d5XB/B7kW55jzbknvuY8MKrIKAfBstHlBRHVt+FNjz
HLjRdfGpI59djrnfSODn+JQmqc88fEBKSl1XRFr4dX5p+hO1AQLzNPH58m3hMFhihRH
RVMdGthKONYiOZzzQcCz2NJypmfeNNCvv5H7S8TE7NbDtCI9ZErOGqrE0BlEW5NlIGp
fgZGTak6nflLL7y43OGlTEzZSvhY07pJQLYGwIDAQABMA0GCSqGSIb3DQEBCwUAA4IB
1OBGLEMTNGGVsjypYB+NmNb6P0IRwgw6fkeaB+ukClGXx4iueyxnUeQCrZKpzMlrb2y
peGvpePaEwtCXU66KAmDD9soBhzJiN2c13Sz3+bMmhrHCkuD9j4oTlJmApQ1uA6eVS4
GVGKtpkF1KbjMhl0axjIAW2cP02/CvSWHHUABcrv/n+9Oc+E82W7gHN2XrIE7fdeaKb
jLF/epvyZwPYZZ9Xy98D/i3vQJEj2kC8A70oKA7sy3dpod50Lg0P9yi2y89A156xj1z
iMcncQhxvxrSvwt3adk3JhRV1VoLHDy
        </idpSignCert>
```

3.3 Sample xray_samlsso.xml file using Okta

```
<!-- SAML SSO handlers configurations  -->
<configs>
<!-- SAML SSO handler configuration -->
    <config>
<!-- Unique name to select required handler, User defined -->
        <name>xray-okta</name>
      <!-- Description to show on link or button, User defined -->
        <descr>Login via Okta SSO</descr>
      <!-- Image can be added /image/path/img.* By default it will display an icon -->
       <!-- <buttonIcon>image.png</buttonIcon>-->
      <!-- Button or link text (name), User defined -->
        <buttonText>Okta login</buttonText>
<!-- Color code for button background(#FFFFFF-white #000000-black), User defined -->
        <buttonColor>#ffffff</buttonColor>
      <!-- Position, User defined -->
        <position>3</position>


      <!-- Service Provider client ID, issuer on authentication request, User
                  defined (must be same as on IdP) -->
        <spEntityId>xray-okta</spEntityId>


      <!-- Identity Provider entityID, From IdP metadata [EntityDescriptor > entityID] -->
        <idpEntityId>http://www.okta.com/exk4fzbq289dgiTH5697</idpEntityId>
      <!-- Identity Provider SSO service URL, From IdP metadata [EntityDescriptor
                  > IDPSSODescriptor > SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->
        <idpSsoServiceUrl>https://trial-1609290.okta.com/app/trial-
1609290_ssotest_1/exk4fzbq289dgiTH5697/sso/saml
        </idpSsoServiceUrl>
      <!-- Identity Provider SSO artifact resolve URL, From IdP metadata [EntityDescriptor
                  > IDPSSODescriptor > ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"] -->
        <idpArtifactResolveServiceUrl>https://trial-1609290.okta.com/app/trial-
1609290_ssotest_1/exk4fzbq289dgiTH5697/sso/saml
        </idpArtifactResolveServiceUrl>
      <!-- Identity Provider SLO service URL, From IdP metadata [EntityDescriptor
                 > IDPSSODescriptor > SSingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->
        <idpSloServiceUrl>https://trial-1609290.okta.com/app/trial-
1609290_ssotest_1/exk4fzbq289dgiTH5697/sso/saml
        </idpSloServiceUrl>
        <!-- Identity Provider certificate will be used to validate signatures,
                  From IdP metadata [EntityDescriptor > IDPSSODescriptor > KeyDescriptor use="signing"
          > KeyInfo > X509Data > X509Certificate] -->
        <idpSignCert>
```

```
MIIDqjCCApKgAwIBAgIGAYa2+1N1MA0GCSqGSIb3DQEBCwUAMIGVMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAs
GA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDXRyaWFsLTE2
MDkyOTAxHDAaBgkqhkiG9w0BCQEWDWluZm9Ab2t0YS5jb20wHhcNMjMwMzA2MTI1MTQ
5WhcNMzMwMzA2MTI1MjQ5WjCBlTELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb
3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTALBgNVBAoMBE9rdGExFDASBgNVBAs
MC1NTT1Byb3ZpZGVyMRYwFAYDVQQDDA10cmlhbC0xNjA5MjkwMRwwGgYJKoZIhvcNAQk
BFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqoGMSk
n0dv3obE+XQ8eMcfOVLiuxlHxEgdpw/ANXWui9gUi+jaDT98HSYIIOWxpalVVdWuOiHNK6wri8
HyVcXm1m3Mk2EXmCBSb8dj426XD2ex14KfbPuZ0fejCLnIoTDivWKH8E2lkB9ZQqPxpNUJc5t
6wRdWxajtTneNaNt/42QbJ9K93hnxp5K7R8J3XRFXePArkadCYe0Z6+ipG82YbnMK6ewcEN0Q
C6GlbqSIjwYvWk+xS7/0X2qGThn4ZxFFNGAx8n0g4LPovvTEVOFS2hBXQLrQbrEumlI9TvDs//s
R3hMWwb+VbBDHHYCpxAF/BkIAHhE9UsjOOkFtQECQIDAQABMA0GCSqGSIb3DQEBCwUAA
4IBAQAMeTmDDgKmLZIiiXPOFwoAdQYkn7zEYTz2e1pQ5sUSUHdwKpjctuR4il0MWZxXpGQd
hs1MZIzj+U7y/Squ3On/NdV8b9yshXW6EQSVFokph8QyKXlUTJ8/fjOgBzbXkrPZj6rOjCQxn4ls/
eHQ/AKcllsqPj1ziSRAx3kuZHGG4XhrxmRfM9faYrZyeLWtHW4Iz8xcPMTv/zUAomiVcp9CsYUU
6fGJpe4Oa8hfmWRjxSSxW69xan/m6XJ1V1F41+75hewRuvTbVDgAMlT4Odxou/zamCwF7yR3
57A3cRZbI7GDI7K3m9mEBEtAd7vBJDv4Ck30b4Mef6zsqWqorzYa

            </idpSignCert>


         <!-- Service Provider must sign authentication request, User defined -->

            <authnRequestSigned>true</authnRequestSigned>

         <!-- Service Provider must sign artifact resolve request, User defined -->

            <resolveArtifactRequestSigned>true</resolveArtifactRequestSigned>

         <!-- Service Provider must sign logout request, User defined -->

            <logoutRequestSigned>true</logoutRequestSigned>


      </config>


</configs>
```

3.4 Sample apwmq_samlsso.xml file using Okta

```
  <!-- SAML SSO handler configuration -->

         <configs>

      <config>

         <!-- Unique name to select required handler, User defined -->

            <name>navigator</name>

         <!-- Description to show on link or button, User defined -->

            <descr>Login via Okta SSO</descr>
```

```
        <!-- Position, User defined -->
          <position>2</position>
        <!-- Service Provider client ID, issuer on authentication request, User
                    defined (must be same as on IdP) -->
          <spEntityId>navigator-okta</spEntityId>
        <!-- Service Provider certificate will be used to sign requests or decrypt
                    assertion, User defined (must be same as on IdP) -->


        <!-- Identity Provider entityID, From IdP metadata [EntityDescriptor >
                    entityID] -->
          <idpEntityId>http://www.okta.com/exk8tr000xGFbYLVX5d7</idpEntityId>
        <!-- Identity Provider SSO service URL, From IdP metadata [EntityDescriptor
                    > IDPSSODescriptor > SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->
          <idpSsoServiceUrl>https://dev-03395477.okta.com/app/dev-
03395477_navigator_1/exk8tr000xGFbYLVX5d7/sso/saml
          </idpSsoServiceUrl>
        <!-- Identity Provider SSO artifact resolve URL, From IdP metadata [EntityDescriptor
                    > IDPSSODescriptor > ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"] -->
          <idpArtifactResolveServiceUrl>https://dev-03395477.okta.com/app/dev-
03395477_navigator_1/exk8tr000xGFbYLVX5d7/sso/saml
          </idpArtifactResolveServiceUrl>
        <!-- Identity Provider SLO service URL, From IdP metadata [EntityDescriptor
                    > IDPSSODescriptor > SSingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->
          <idpSloServiceUrl>https://dev-03395477.okta.com/app/dev-
03395477_navigator_1/exk8tr000xGFbYLVX5d7/sso/saml
          </idpSloServiceUrl>
        <!-- Identity Provider certificate will be used to validate signatures,
                    From IdP metadata [EntityDescriptor > IDPSSODescriptor > KeyDescriptor use="signing"
          > KeyInfo > X509Data > X509Certificate] -->
          <idpSignCert>
MIIDqDCCApCgAwIBAgIGAYcNpg1/MA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAs
GA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi0wMzM5
NTQ3NzEcMBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTAeFw0yMzAzMjMwODQ1Mzh
aFw0zMzAzMjMwODQ2MzhaMIGUMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZv
cm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEUMBIGA1UE
```

```
CwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi0wMzM5NTQ3NzEcMBoGCSqGSIb3DQEJA
RYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI5zkk
PCKFx0rLZL8qdHwonQSHUIq9K4lyPAbWieBnKMdIWcPXSUGCtUFqUpKwzQOnPGOhKnMtri
826UlZ/Hoju7tvVqrbC03E5a59DPLeznBn/Byr/6UIpUs3xLTN+1GUP1HASiDq/a7SxZ+9S60y0x
Vlomx7rBsuJdt9N40IqIqT5Y+6w5zDkLy8LW9fMZVga1c72bPOaqc6WDRXfECWmXzRo0JCmyX
11E8po5z+KLJa8fHSIbAT4RW0p/0YDyoI59NwtzRayI3LzhV/5lHTNeFNmFPDziBP35sCc1hD9M
c7PIqfxPp0xKKEqHObrW4f+VucynuetTrSRY0xzakZcCAwEAATANBgkqhkiG9w0BAQsFAAOCA
QEATvemmBRocEShEWv/uXEiGBVdsvmWVpMA6JLWczEg/CaLqYmrckIrsfL7xhiq1CpBr7luR8y
W/ukaQVToSZXcGEAnUo/Fp5KSgtDGjk3HBHhHiN/1aBj7iwqFx3LuM5UN8K/6XYl7lcVmP0wM
3a8nwPex7ChxOP758egWbGpgSVLNs9WyVx/rDonSXQysy8KpVZoZUtevSgjF8bgW8dKB6kvw
DIvwHVBMJzK8gNmXOxw9Kc5T0OjgpxsrZqBHKi8bNuW7xAInbx1xhGrabqUn+jtEPc6CTEe9F
SwHkrpQgECUW9VAhiaX/nsdIsrsqohEKNofuIOfJU9ADEAb5Kku4g==

        </idpSignCert>


      <!-- Service Provider must sign authentication request, User defined -->

        <authnRequestSigned>true</authnRequestSigned>

      <!-- Service Provider must sign artifact resolve request, User defined -->

        <resolveArtifactRequestSigned>true</resolveArtifactRequestSigned>

      <!-- Service Provider must sign logout request, User defined -->

        <logoutRequestSigned>true</logoutRequestSigned>

      <!-- Image can be added /image/path/img.* By default it will display an icon -->

       <!-- <buttonIcon>image.png</buttonIcon>-->

        <buttonText>Okta login</buttonText>

        <buttonColor>#ffffff</buttonColor>

  </config>





  </configs>
```

3.5 Add Users and Groups

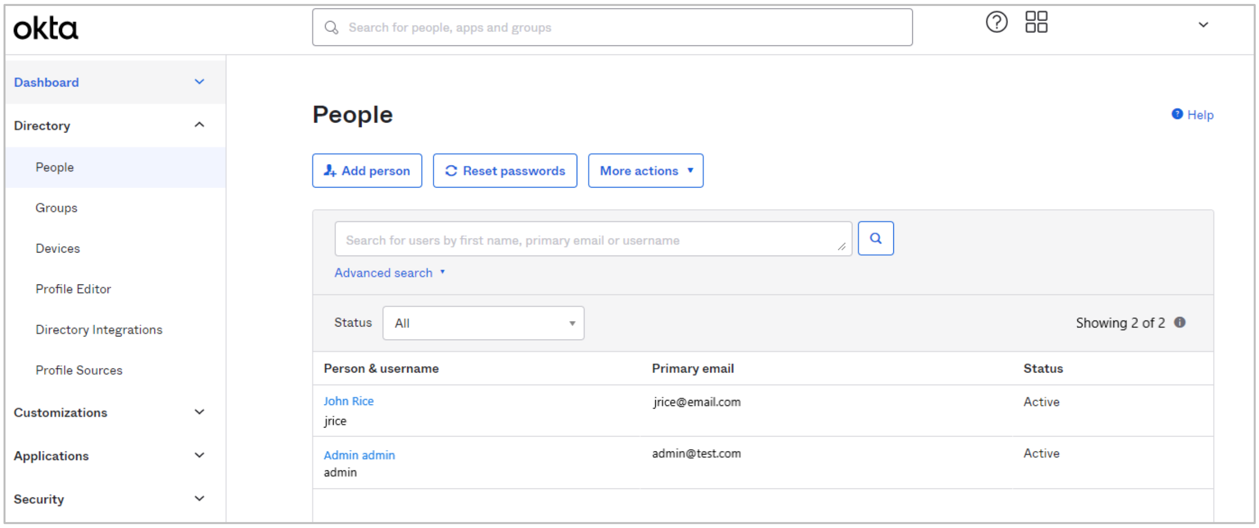
⚠ **IMPORTANT!**

When entering a username in Okta, follow these rules:

- Do not use the asterisk (@) symbol.
- Do not use an email address.
- Make sure the username contains fewer than 64 characters.

To add users or groups to the directory:

1. Expand **Directory** on the left side and select **People** or **Groups**.



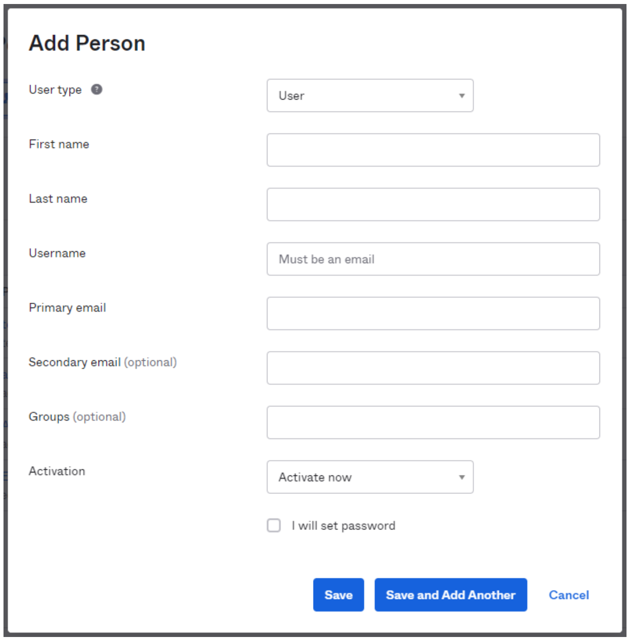
People

Status: All

Showing 2 of 2

Person & username	Primary email	Status
John Rice jrice	jrice@email.com	Active
Admin admin admin	admin@test.com	Active

2. Click **Add person**. The *Add person* dialog is displayed.



Add Person

User type	User
First name	
Last name	
Username	Must be an email
Primary email	
Secondary email (optional)	
Groups (optional)	
Activation	Activate now

□ I will set password

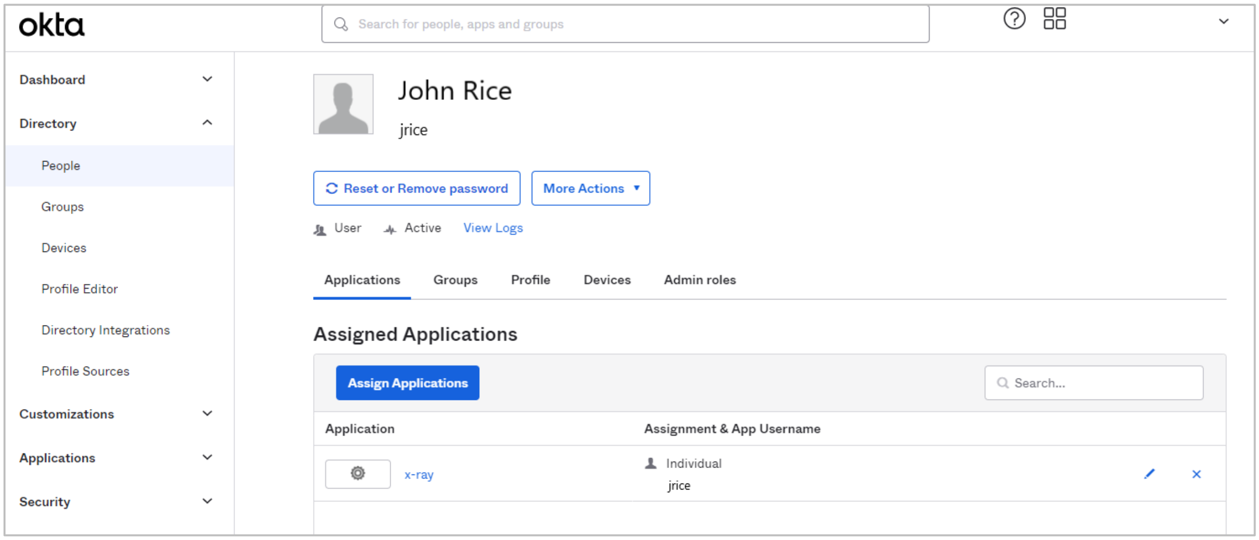
3. Fill in the dialog and click **Save**.

3.6 Assign users or groups to an application

There are two ways to add auser to application: from the user (or group) record or from an application.

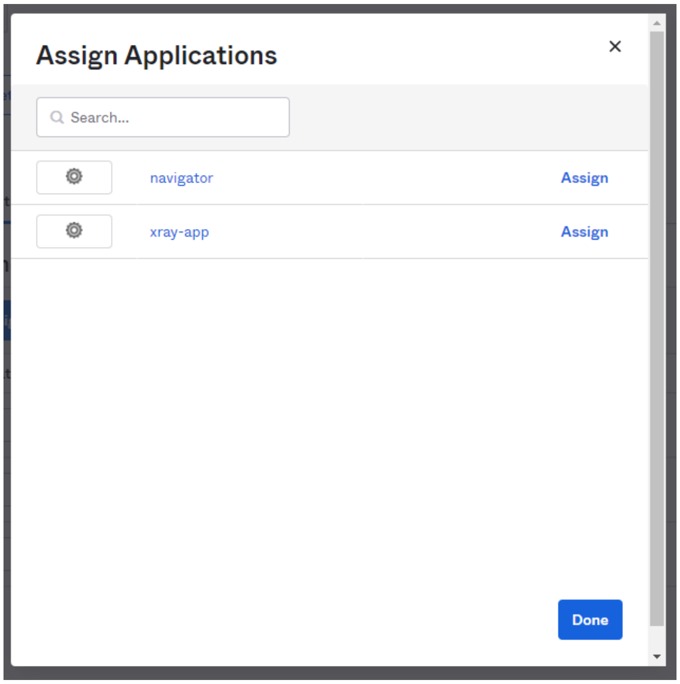
3.6.1 Assign users or groups from a user or group record

1. Expand **Directory** on the left side and select **People** or **Groups**.
2. Select the user by clicking the link in the Person and username column.



Application	Assignment & App Username
x-ray	Individual jrice

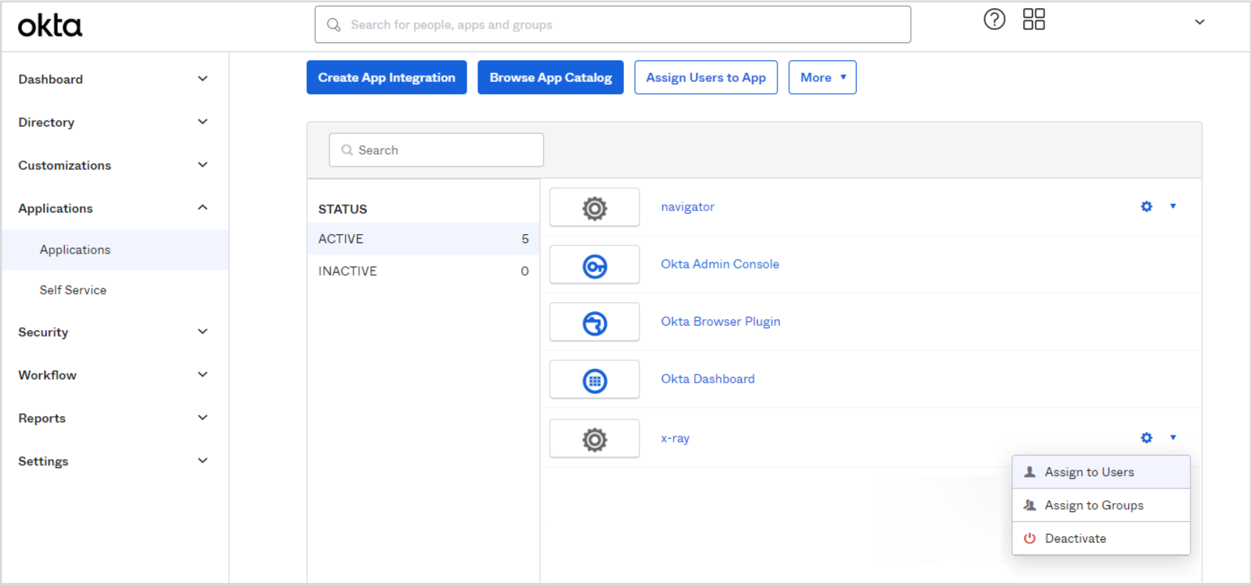
3. Click **Assign Applications**. The *Assign Applications* dialog is displayed.



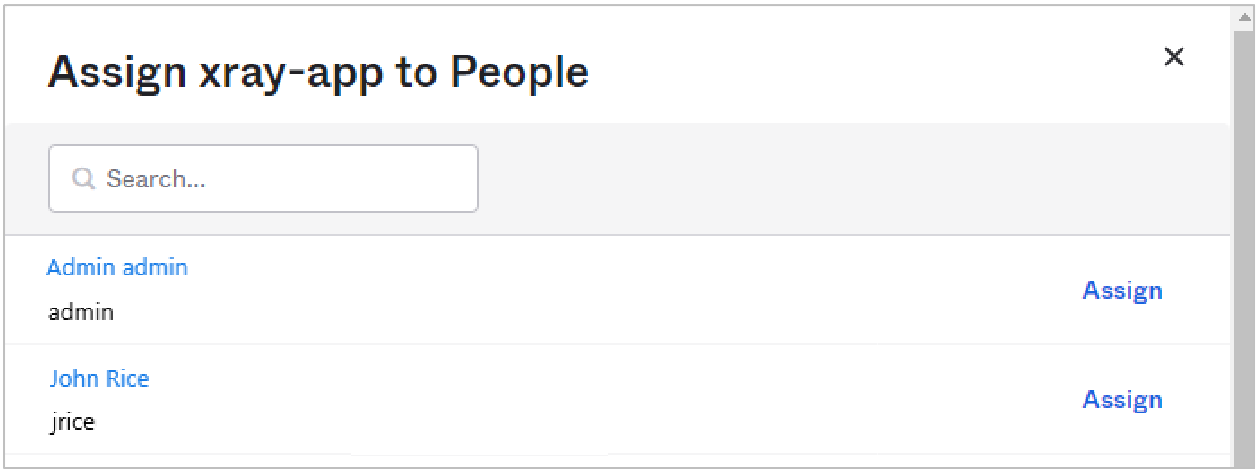
4. Click Assign for the application that you want to provide the user or group access to.
5. Click **Done**.

3.6.2 Assign users or groups from an application

1. From the left pane, select **Applications** > **Applications**.



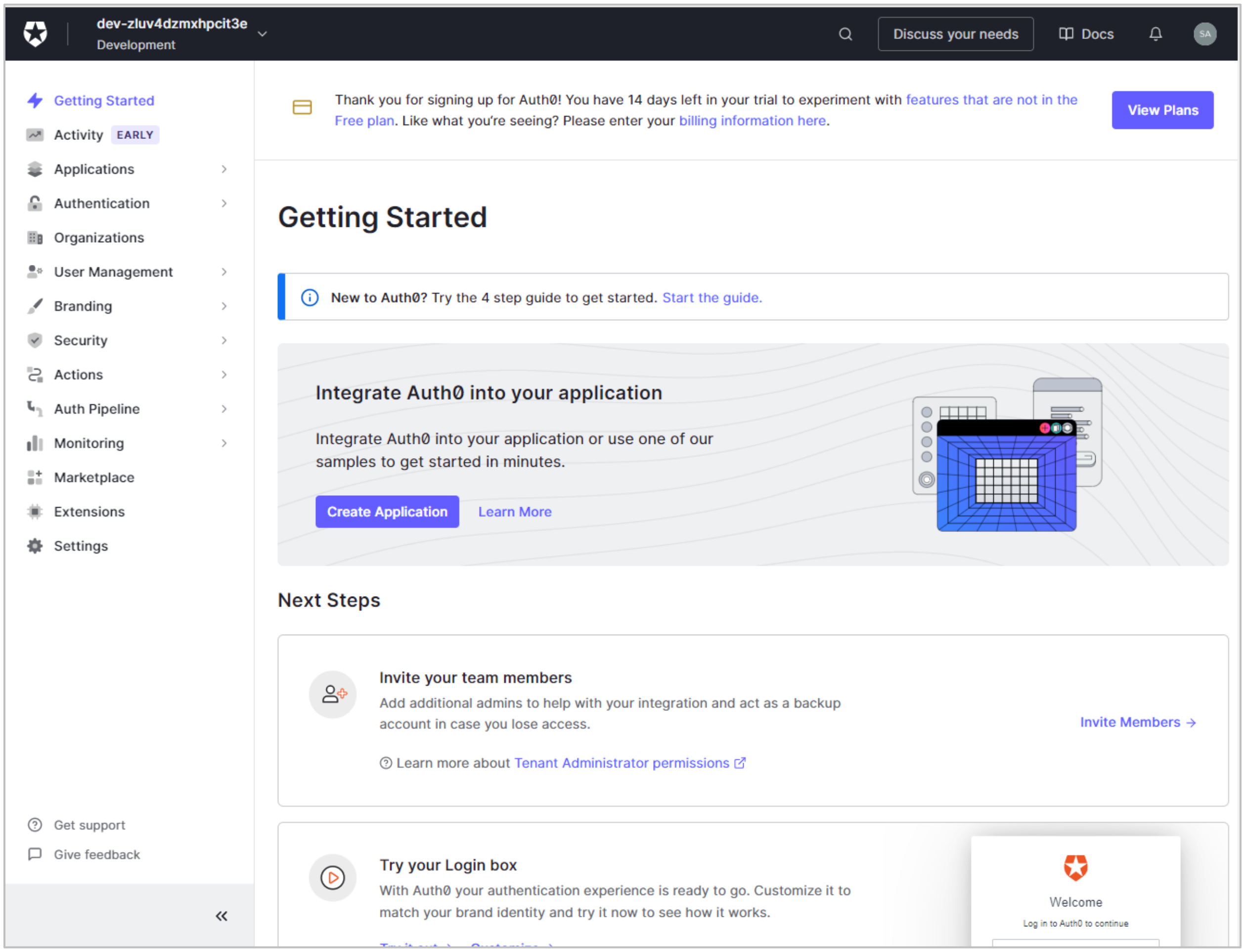
2. Click the arrow next to the settings icon for the application and select **Assign to Users** or **Assign to Groups**. The *Assign [application] to People* (or *Assign [application] to Group*) dialog is displayed.



3. Click **Assign** for each user or group for which you want to provide access to this application.
4. Click **Done**.

Chapter 4: Auth0 (Navigator Example)

When you first log into Auth0, the Getting Started page is displayed.



Thank you for signing up for Auth0! You have 14 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.

Getting Started

New to Auth0? Try the 4 step guide to get started. Start the guide.

Integrate Auth0 into your application

Integrate Auth0 into your application or use one of our samples to get started in minutes.

Next Steps

Invite your team members

Add additional admins to help with your integration and act as a backup account in case you lose access.

Learn more about Tenant Administrator permissions

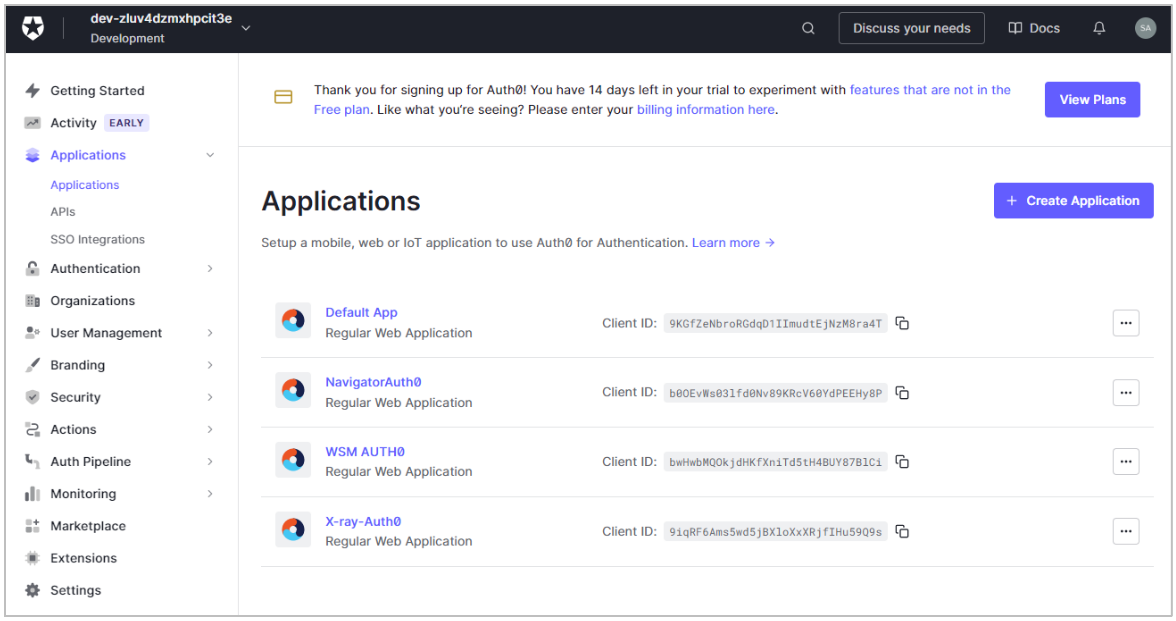
Try your Login box

With Auth0 your authentication experience is ready to go. Customize it to match your brand identity and try it now to see how it works.

4.1 Auth0 Identity Provider Configuration

First, set up the application to which you are providing SSO access through Auth0.

1. From the left pane, select **Applications**.
2. Click **+ Create Application** on the right side.



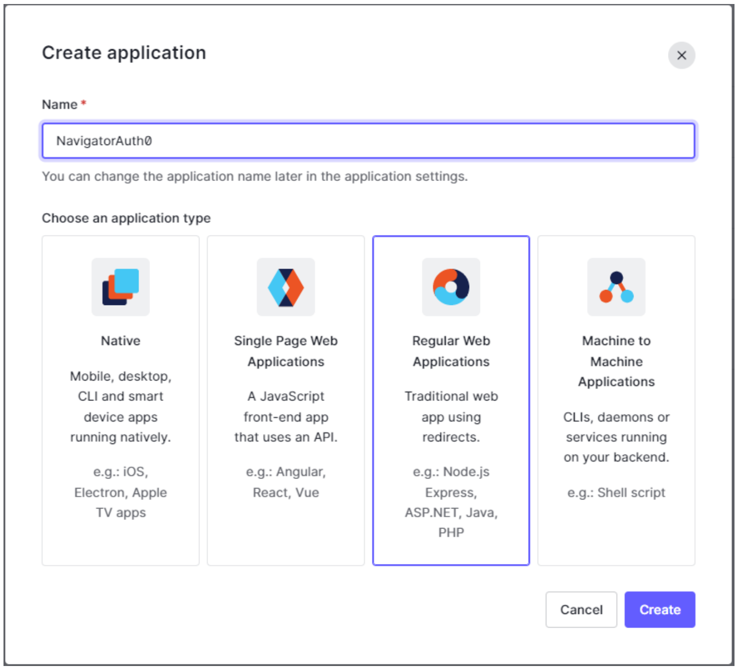
Thank you for signing up for Auth0! You have 14 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.

Applications

Setup a mobile, web or IoT application to use Auth0 for Authentication. Learn more →

Default App Regular Web Application	Client ID:	9KGfZeNbroRGdqD1IImudtEjNzM8ra4T
NavigatorAuth0 Regular Web Application	Client ID:	b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P
WSM AUTH0 Regular Web Application	Client ID:	bwHwbMQOkjdHKfXniTd5tH4BUY87BlCi
X-ray-Auth0 Regular Web Application	Client ID:	9iqRF6Ams5wd5jBXloXxXRjfIHu59Q9s

3. Enter the name of the new application and select **Regular Web Applications**.



Create application

Name *

NavigatorAuth0

You can change the application name later in the application settings.

Choose an application type

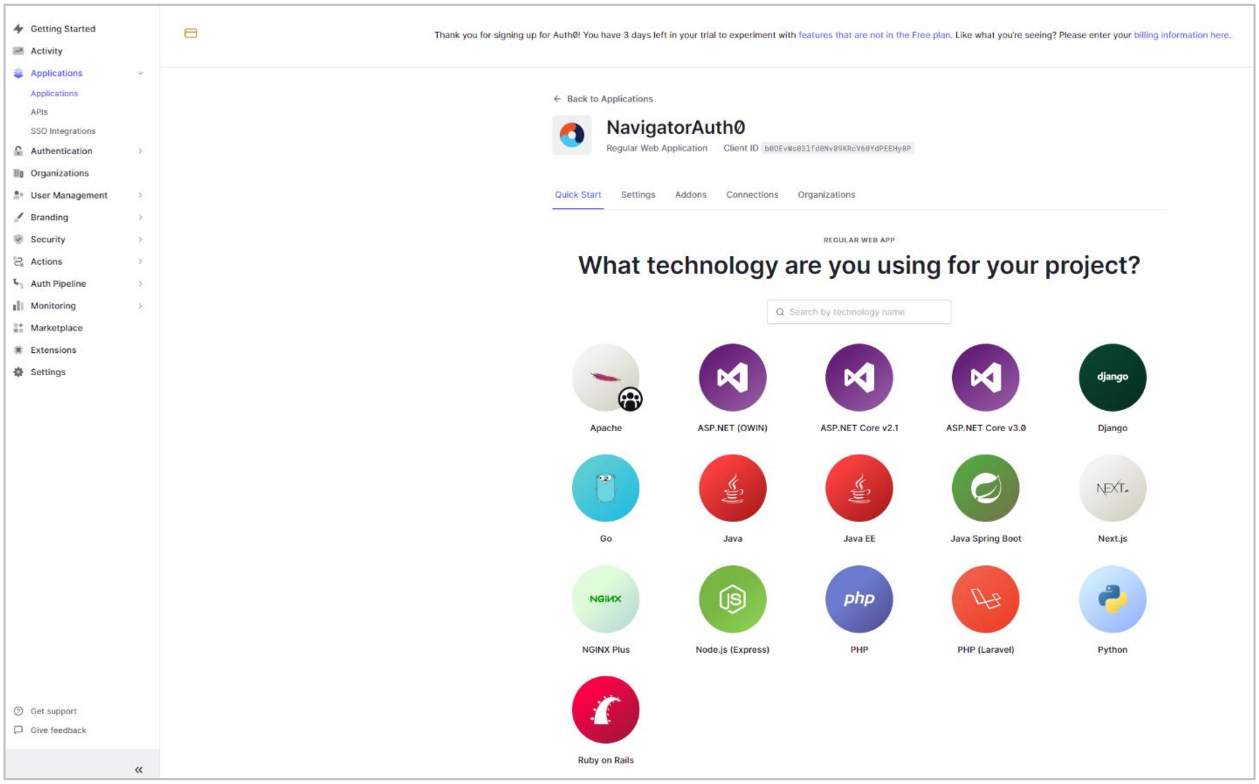
Native: Mobile, desktop, CLI and smart device apps running natively. e.g.: iOS, Electron, Apple TV apps

Single Page Web Applications: A JavaScript front-end app that uses an API. e.g.: Angular, React, Vue

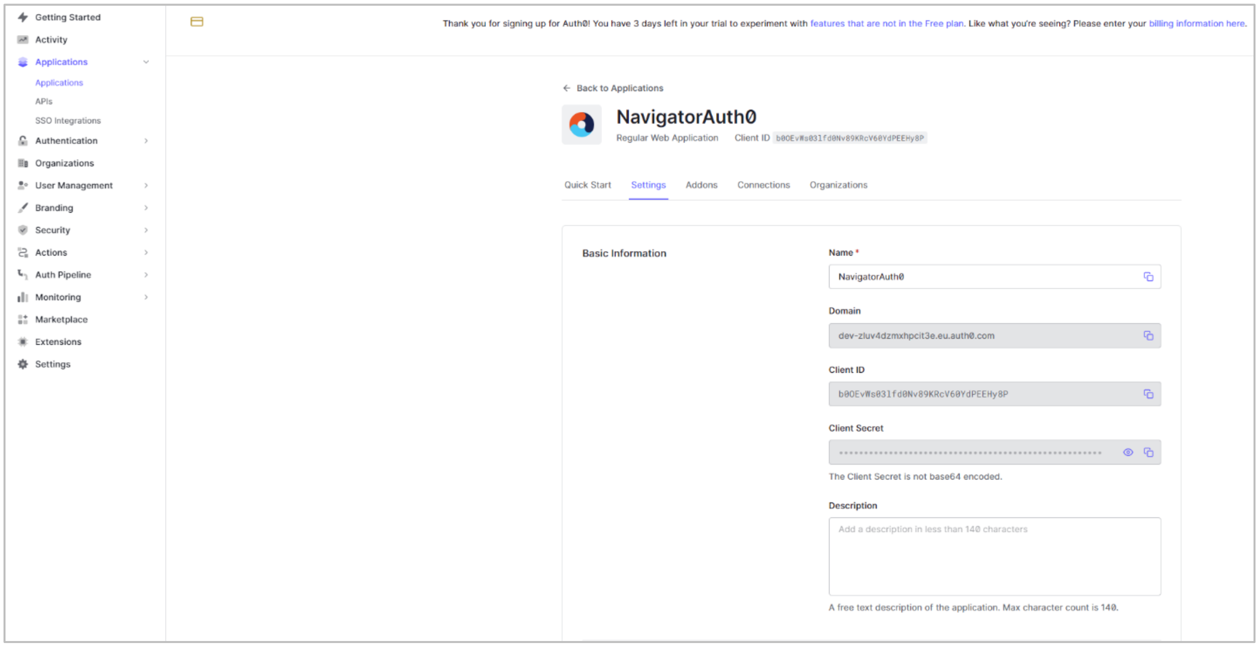
Regular Web Applications: Traditional web app using redirects. e.g.: Node.js Express, ASP.NET, Java, PHP

Machine to Machine Applications: CLIs, daemons or services running on your backend. e.g.: Shell script

4. Click **Create**. The **Quick Start** tab for the created application is displayed.



5. Select the **Settings** tab.



Basic Information

Name *
NavigatorAuth0

Domain
dev-zluv4dzmxhpcit3e.eu.auth0.com

Client ID
b0OEvWs031fd0Nv89KRcV60YdPEEHy8P

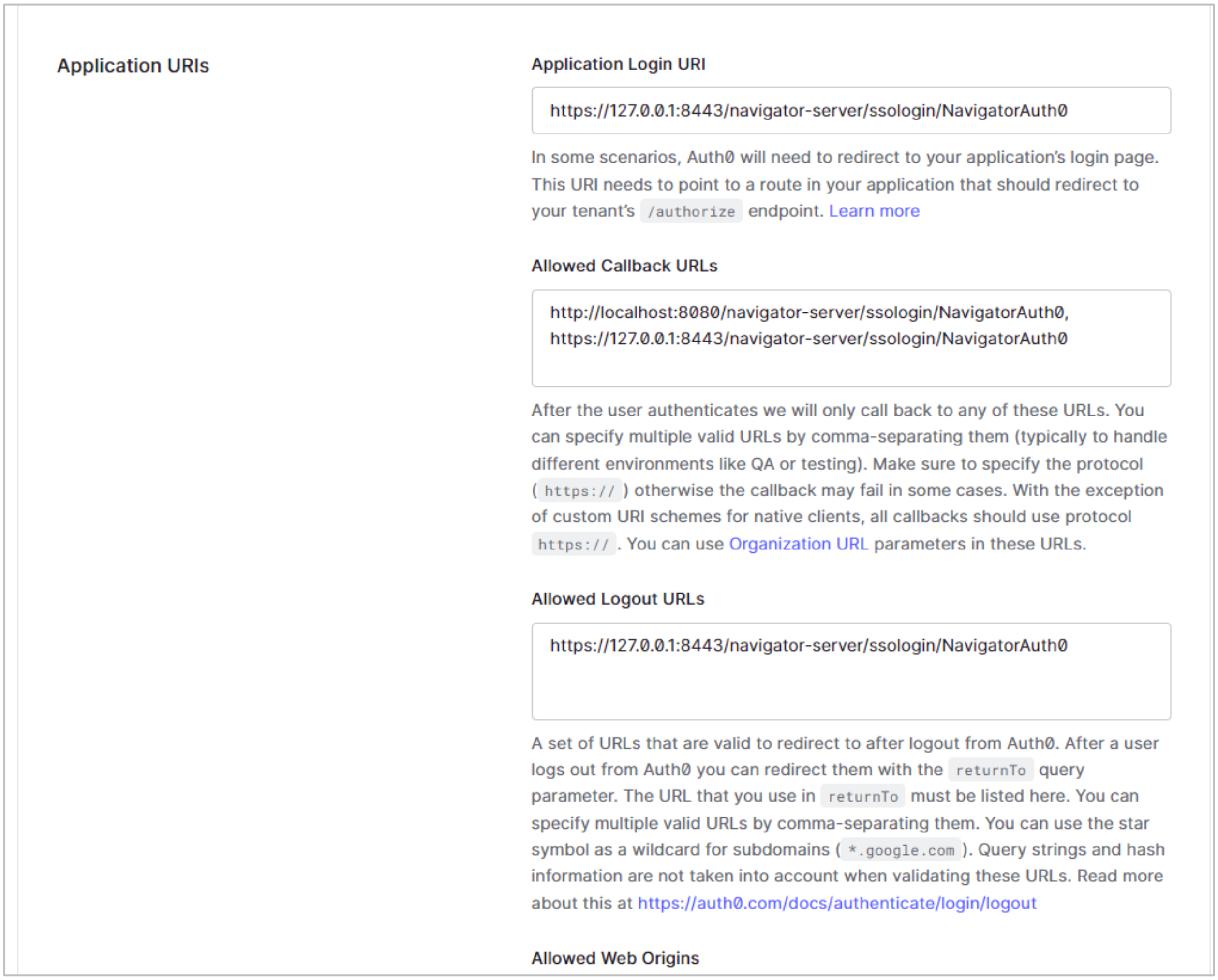
Client Secret
••

The Client Secret is not base64 encoded.

Description
Add a description in less than 140 characters

A free text description of the application. Max character count is 140.

6. Scroll down until you see the **Application URIs** section.



Application URIs

Application Login URI

https://127.0.0.1:8443/navigator-server/ssologin/NavigatorAuth0

In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's `/authorize` endpoint. Learn more

Allowed Callback URLs

http://localhost:8080/navigator-server/ssologin/NavigatorAuth0,
https://127.0.0.1:8443/navigator-server/ssologin/NavigatorAuth0

After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol (`https://`) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol `https://` . You can use Organization URL parameters in these URLs.

Allowed Logout URLs

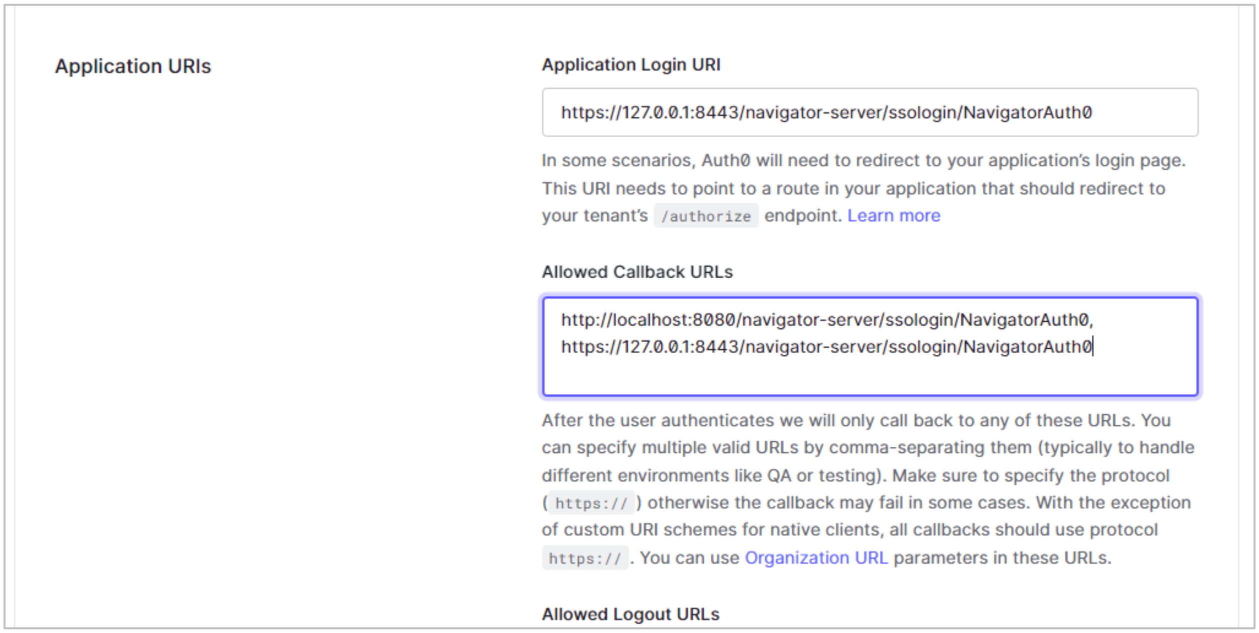
https://127.0.0.1:8443/navigator-server/ssologin/NavigatorAuth0

A set of URLs that are valid to redirect to after logout from Auth0. After a user logs out from Auth0 you can redirect them with the `returnTo` query parameter. The URL that you use in `returnTo` must be listed here. You can specify multiple valid URLs by comma-separating them. You can use the star symbol as a wildcard for subdomains (`*.google.com`). Query strings and hash information are not taken into account when validating these URLs. Read more about this at https://auth0.com/docs/authenticate/login/logout

Allowed Web Origins

7. Fill in the **Allowed Callback URLs**. When accessing Navigator, if you use a URL that is not provided in this list, you will not be able to log in.
8. Make sure that URLs end with /ssologin/{name-of-config}.
   ssologin is used in the login servlet. {name-of-config} is the value in the <name> parameter in xray_samlsso.xml (the Tomcat samlsso configuration file).

⚠ **IMPORTANT!** If more than one address is needed, use commas to separate them. Do not use spaces or NEWLINE to separate addresses when configuring Auth0.



Application URIs

Application Login URI

https://127.0.0.1:8443/navigator-server/ssologin/NavigatorAuth0

In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's `/authorize` endpoint. Learn more

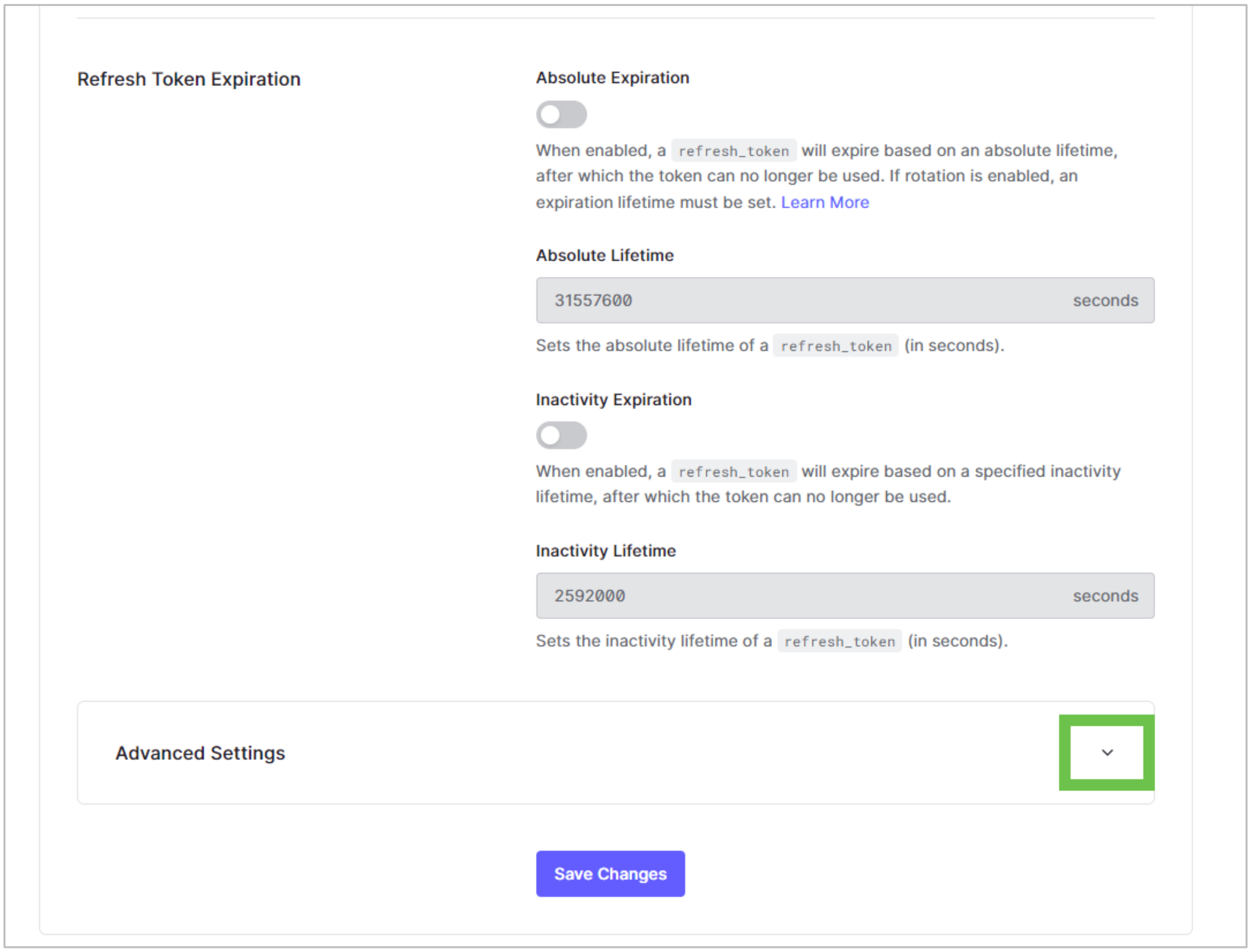
Allowed Callback URLs

http://localhost:8080/navigator-server/ssologin/NavigatorAuth0,
https://127.0.0.1:8443/navigator-server/ssologin/NavigatorAuth0

After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol (`https://`) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol `https://` . You can use Organization URL parameters in these URLs.

Allowed Logout URLs

9. Scroll down until you see the **Advanced Settings** section. Expand this section by clicking the arrow: ⌄.



Refresh Token Expiration

Absolute Expiration

When enabled, a `refresh_token` will expire based on an absolute lifetime, after which the token can no longer be used. If rotation is enabled, an expiration lifetime must be set. Learn More

Absolute Lifetime

31557600 seconds

Sets the absolute lifetime of a `refresh_token` (in seconds).

Inactivity Expiration

When enabled, a `refresh_token` will expire based on a specified inactivity lifetime, after which the token can no longer be used.

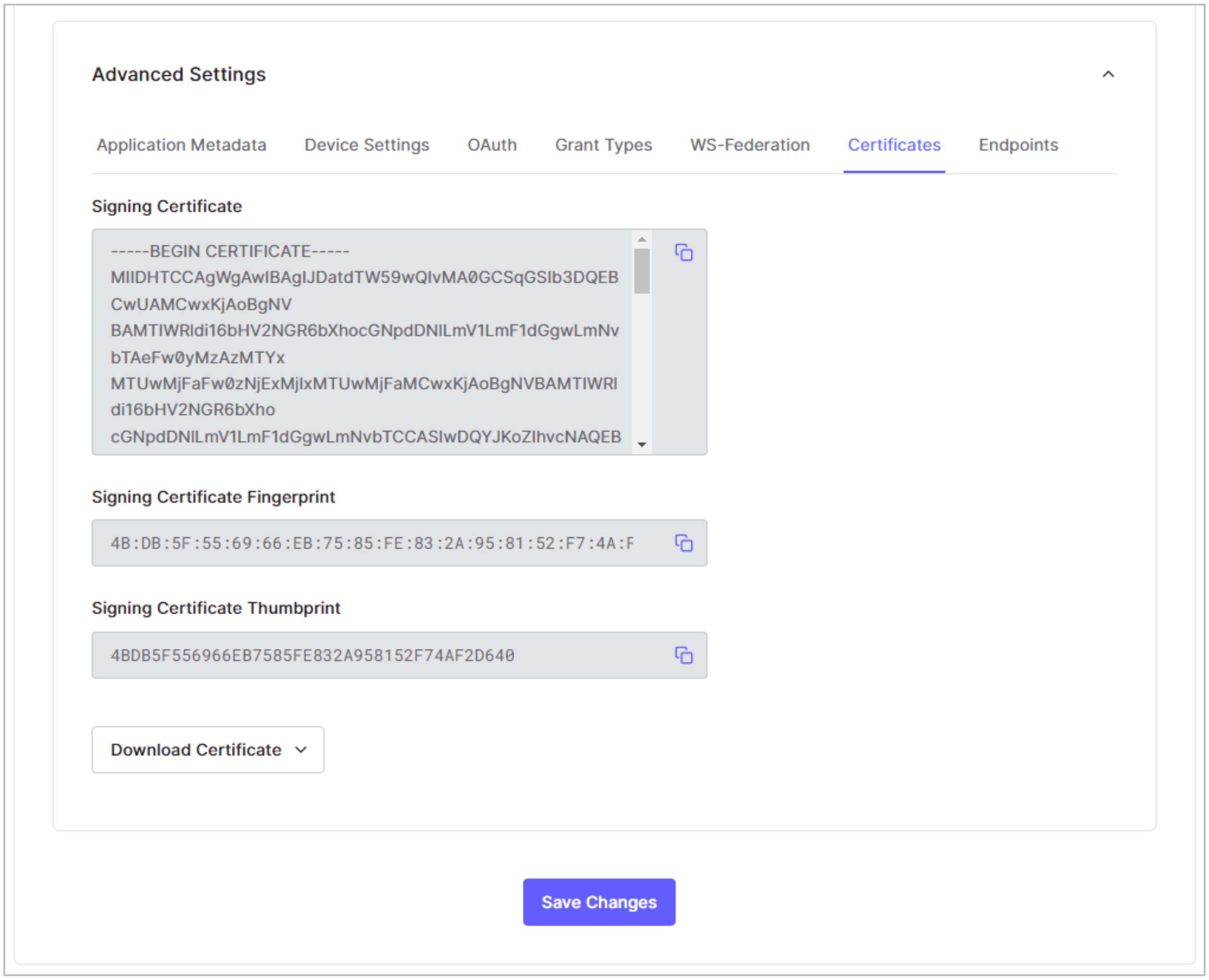
Inactivity Lifetime

2592000 seconds

Sets the inactivity lifetime of a `refresh_token` (in seconds).

Advanced Settings

10. Select the **Certificates** tab.



Advanced Settings

Signing Certificate

```
-----BEGIN CERTIFICATE-----
MIIDHTCCAgWgAwIBAgIJDatdTW59wQIvMA0GCSqGSIb3DQEB
CwUAMCwxKjAoBgNV
BAMTIWRldi16bHV2NGR6bXhocGNpdDNlLmV1LmF1dGgwLmNv
bTAeFw0yMzAzMTYx
MTUwMjFaFw0zNjExMjIxMTUwMjFaMCwxKjAoBgNVBAMTIWRl
di16bHV2NGR6bXho
cGNpdDNlLmV1LmF1dGgwLmNvbTCCASIwDQYJKoZIhvcNAQEB
```

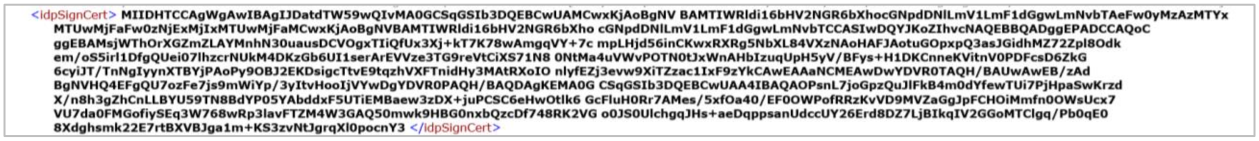
Signing Certificate Fingerprint

```
4B:DB:5F:55:69:66:EB:75:85:FE:83:2A:95:81:52:F7:4A:F
```

Signing Certificate Thumbprint

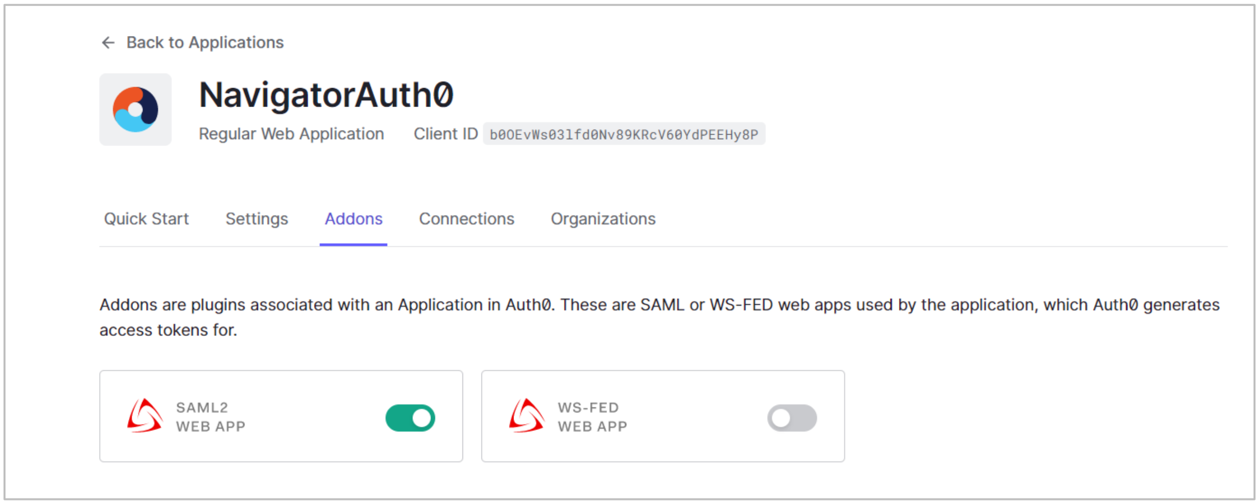
```
4BDB5F556966EB7585FE832A958152F74AF2D640
```

11. Click ⧉ to copy the value in the **Signing Certificate** field and paste it into the <idpSignCert> in the Tomcat samlsso configuration file.



```
<idpSignCert> MIIDHTCCAgWgAwIBAgIJDatdTW59wQIvMA0GCSqGSIb3DQEBCwUAMCwxKjAoBgNV BAMTIWRldi16bHV2NGR6bXhocGNpdDNlLmV1LmF1dGgwLmNvbTAeFw0yMzAzMTYx
    MTUwMjFaFw0zNjExMjIxMTUwMjFaMCwxKjAoBgNVBAMTIWRldi16bHV2NGR6bXho cGNpdDNlLmV1LmF1dGgwLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
    ggEBAMsjWThOrXGZmZLAYMnhN30uausDCVOgxTIiQfUx3Xj+kT7K78wAmgqVY+7c mpLHjd56inCKwxRXRg5NbXL84VXzNAoHAFJAotuGOpxpQ3asJGidhMZ72Zpl8Odk
    em/oS5irl1DfgQUei07lhzcrNUkM4DKzGb6UI1serArEVVze3TG9reVtCiXS71N8 0NtMa4uVWvPOTN0tJxWnAHbIzuqUpH5yV/BFys+H1DKCnneKVitnV0PDFcsD6ZkG
    6cyiJT/TnNgIyynXTBYjPAoPy9OBJ2EKDsigcTtvE9tqzhVXFTnidHy3MAtRXoIO nlyfEZj3evw9XiTZzac1IxF9zYkCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAd
    BgNVHQ4EFgQU7ozFe7js9mWiYp/3yItvHooIjVYwDgYDVR0PAQH/BAQDAgKEMA0G CSqGSIb3DQEBCwUAA4IBAQAOPsnL7joGpzQuJlFkB4m0dYfewTUi7PjHpaSwKrzd
    X/n8h3gZhCnLLBYU59TN8BdYP05YAbddxF5UTiEMBaew3zDX+juPCSC6eHwOtlk6 GcFluH0Rr7AMes/5xfOa40/EF0OWPofRRzKvVD9MVZaGgJpFCHOiMmfn0OWsUcx7
    VU7da0FMGofiySEq3W768wRp3lavFTZM4W3GAQ50mwk9HBG0nxbQzcDf748RK2VG o0JS0UlchgqJHs+aeDqppsanUdccUY26Erd8DZ7LjBIkqIV2GGoMTClgq/Pb0qE0
    8Xdghsmk22E7rtBXVBJga1m+KS3zvNtJgrqXl0pocnY3 </idpSignCert>
```

12. Scroll back up to return to the top of the **Settings** tab. Select the **Addons** tab and select SAML2 web app to enable the addon.

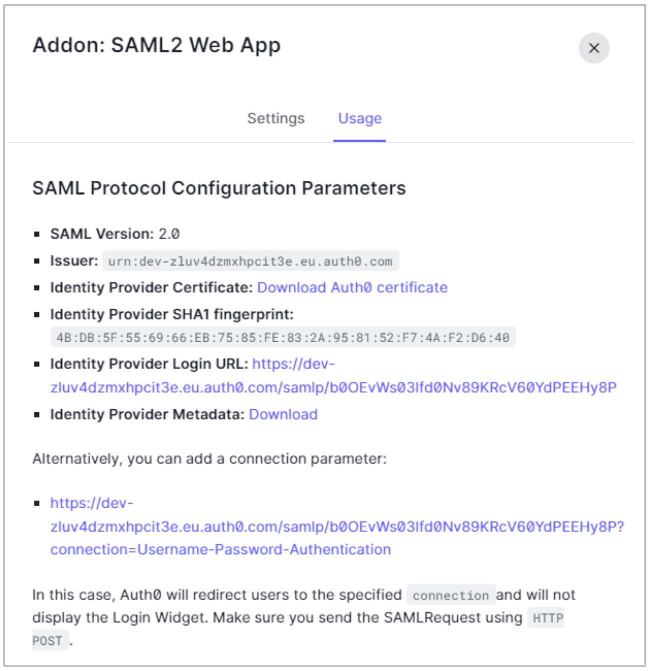


Addons are plugins associated with an Application in Auth0. These are SAML or WS-FED web apps used by the application, which Auth0 generates access tokens for.

13. The Addon: SAML2 Web Apps pop-up window is displayed. Copy values to the Tomcat samlsso configuration file XML parameters as follows:

Table 3 Auth0 Parameter Mapping

Auth0 Addon: SAML2 Web Apps window	XML Parameter
1. Identity Provider Login URL	used in idpSsoServiceUrl, idpArtifactResolveServiceUrl and idpSloServiceUrl
2. Issuer	idpEntityId



SAML Protocol Configuration Parameters

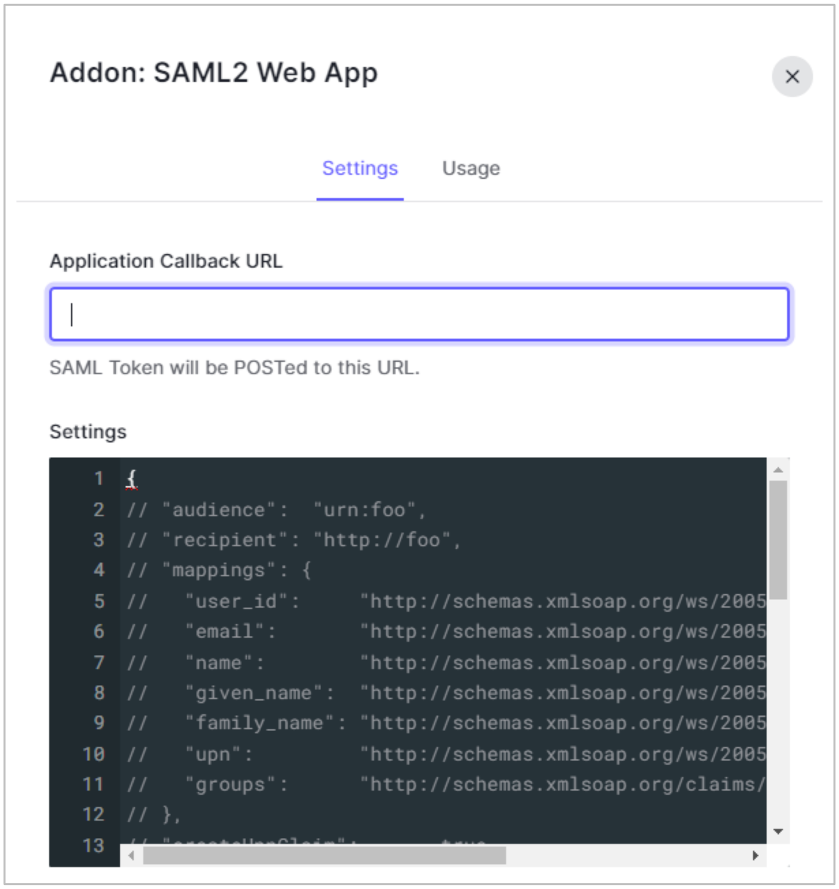
- **SAML Version:** 2.0
- **Issuer:** `urn:dev-zluv4dzmxhpcit3e.eu.auth0.com`
- **Identity Provider Certificate:** Download Auth0 certificate
- **Identity Provider SHA1 fingerprint:** `4B:DB:5F:55:69:66:EB:75:85:FE:83:2A:95:81:52:F7:4A:F2:D6:40`
- **Identity Provider Login URL:** https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P
- **Identity Provider Metadata:** Download

Alternatively, you can add a connection parameter:

- https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P?connection=Username-Password-Authentication

In this case, Auth0 will redirect users to the specified `connection` and will not display the Login Widget. Make sure you send the SAMLRequest using `HTTP POST` .

14. Select the **Settings** tab.



Application Callback URL

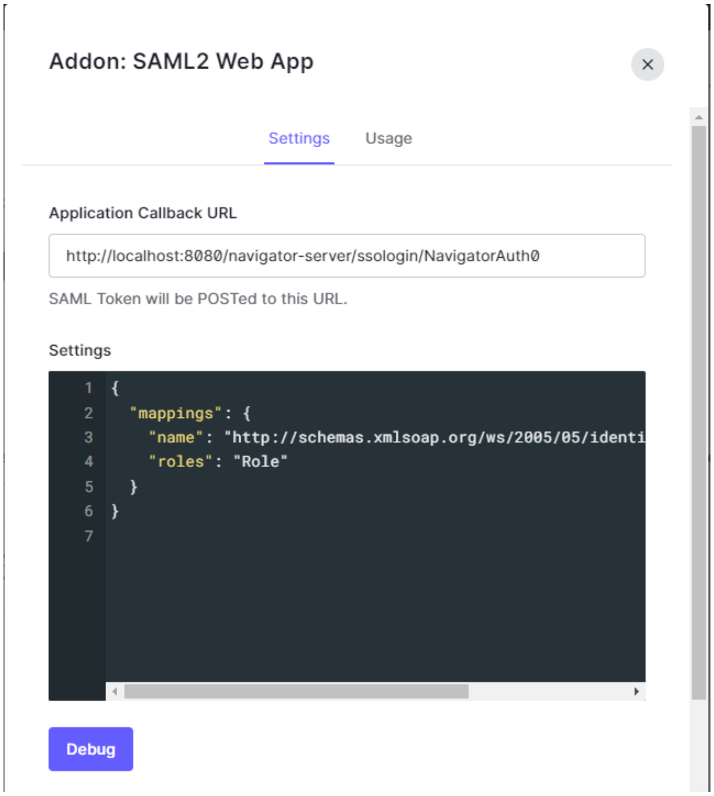
SAML Token will be POSTed to this URL.

Settings

```
{
// "audience":  "urn:foo",
// "recipient": "http://foo",
// "mappings": {
//   "user_id":     "http://schemas.xmlsoap.org/ws/2005
//   "email":       "http://schemas.xmlsoap.org/ws/2005
//   "name":        "http://schemas.xmlsoap.org/ws/2005
//   "given_name":  "http://schemas.xmlsoap.org/ws/2005
//   "family_name": "http://schemas.xmlsoap.org/ws/2005
//   "upn":         "http://schemas.xmlsoap.org/ws/2005
//   "groups":      "http://schemas.xmlsoap.org/claims/
// },
```

15. Enter the URL to which you want to post the SAML Token in the **Application Callback URL** field.
16. In the **Settings** area, paste the following:

```
{
 "mappings": {
  "name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
  "roles": "Role"
 }
}
```



Addon: SAML2 Web App

Application Callback URL

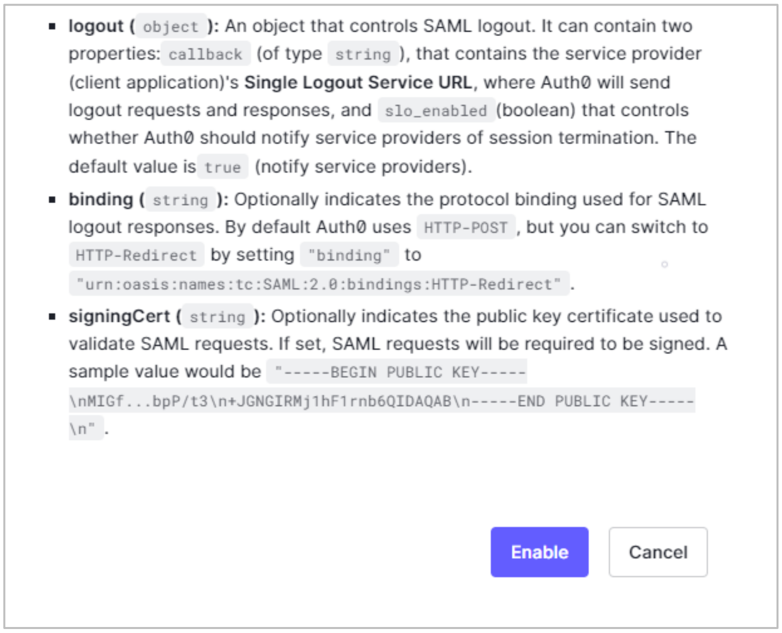
http://localhost:8080/navigator-server/ssologin/NavigatorAuth0

SAML Token will be POSTed to this URL.

Settings

```
{
  "mappings": {
    "name": "http://schemas.xmlsoap.org/ws/2005/05/identi
    "roles": "Role"
  }
}

```

17. Click **Enable**.



- **logout (** `object` **):** An object that controls SAML logout. It can contain two properties: `callback` (of type `string`), that contains the service provider (client application)'s **Single Logout Service URL**, where Auth0 will send logout requests and responses, and `slo_enabled` (boolean) that controls whether Auth0 should notify service providers of session termination. The default value is `true` (notify service providers).
- **binding (** `string` **):** Optionally indicates the protocol binding used for SAML logout responses. By default Auth0 uses `HTTP-POST` , but you can switch to `HTTP-Redirect` by setting `"binding"` to `"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"` .
- **signingCert (** `string` **):** Optionally indicates the public key certificate used to validate SAML requests. If set, SAML requests will be required to be signed. A sample value would be `"-----BEGIN PUBLIC KEY-----\nMIGf...bpP/t3\n+JGNGIRMj1hF1rnb6QIDAQAB\n-----END PUBLIC KEY-----\n"` .

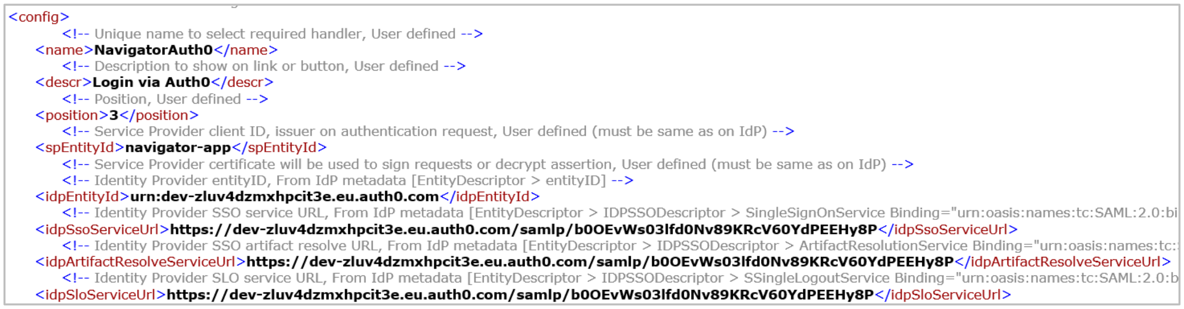
4.2 Important Configuration Parameters

4.2.1 For Service Providers

spEntityId – Specify the name of the service provider.

4.2.2 For Identity Providers

IdpEntityId, *idpSsoServiceUrl*, *idpArtifactResolveServiceUrl* and *idpSloServiceUrl*.
Make sure you have entered the parameters from step 13 of Auth0 Identity Provider Configuration in the Tomcat samlsso configuration file, as shown below:



```
<config>
        <!-- Unique name to select required handler, User defined -->
    <name>NavigatorAuth0</name>
        <!-- Description to show on link or button, User defined -->
    <descr>Login via Auth0</descr>
        <!-- Position, User defined -->
    <position>3</position>
        <!-- Service Provider client ID, issuer on authentication request, User defined (must be same as on IdP) -->
    <spEntityId>navigator-app</spEntityId>
        <!-- Service Provider certificate will be used to sign requests or decrypt assertion, User defined (must be same as on IdP) -->
        <!-- Identity Provider entityID, From IdP metadata [EntityDescriptor > entityID] -->
    <idpEntityId>urn:dev-zluv4dzmxhpcit3e.eu.auth0.com</idpEntityId>
        <!-- Identity Provider SSO service URL, From IdP metadata [EntityDescriptor > IDPSSODescriptor > SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bi
    <idpSsoServiceUrl>https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P</idpSsoServiceUrl>
        <!-- Identity Provider SSO artifact resolve URL, From IdP metadata [EntityDescriptor > IDPSSODescriptor > ArtifactResolutionService Binding="urn:oasis:names:tc:
    <idpArtifactResolveServiceUrl>https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P</idpArtifactResolveServiceUrl>
        <!-- Identity Provider SLO service URL, From IdP metadata [EntityDescriptor > IDPSSODescriptor > SSingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:b
    <idpSloServiceUrl>https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P</idpSloServiceUrl>
```

4.3 Sample apwmq_samlsso.xml file using Auth0

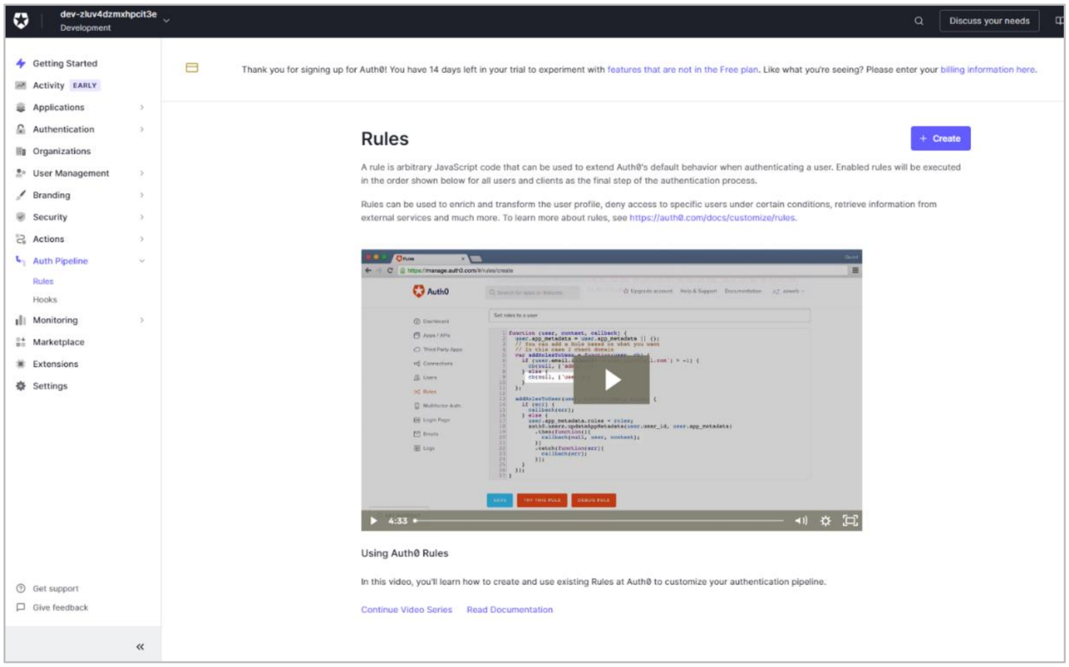
```
<?xml version="1.0"?>
<!-- SAML SSO handlers configurations -->
<configs>
<!-- SAML SSO handler configuration -->
<config>
<!-- Unique name to select required handler, User defined -->
<name>NavigatorAuth0</name>
<!-- Description to show on link or button, User defined -->
<descr>Login via Auth0</descr>
<!-- Position, User defined -->
<position>1</position>
<!-- Service Provider client ID, issuer on authentication request, User defined (must be same as on IdP) -->
<spEntityId>navigator-app</spEntityId>
<!-- Identity Provider entityID, From IdP metadata [EntityDescriptor > entityID] -->
<idpEntityId>urn:dev-zluv4dzmxhpcit3e.eu.auth0.com</idpEntityId>
<!-- Identity Provider SSO service URL, From IdP metadata [EntityDescriptor > IDPSSODescriptor > SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->
<idpSsoServiceUrl>https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P?organization=org_ISxEm3h4DDFPMImn</idpSsoServiceUrl>
```

```
<!-- Identity Provider SSO artifact resolve URL, From IdP metadata [EntityDescriptor >
IDPSSODescriptor > ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"] -->

<idpArtifactResolveServiceUrl>https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P?organization=org_ISxEm3h4DDFPMImn</idpArtifactResolveServiceUrl>

<!-- Identity Provider SLO service URL, From IdP metadata [EntityDescriptor > IDPSSODescriptor >
SSingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->

<idpSloServiceUrl>https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P</idpSloServiceUrl>

<!-- Identity Provider certificate will be used to validate signatures, From IdP metadata [EntityDescriptor
> IDPSSODescriptor > KeyDescriptor use="signing" > KeyInfo > X509Data > X509Certificate] -->

<idpSignCert>
MIIDHTCCAgWgAwIBAgIJDatdTW59wQIvMA0GCSqGSIb3DQEBCwUAMCwxKjAoBgNVBAMTI
WRldi16bHV2NGR6bXhocGNpdDNlLmV1LmF1dGgwLmNvbTAeFw0yMzAzMTYxMTUwMjFaFw0
zNjExMjIxMTUwMjFaMCwxKjAoBgNVBAMTIWRldi16bHV2NGR6bXhocGNpdDNlLmV1LmF1dG
gwLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMsjWThOrXGZmZLAY
MnhN30uausDCVOgxTIiQfUx3Xj+kT7K78wAmgqVY+7cmpLHjd56inCKwxRXRg5NbXL84VXzNA
oHAFJAotuGOpxpQ3asJGidhMZ72Zpl8Odkem/oS5irl1DfgQUei07lhzcrNUkM4DKzGb6UI1serArEVV
ze3TG9reVtCiXS71N80NtMa4uVWvPOTN0tJxWnAHbIzuqUpH5yV/BFys+H1DKCnneKVitnV0PDFc
sD6ZkG6cyiJT/TnNgIyynXTBYjPAoPy9OBJ2EKDsigcTtvE9tqzhVXFTnidHy3MAtRXoIOnlyfEZj3ev
w9XiTZzac1IxF9zYkCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU7oz
Fe7js9mWiYp/3yItvHooIjVYwDgYDVR0PAQH/BAQDAgKEMA0GCSqGSIb3DQEBCwUAA4IBAQ
AOPsnL7joGpzQuJlFkB4m0dYfewTUi7PjHpaSwKrzdX/n8h3gZhCnLLBYU59TN8BdYP05YAbddxF5
UTiEMBaew3zDX+juPCSC6eHwOtlk6GcFluH0Rr7AMes/5xfOa40/EF0OWPofRRzKvVD9MVZaGgJp
FCHOiMmfn0OWsUcx7VU7da0FMGofiySEq3W768wRp3lavFTZM4W3GAQ50mwk9HBG0nxbQzcD
f748RK2VGo0JS0UlchgqJHs+aeDqppsanUdccUY26Erd8DZ7LjBIkqIV2GGoMTClgq/Pb0qE08Xdghs
mk22E7rtBXVBJga1m+KS3zvNtJgrqXl0pocnY3</idpSignCert>

<!-- Service Provider must sign authentication request, User defined -->

<authnRequestSigned>true</authnRequestSigned>

<!-- Service Provider must sign artifact resolve request, User defined -->

<resolveArtifactRequestSigned>true</resolveArtifactRequestSigned>

<!-- Service Provider must sign logout request, User defined -->

<logoutRequestSigned>true</logoutRequestSigned>

<!-- Image can be added /image/path/img.* By default it will display an icon -->

<!-- <buttonIcon>image.png</buttonIcon>-->

<buttonText>Auth0 login</buttonText><buttonColor>#ffffff</buttonColor>

</config>
</configs>
```

4.4 Create rules

To allow user roles to be used for authorization as part of the authentication process, you must set up a rule.

1. From the left pane, select **Auth Pipeline > Rules**.



Thank you for signing up for Auth0! You have 14 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.

Rules

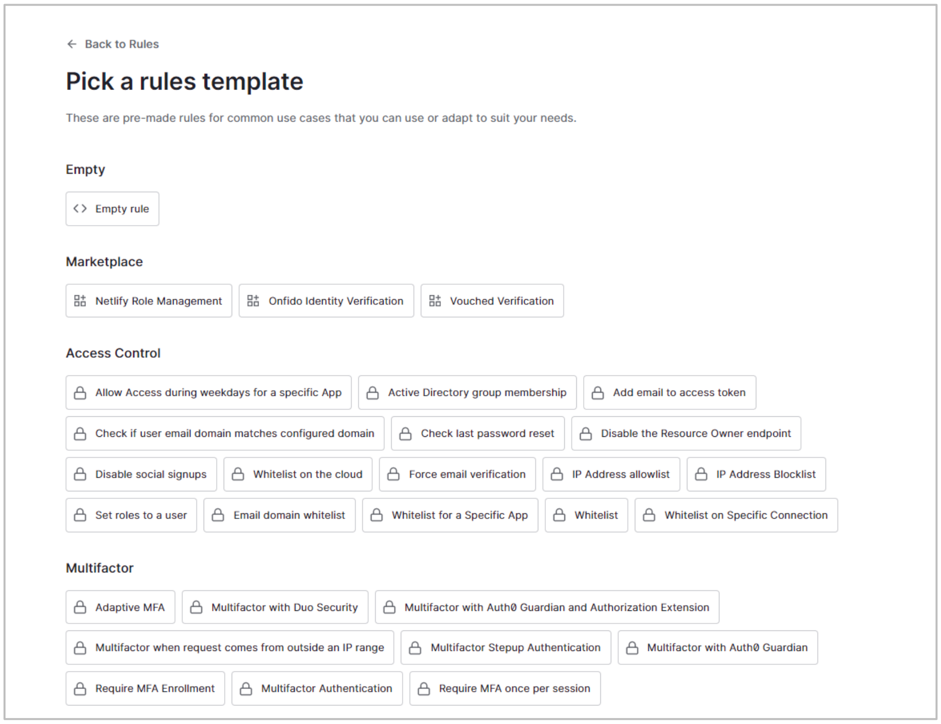
A rule is arbitrary JavaScript code that can be used to extend Auth0's default behavior when authenticating a user. Enabled rules will be executed in the order shown below for all users and clients as the final step of the authentication process.

Rules can be used to enrich and transform the user profile, deny access to specific users under certain conditions, retrieve information from external services and much more. To learn more about rules, see https://auth0.com/docs/customize/rules.

Using Auth0 Rules

In this video, you'll learn how to create and use existing Rules at Auth0 to customize your authentication pipeline.

2. Click **+ Create** on the right side.
3. Select **Empty rule**.


Back to Rules
Empty
Empty rule
Marketplace
Netlify Role Management
Onfido Identity Verification
Vouched Verification
Access Control
Allow Access during weekdays for a specific App
Active Directory group membership
Add email to access token
Check if user email domain matches configured domain
Check last password reset
Disable the Resource Owner endpoint
Disable social signups
Whitelist on the cloud
Force email verification
IP Address allowlist
IP Address Blocklist
Set roles to a user
Email domain whitelist
Whitelist for a Specific App
Whitelist
Whitelist on Specific Connection
Multifactor
Adaptive MFA
Multifactor with Duo Security
Multifactor with Auth0 Guardian and Authorization Extension
Multifactor when request comes from outside an IP range
Multifactor Stepup Authentication
Multifactor with Auth0 Guardian
Require MFA Enrollment
Multifactor Authentication
Require MFA once per session

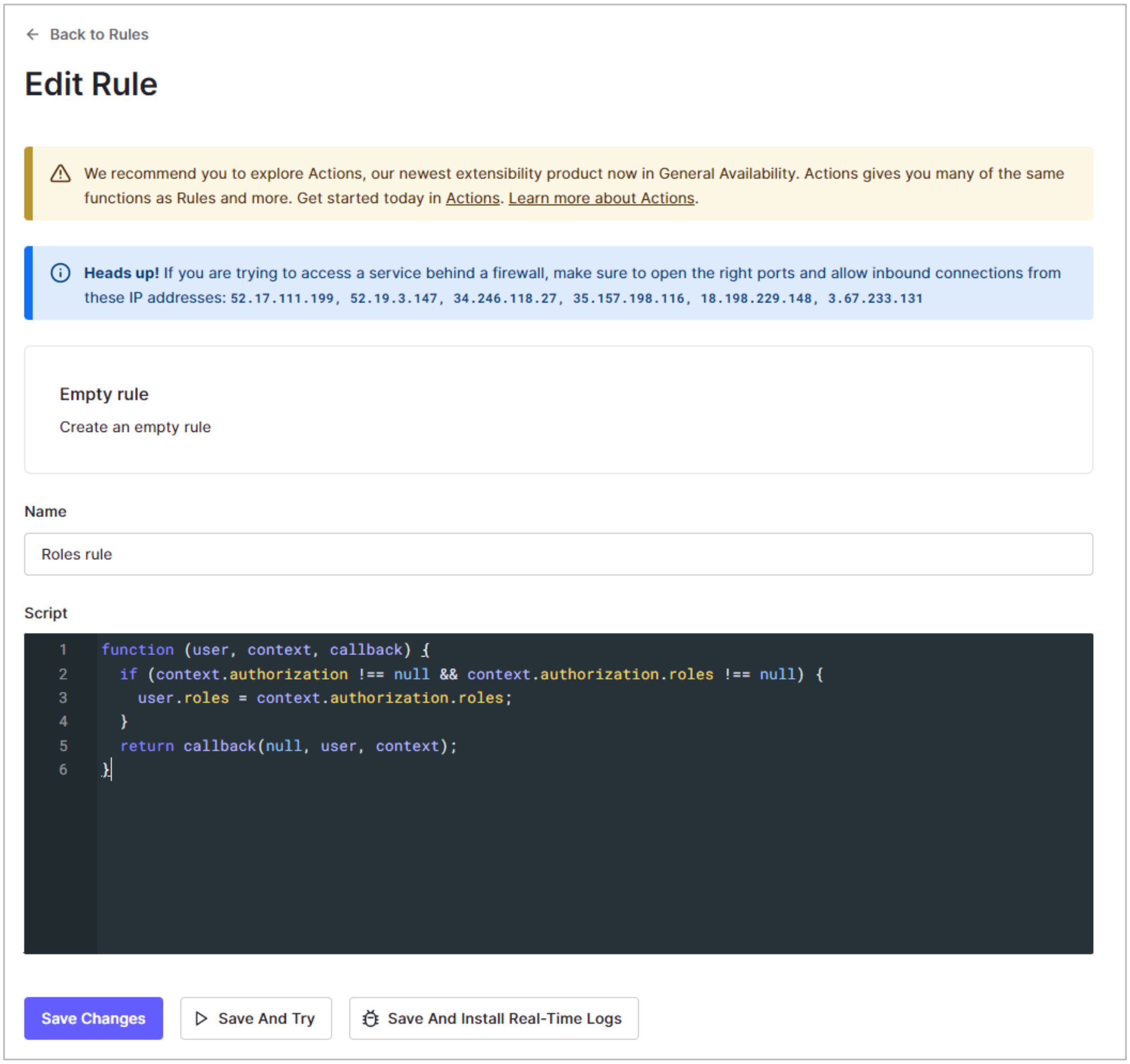
Pick a rules template

These are pre-made rules for common use cases that you can use or adapt to suit your needs.

4. Assign a **Name** to the rule.

Copy the text below and paste it in the Script field:

```
function (user, context, callback) {
  if (context.authorization !== null && context.authorization.roles !== null) {
                        user.roles = context.authorization.roles;
  }
  return callback(null, user, context);
}
```



Edit Rule

We recommend you to explore Actions, our newest extensibility product now in General Availability. Actions gives you many of the same functions as Rules and more. Get started today in Actions. Learn more about Actions.

Heads up! If you are trying to access a service behind a firewall, make sure to open the right ports and allow inbound connections from these IP addresses: `52.17.111.199, 52.19.3.147, 34.246.118.27, 35.157.198.116, 18.198.229.148, 3.67.233.131`

Empty rule

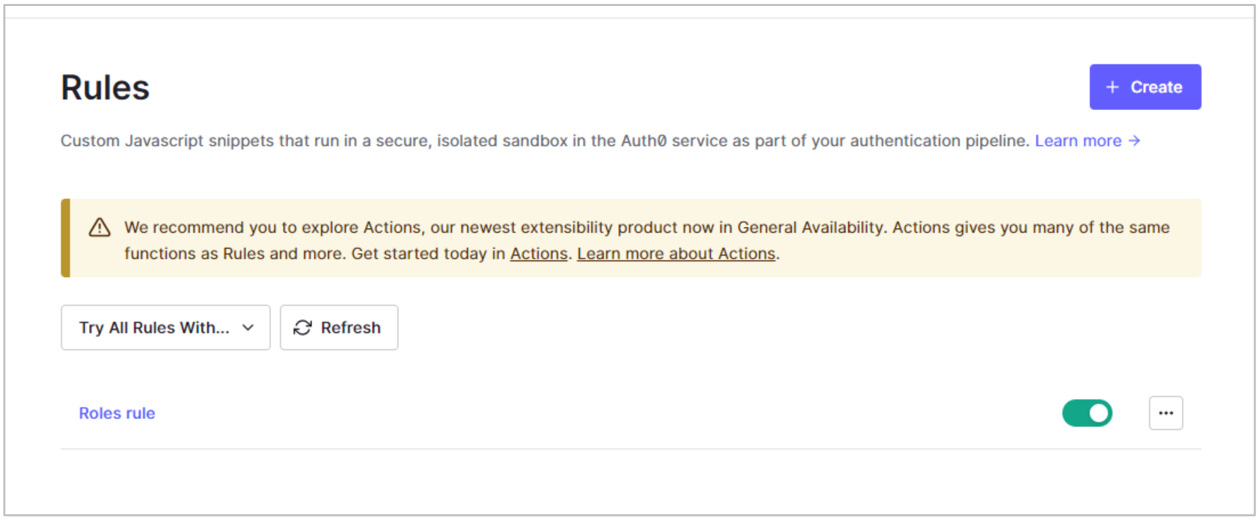
Create an empty rule

Name: Roles rule

Script

```
function (user, context, callback) {
  if (context.authorization !== null && context.authorization.roles !== null) {
    user.roles = context.authorization.roles;
  }
  return callback(null, user, context);
}
```

5. Click **Save Changes** to return to the Rules page. The new rule is visible and active.



Rules

Custom Javascript snippets that run in a secure, isolated sandbox in the Auth0 service as part of your authentication pipeline. Learn more →

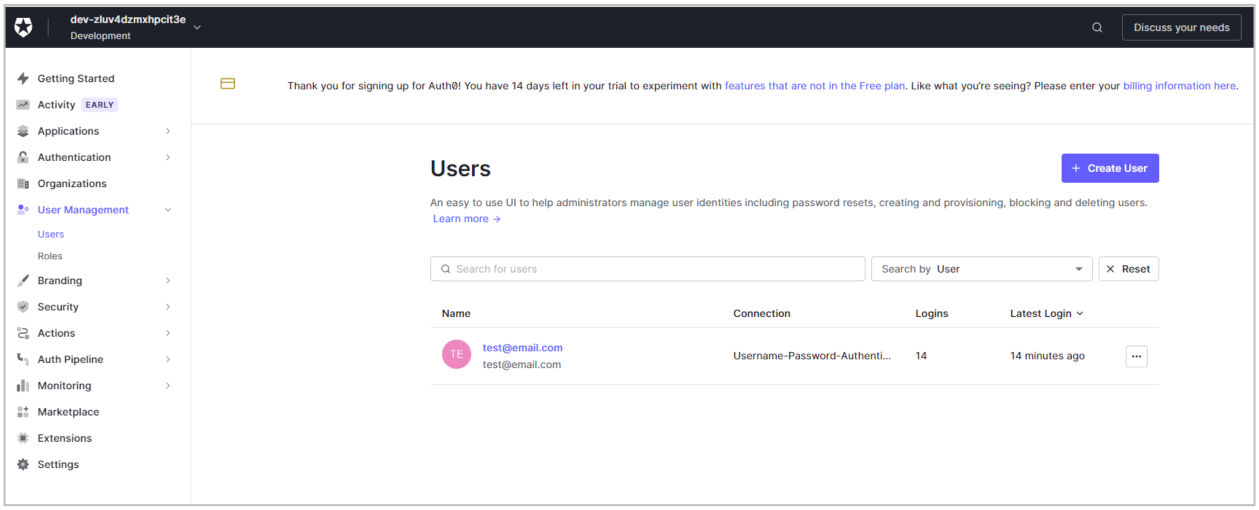
We recommend you to explore Actions, our newest extensibility product now in General Availability. Actions gives you many of the same functions as Rules and more. Get started today in Actions. Learn more about Actions.

Roles rule

4.5 Add Users and Roles

4.5.1 Create users

1. From the left pane, expand **User Management and** select **Users**.



Thank you for signing up for Auth0! You have 14 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.

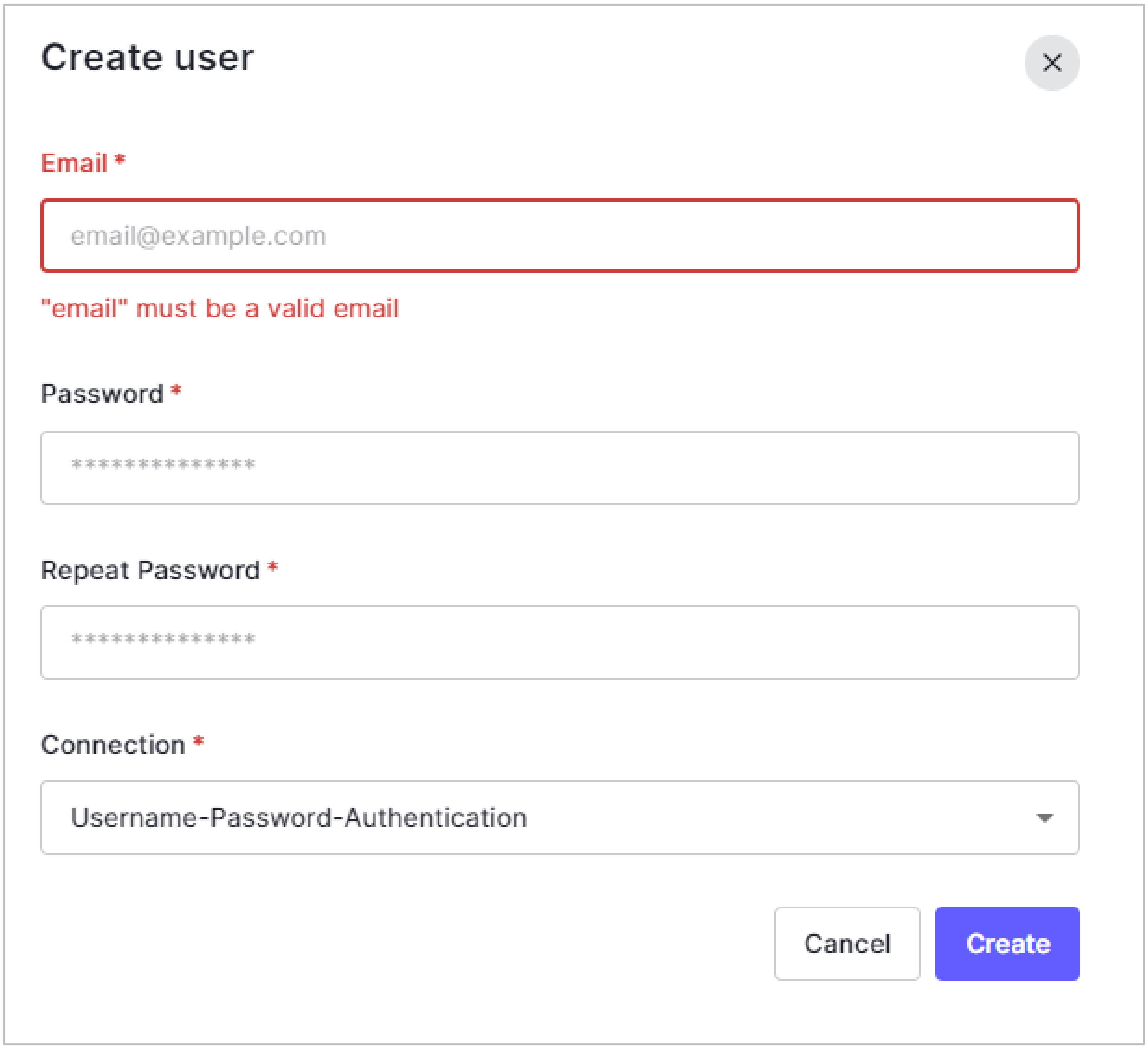
Users

An easy to use UI to help administrators manage user identities including password resets, creating and provisioning, blocking and deleting users. Learn more →

Name	Connection	Logins	Latest Login
TE test@email.com test@email.com	Username-Password-Authenti...	14	14 minutes ago

2. Click **+ Create User**.

3. Enter an **Email** address for the user.



Create user

Email *

email@example.com

"email" must be a valid email

Password *

****

Repeat Password *

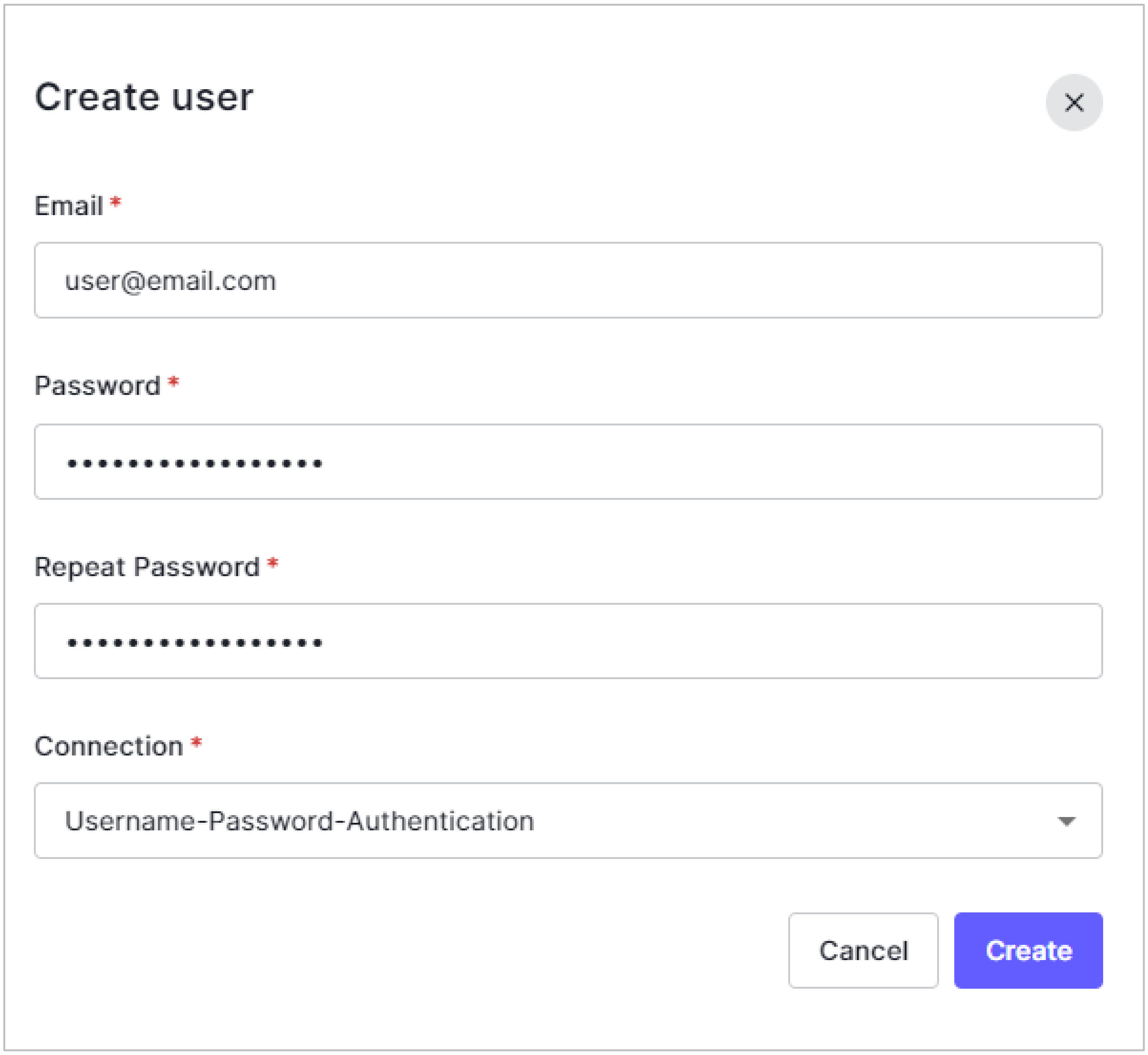
****

Connection *

Username-Password-Authentication

4. Enter a **Password**, then retype the password in the **Repeat Password** field to confirm it.

5. Select a **Connection** type.



Create user

Email * user@email.com

Password * •••••••••••••••••

Repeat Password * •••••••••••••••••

Connection * Username-Password-Authentication

6. Click **Create**. The settings for the new user are displayed.

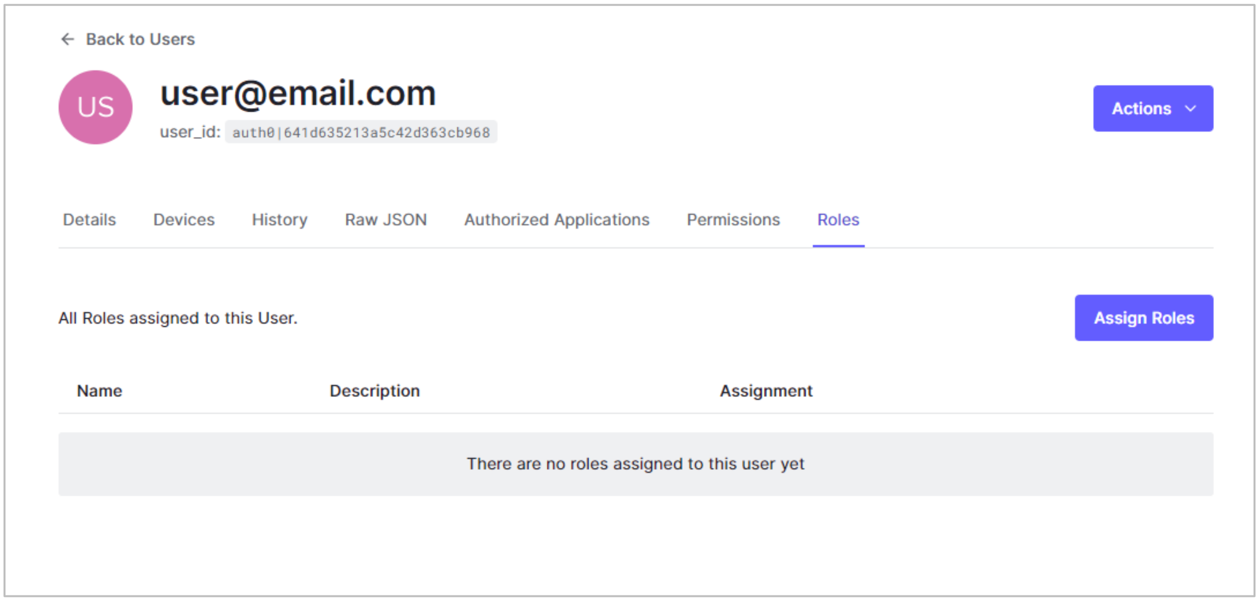
4.5.2 Assign roles to users

NOTE

Before assigning roles to users, you must first create a rule. See Create rules for instructions.

To assign a role to a user:

1. Select the **Roles** tab.



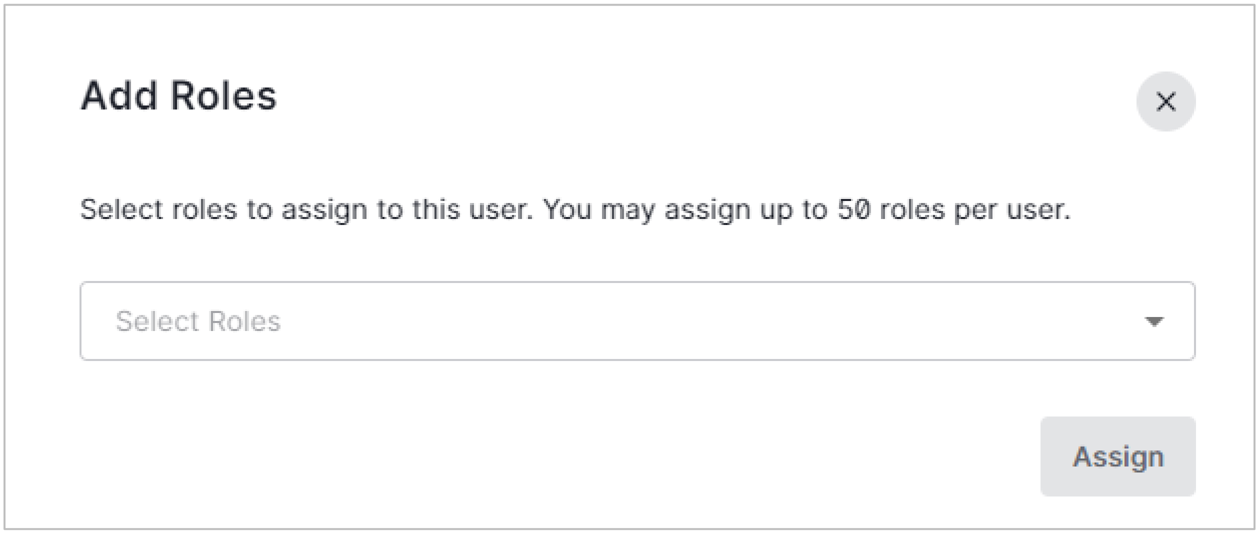
user@email.com

user_id: auth0|641d635213a5c42d363cb968

All Roles assigned to this User.

Name	Description	Assignment
There are no roles assigned to this user yet		

2. Click **Assign Roles**. The *Add Roles* dialog opens.

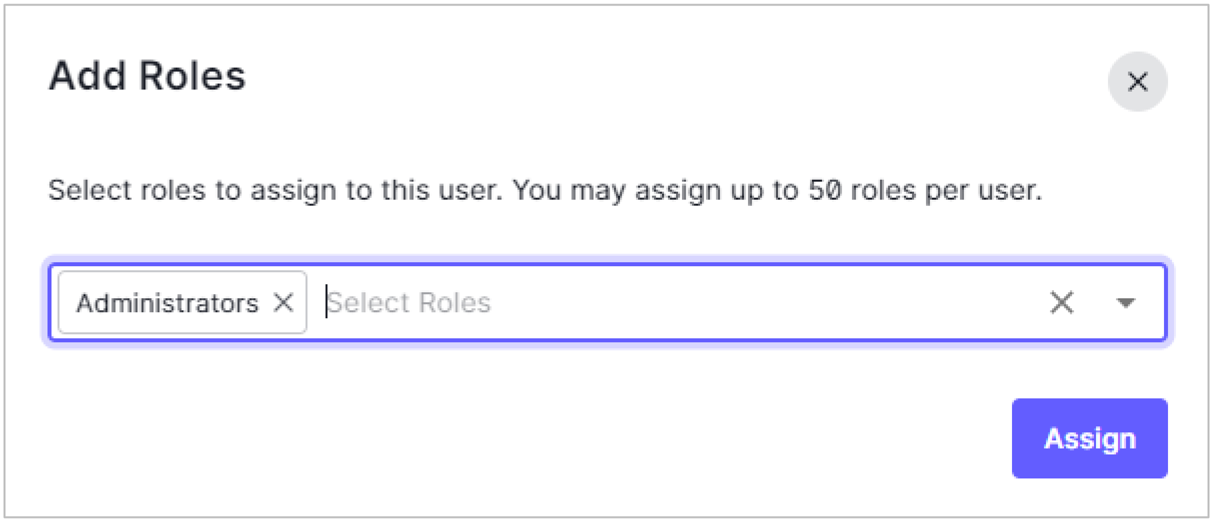


Add Roles

Select roles to assign to this user. You may assign up to 50 roles per user.

3. Begin typing the name of the role that you want to assign to the user. The list of roles is filtered automatically. Select the role.

4. Repeat the previous step until you have assigned all the roles that apply to this user.

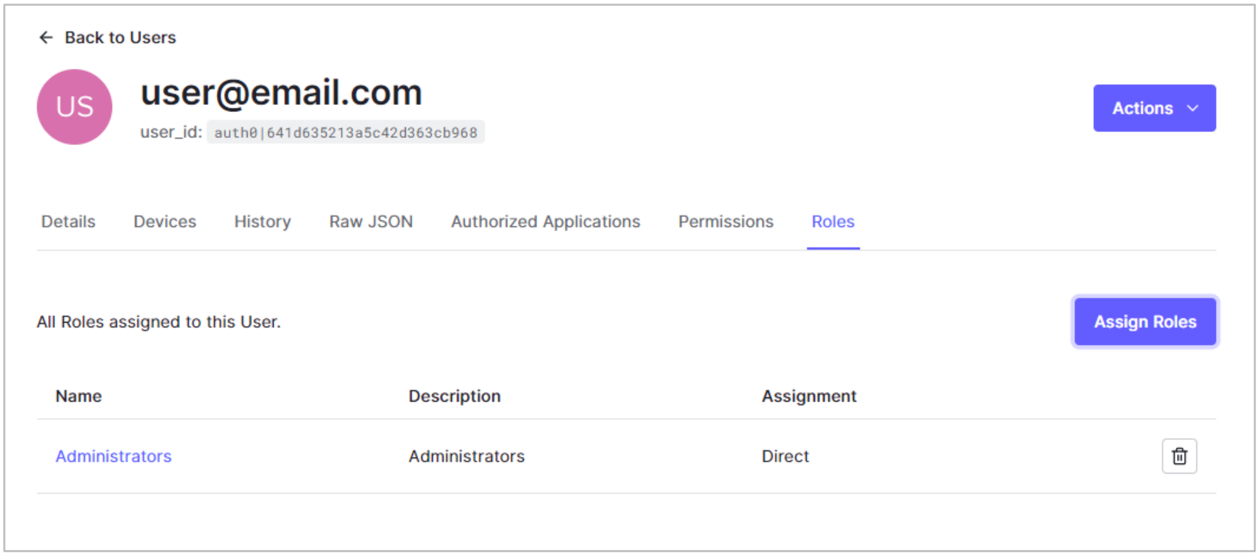


Add Roles

Select roles to assign to this user. You may assign up to 50 roles per user.

Administrators

5. Click **Assign**. The **Roles** tab is displayed and shows the newly assigned role.



user@email.com

user_id: auth0|641d635213a5c42d363cb968

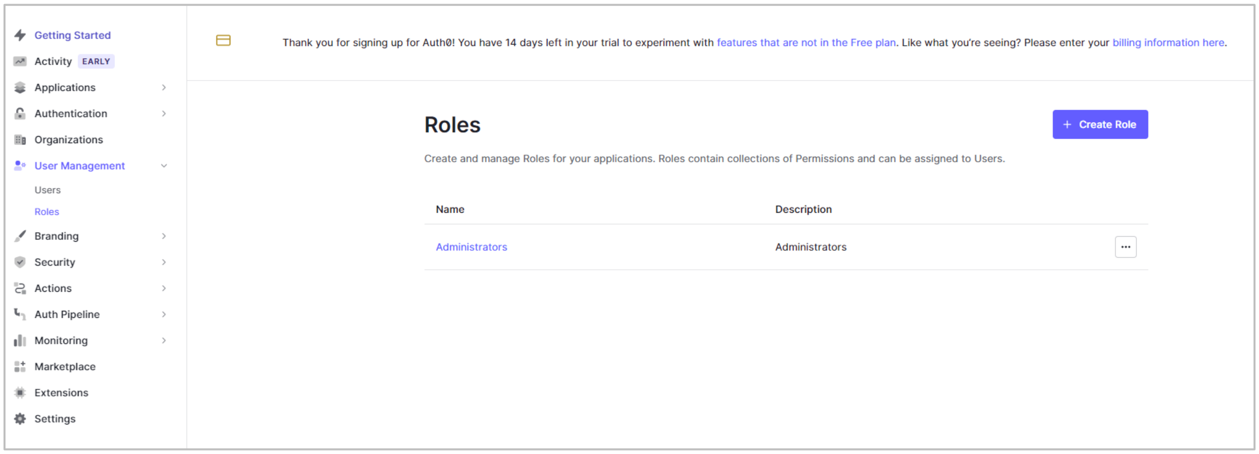
All Roles assigned to this User.

Name	Description	Assignment
Administrators	Administrators	Direct

4.5.3 Create roles

To create a role:

1. From the left pane, expand **User Management and** select **Roles**.



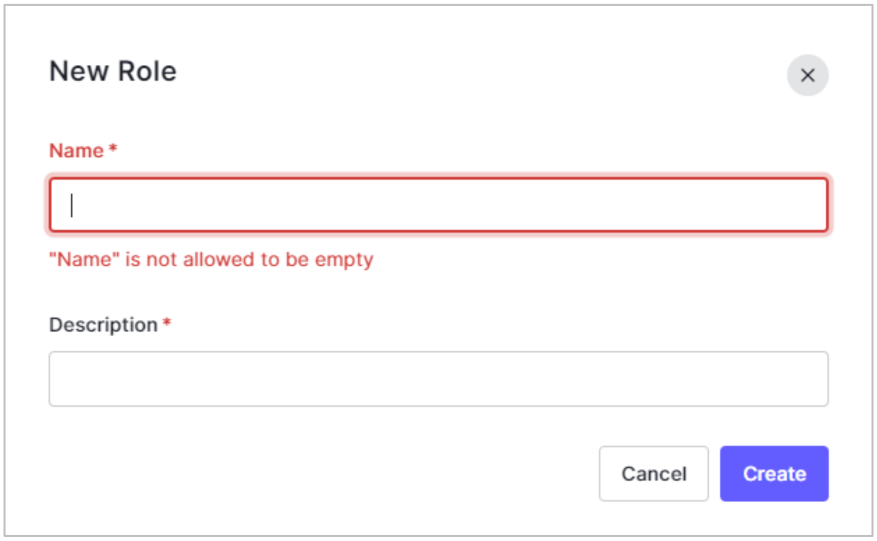
Thank you for signing up for Auth0! You have 14 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.

Roles

Create and manage Roles for your applications. Roles contain collections of Permissions and can be assigned to Users.

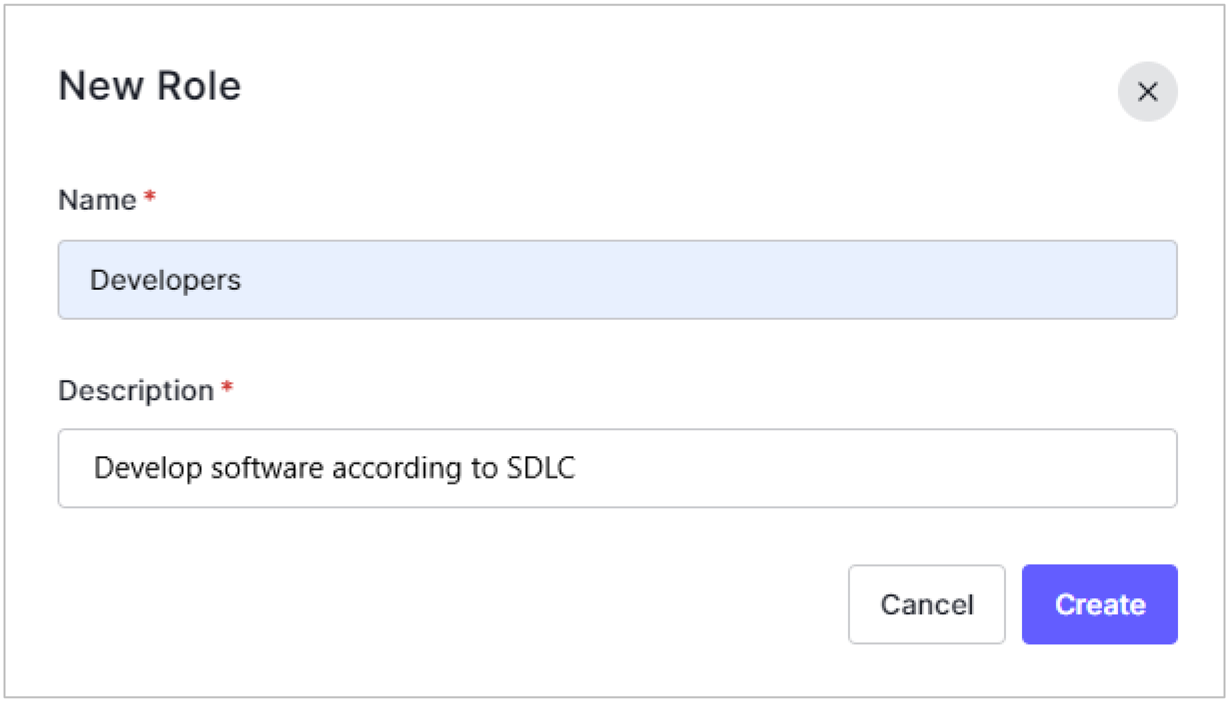
Name	Description
Administrators	Administrators

2. Click **+ Create role**. The *New Role* dialog opens.
3. Enter a **Name** for the new role.



"Name" is not allowed to be empty

4. Enter a **Description**.



New Role

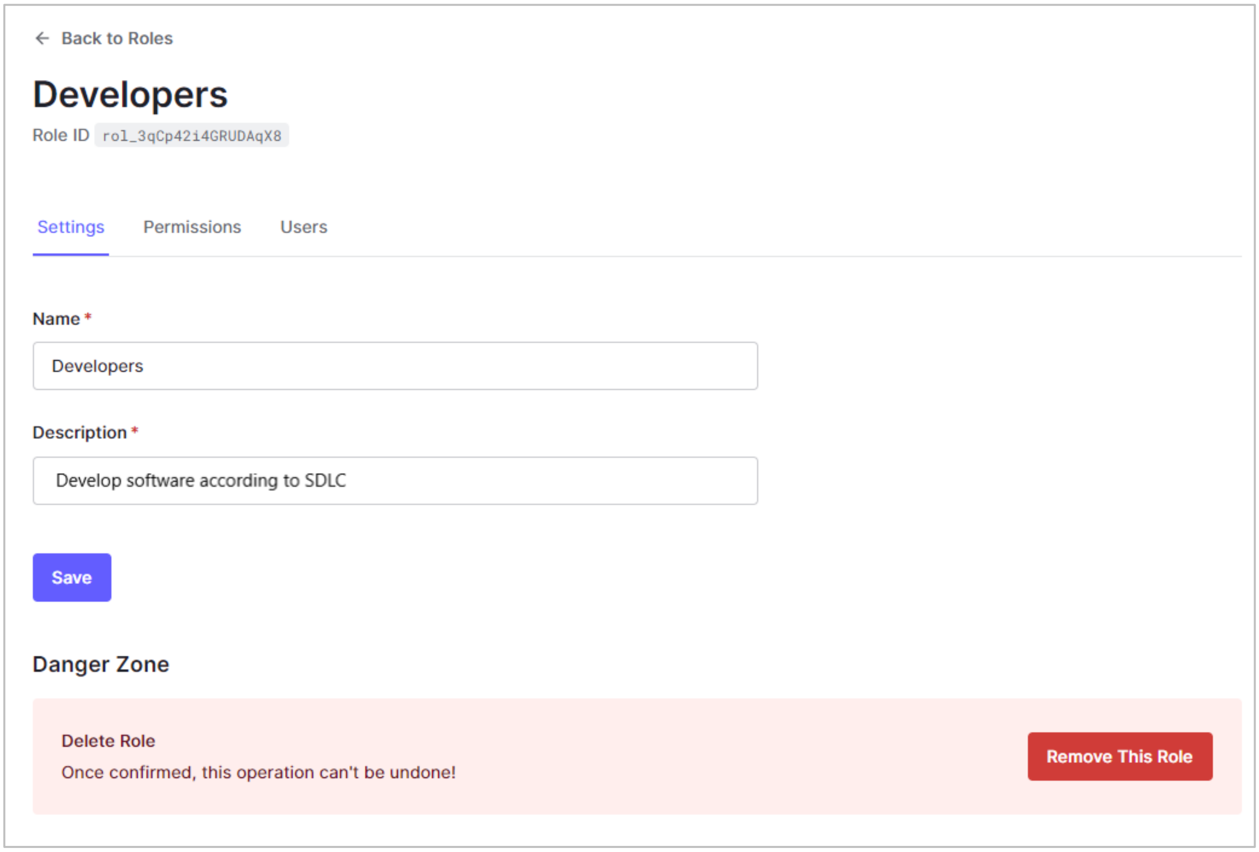
Name *

Developers

Description *

Develop software according to SDLC

5. Click **Create**. The **Settings** tab for the new role is displayed. See the following section for information about adding users to roles.



Developers

Role ID rol_3qCp42i4GRUDAqX8

Name *

Developers

Description *

Develop software according to SDLC

Danger Zone

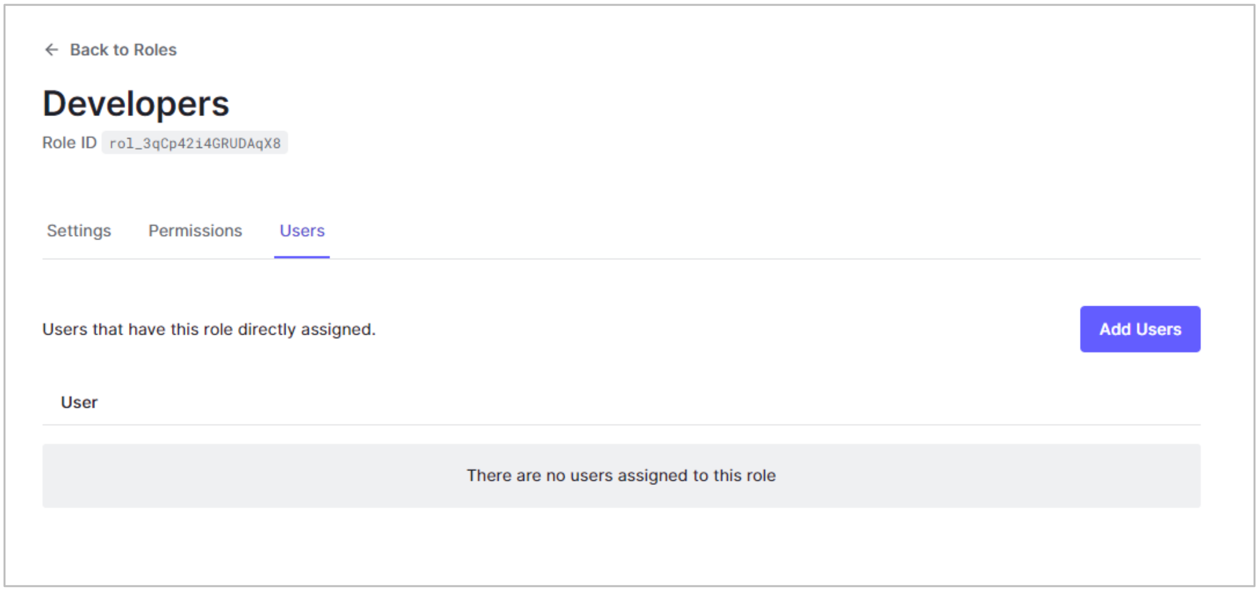
Delete Role

Once confirmed, this operation can't be undone!

4.5.4 Add users to roles

To add users to roles:

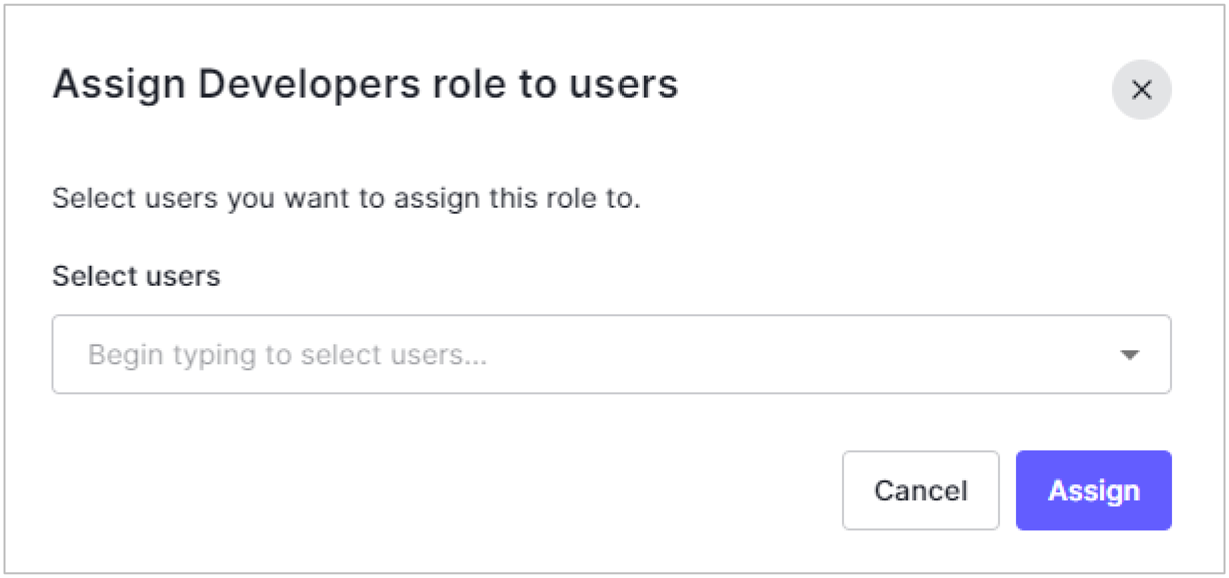
1. From the Role settings, select the **Users** tab.



Users that have this role directly assigned.

There are no users assigned to this role

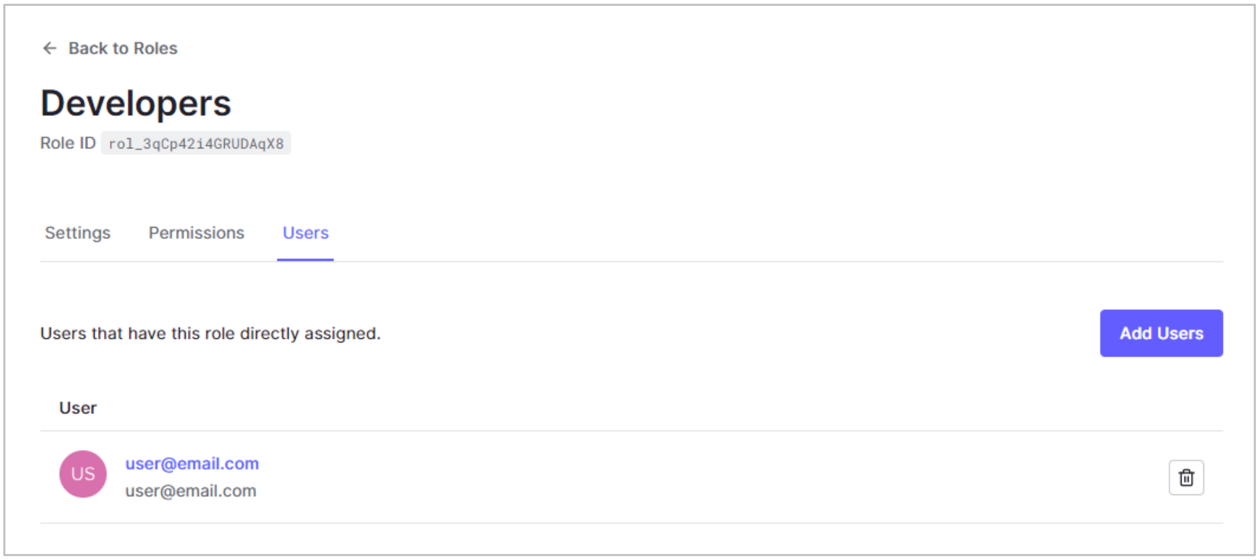
2. Click **Add Users**. The *Assign [role] to users* dialog opens.


Assign Developers role to users
×
Select users
Begin typing to select users...
Cancel
Assign

Select users you want to assign this role to.

3. Begin typing the name of the user to whom you want to assign the role. The list of users is filtered automatically. Select the user.
4. Repeat the previous step until you have added all the users that belong to this role.

5. Click **Assign**. Users that have been added to the role are listed on the **Users** tab.



Developers

Role ID rol_3qCp42i4GRUDAqX8

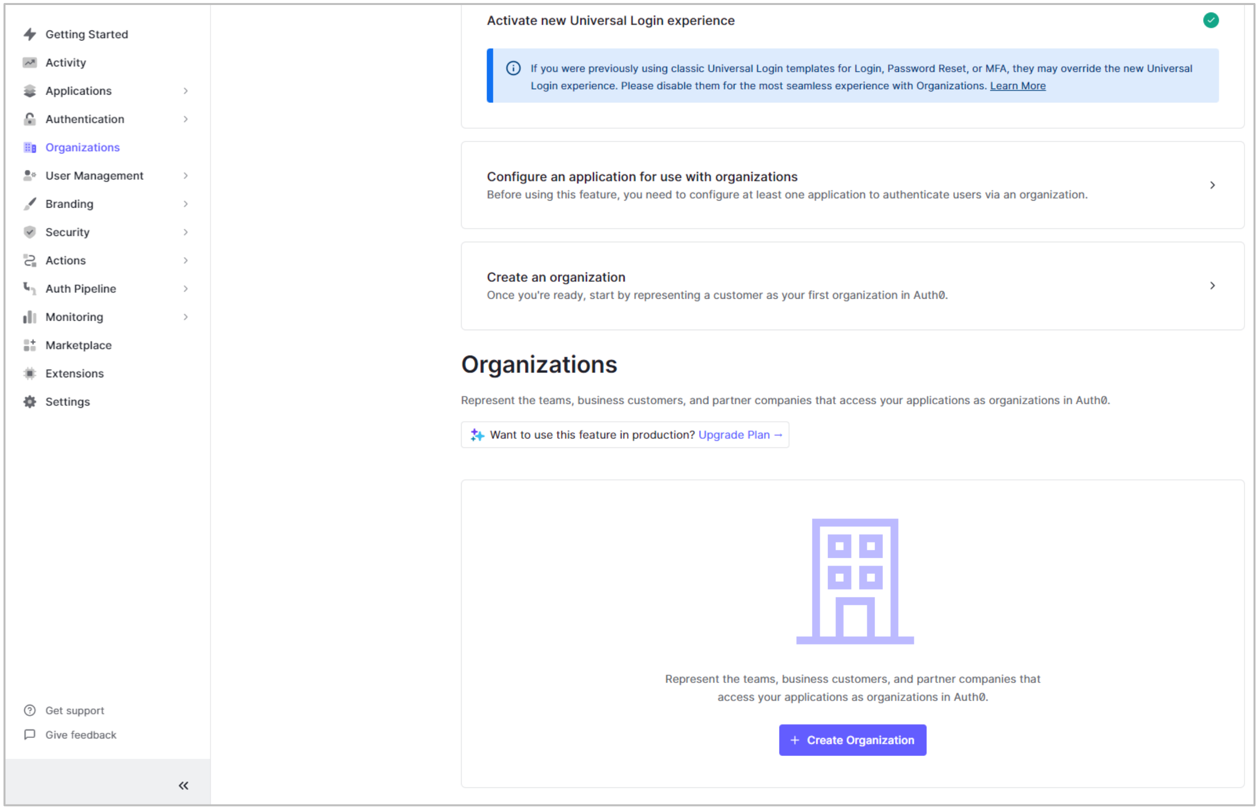
Users that have this role directly assigned.

US user@email.com
user@email.com

4.6 Add an organization

To add an organization, follow the instructions below.

1. From the left pane, select **Organizations**.



Activate new Universal Login experience

If you were previously using classic Universal Login templates for Login, Password Reset, or MFA, they may override the new Universal Login experience. Please disable them for the most seamless experience with Organizations. Learn More

Configure an application for use with organizations
Before using this feature, you need to configure at least one application to authenticate users via an organization.

Create an organization
Once you're ready, start by representing a customer as your first organization in Auth0.

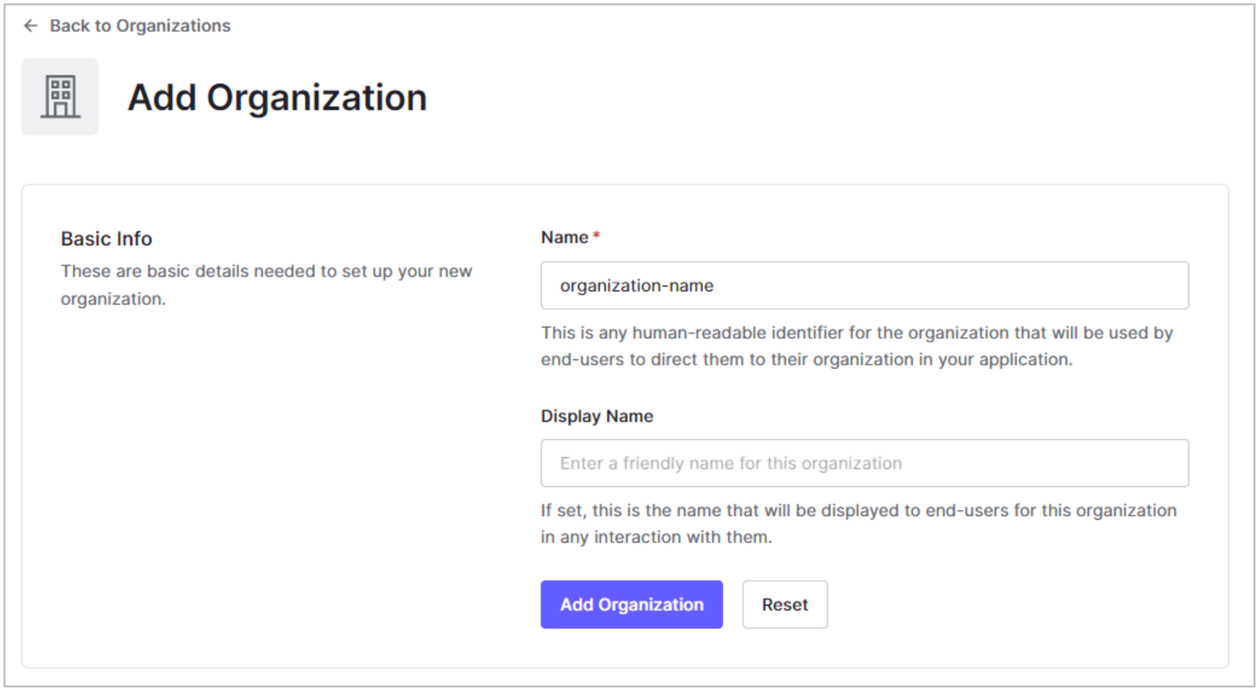
Organizations

Represent the teams, business customers, and partner companies that access your applications as organizations in Auth0.

Want to use this feature in production? Upgrade Plan →

Represent the teams, business customers, and partner companies that access your applications as organizations in Auth0.

2. Click **+ Create Organization**.



← Back to Organizations

Add Organization

Basic Info

These are basic details needed to set up your new organization.

Name *

organization-name

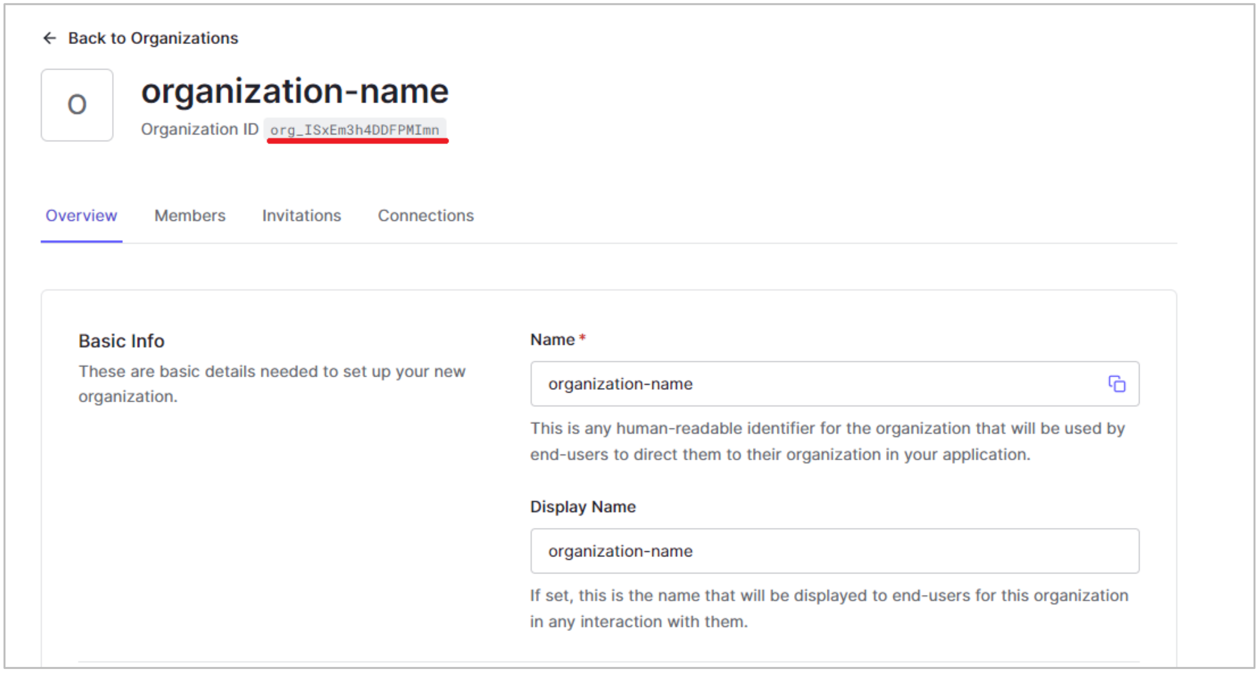
This is any human-readable identifier for the organization that will be used by end-users to direct them to their organization in your application.

Display Name

Enter a friendly name for this organization

If set, this is the name that will be displayed to end-users for this organization in any interaction with them.

3. Enter your organization **Name** and click **Add Organization**.
4. On the Organization page, look for the **Organization ID**, located below the name of your organization.



← Back to Organizations

O organization-name

Organization ID org_ISxEm3h4DDFPMImn

Basic Info

These are basic details needed to set up your new organization.

Name *

organization-name

This is any human-readable identifier for the organization that will be used by end-users to direct them to their organization in your application.

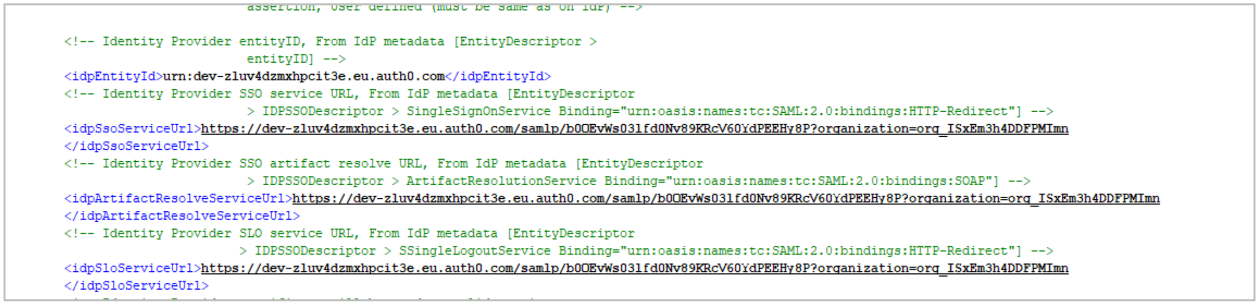
Display Name

organization-name

If set, this is the name that will be displayed to end-users for this organization in any interaction with them.

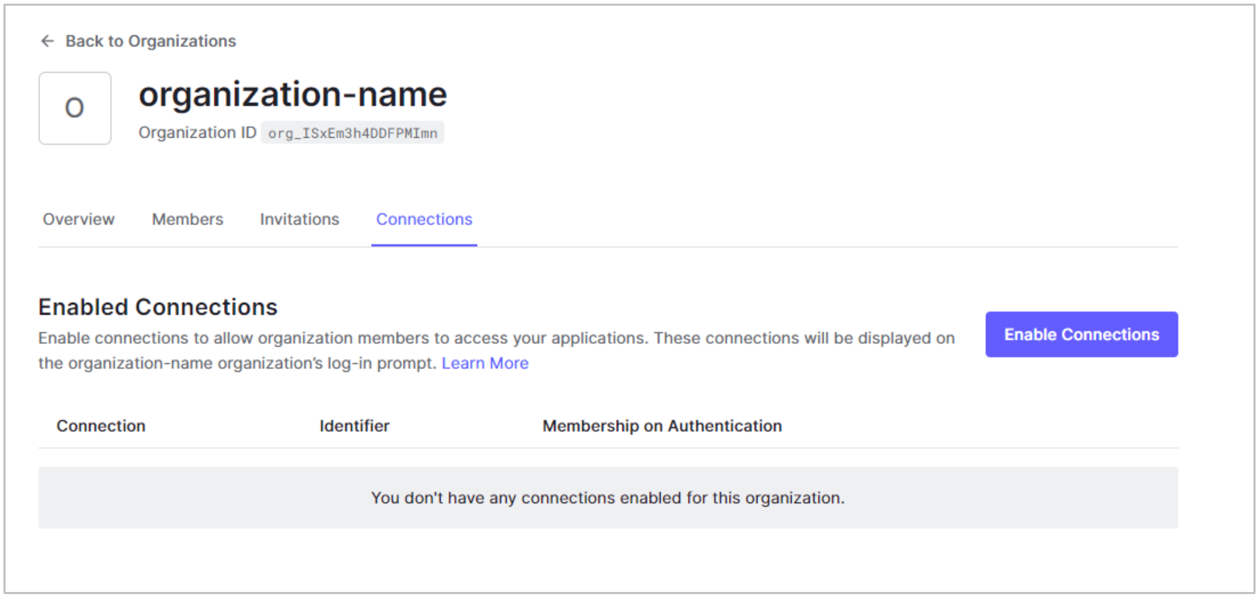
5. Copy this value to the clipboard. In your configuration file, add `?organization={organization-id}` to the end of both the idpSsoServiceUrl and

the idpArtifactResolveServiceUrl. An example is provided below:



```
                        assertion, user defined (must be same as on IdP) -->

<!-- Identity Provider entityID, From IdP metadata [EntityDescriptor >
                        entityID] -->
<idpEntityId>urn:dev-zluv4dzmxhpcit3e.eu.auth0.com</idpEntityId>
<!-- Identity Provider SSO service URL, From IdP metadata [EntityDescriptor
                        > IDPSSODescriptor > SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->
<idpSsoServiceUrl>https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs031fd0Nv89KRcV60YdPEEHy8P?organization=org_ISxEm3h4DDFPMImn
</idpSsoServiceUrl>
<!-- Identity Provider SSO artifact resolve URL, From IdP metadata [EntityDescriptor
                        > IDPSSODescriptor > ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"] -->
<idpArtifactResolveServiceUrl>https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs031fd0Nv89KRcV60YdPEEHy8P?organization=org_ISxEm3h4DDFPMImn
</idpArtifactResolveServiceUrl>
<!-- Identity Provider SLO service URL, From IdP metadata [EntityDescriptor
                       > IDPSSODescriptor > SSingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->
<idpSloServiceUrl>https://dev-zluv4dzmxhpcit3e.eu.auth0.com/samlp/b0OEvWs031fd0Nv89KRcV60YdPEEHy8P?organization=org_ISxEm3h4DDFPMImn
</idpSloServiceUrl>
```

6. To allow organization members to access your applications, you must enable connections. Select the **Connections** tab and click **Enable Connections**.



← Back to Organizations

O **organization-name**

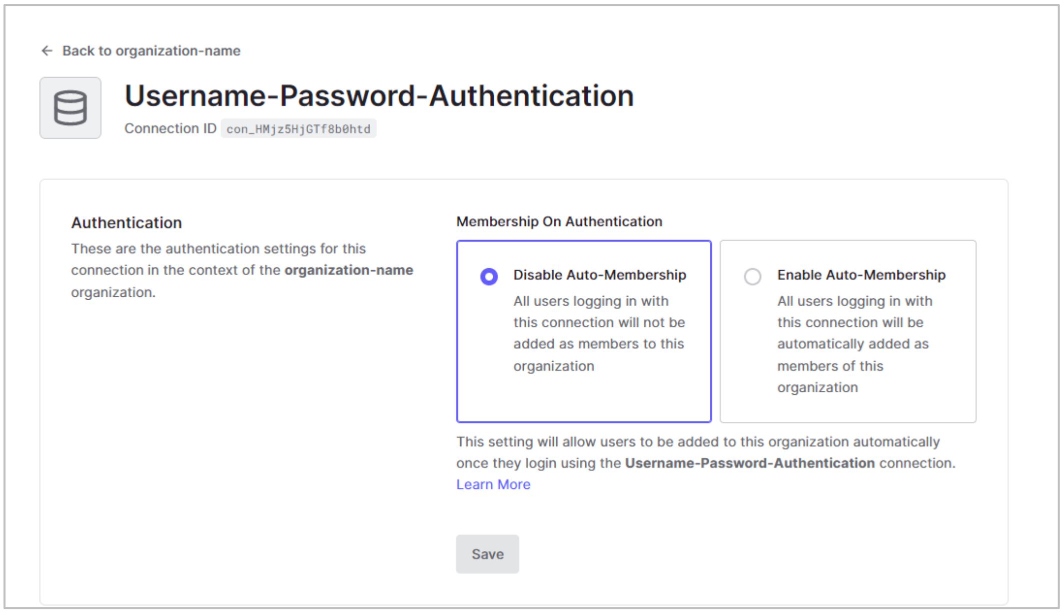
Organization ID `org_ISxEm3h4DDFPMImn`

Enabled Connections

Enable connections to allow organization members to access your applications. These connections will be displayed on the organization-name organization's log-in prompt. Learn More

Connection	Identifier	Membership on Authentication
You don't have any connections enabled for this organization.		

7. Make sure that the Membership on Authentication option is set to **Disable Auto-Membership**. When Auto-Membership is disabled, only members of your organization can log in when this organization is used.



← Back to organization-name

Username-Password-Authentication

Connection ID `con_HMjz5HjGTf8b0htd`

Authentication

These are the authentication settings for this connection in the context of the **organization-name** organization.

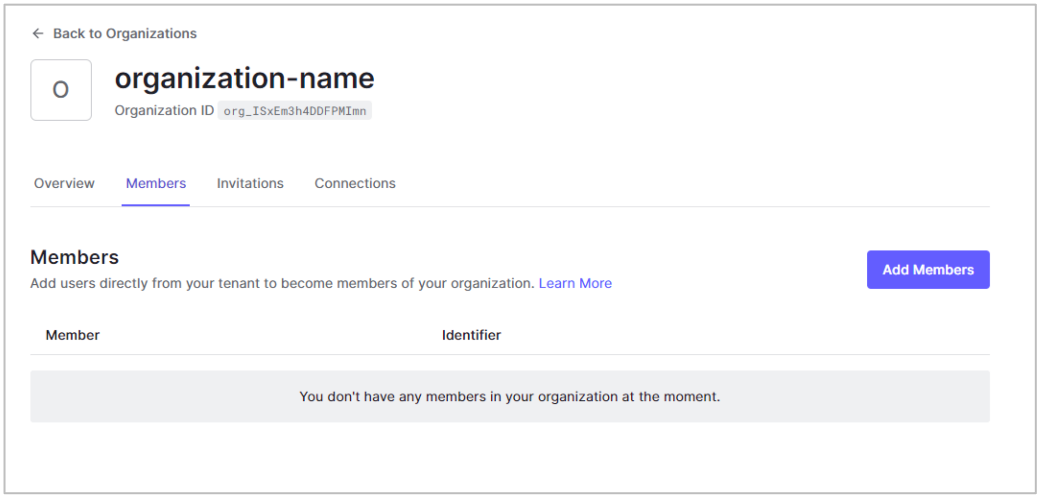
Membership On Authentication

● **Disable Auto-Membership**
All users logging in with this connection will not be added as members to this organization

○ **Enable Auto-Membership**
All users logging in with this connection will be automatically added as members of this organization

This setting will allow users to be added to this organization automatically once they login using the **Username-Password-Authentication** connection. Learn More

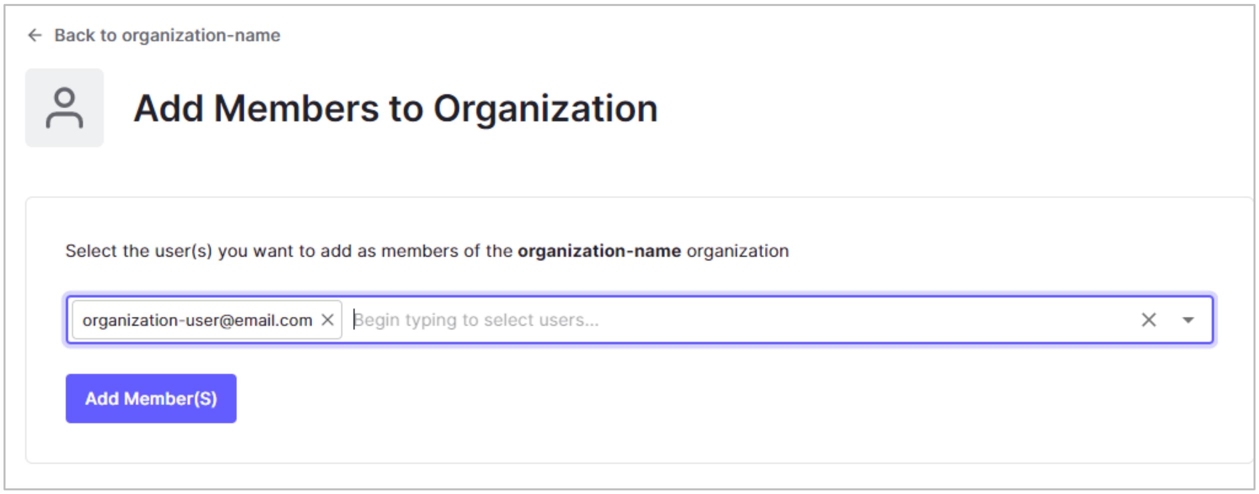
8. Click the **Back to [your organization name]** link in the upper-left corner to return to the page for your organization.
9. Select the **Members** tab to add members:
   a) Click **Add Members**.



Add users directly from your tenant to become members of your organization. Learn More

You don't have any members in your organization at the moment.

   b) Begin entering the name of each user. When the user's name is displayed in the list, select it to add it to the field. Repeat this for each user.
   c) Click **Add Member(s)**.

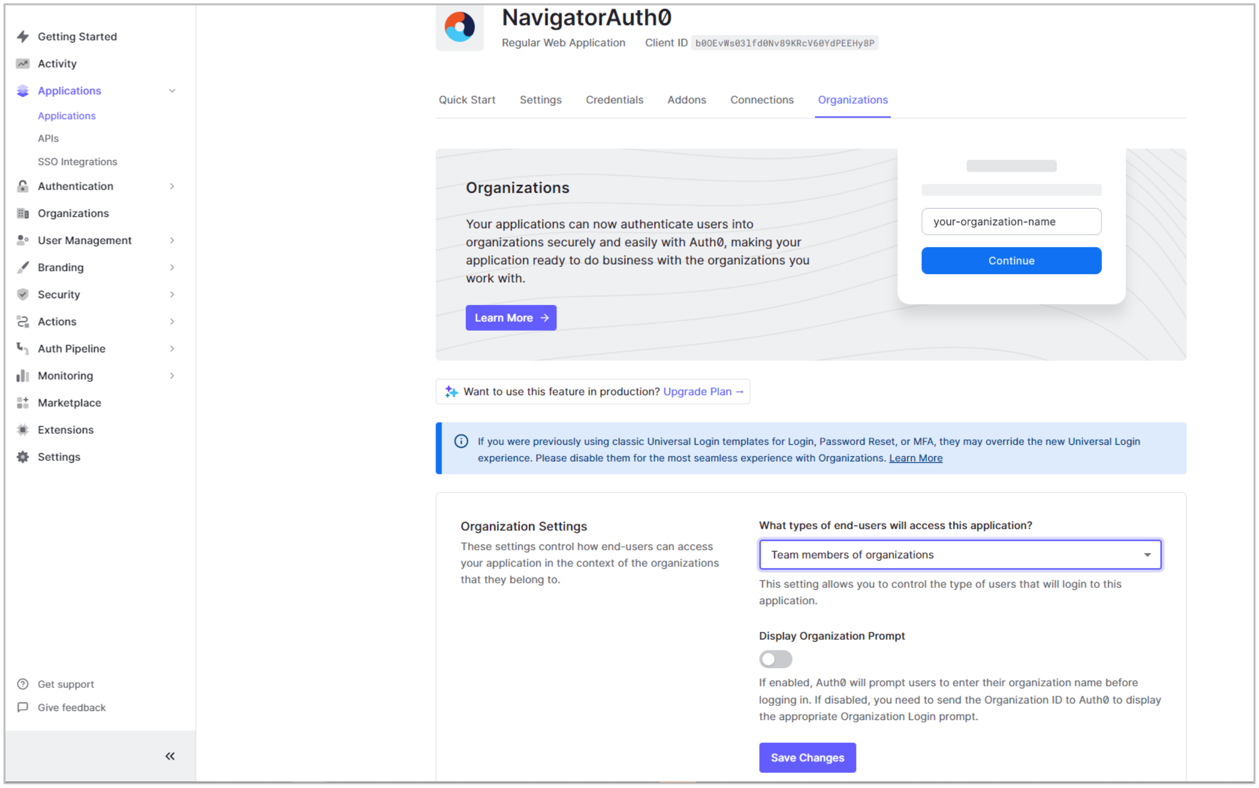


Select the user(s) you want to add as members of the **organization-name** organization

organization-user@email.com × Begin typing to select users...

10. From the left pane, select **Applications**.
11. Select the **Organizations** tab.
12. For the option called **What types of end-users will access this application?**, you can select *Individuals for personal use*, *Team members of organizations*, or *Both*. If you want

only organization users to be able to log in, select *Team members of organizations*.



NavigatorAuth0

Regular Web Application Client ID b0OEvWs03lfd0Nv89KRcV60YdPEEHy8P

Organizations

Your applications can now authenticate users into organizations securely and easily with Auth0, making your application ready to do business with the organizations you work with.

Want to use this feature in production? Upgrade Plan →

If you were previously using classic Universal Login templates for Login, Password Reset, or MFA, they may override the new Universal Login experience. Please disable them for the most seamless experience with Organizations. Learn More

Organization Settings

These settings control how end-users can access your application in the context of the organizations that they belong to.

What types of end-users will access this application?

Team members of organizations

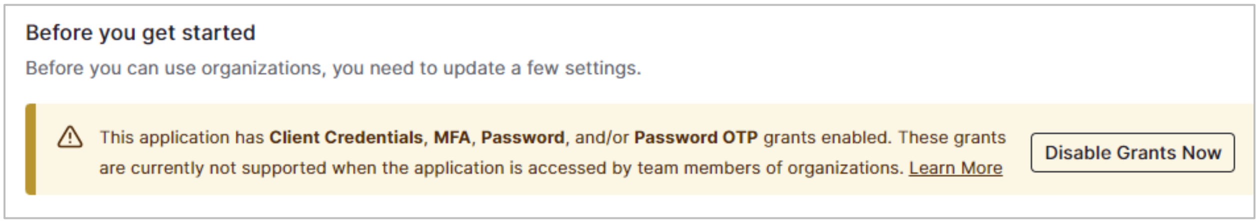
This setting allows you to control the type of users that will login to this application.

Display Organization Prompt

If enabled, Auth0 will prompt users to enter their organization name before logging in. If disabled, you need to send the Organization ID to Auth0 to display the appropriate Organization Login prompt.

NOTE

If the *Team members of organizations* option is unavailable, click **Disable Grants Now** on the same page to make it available. See the image below.



Before you get started

Before you can use organizations, you need to update a few settings.

This application has **Client Credentials**, **MFA**, **Password**, and/or **Password OTP** grants enabled. These grants are currently not supported when the application is accessed by team members of organizations. Learn More

13. Click **Save Changes**.

Chapter 5: Ping (Navigator Example)

5.1 ACS URL Information

Before beginning setup, a secure ACS URL must be established.

Sample ACS URL:

https://ip:port/navigator-server/ssologin/navigator

The secure ACS URL consists of the following parts:

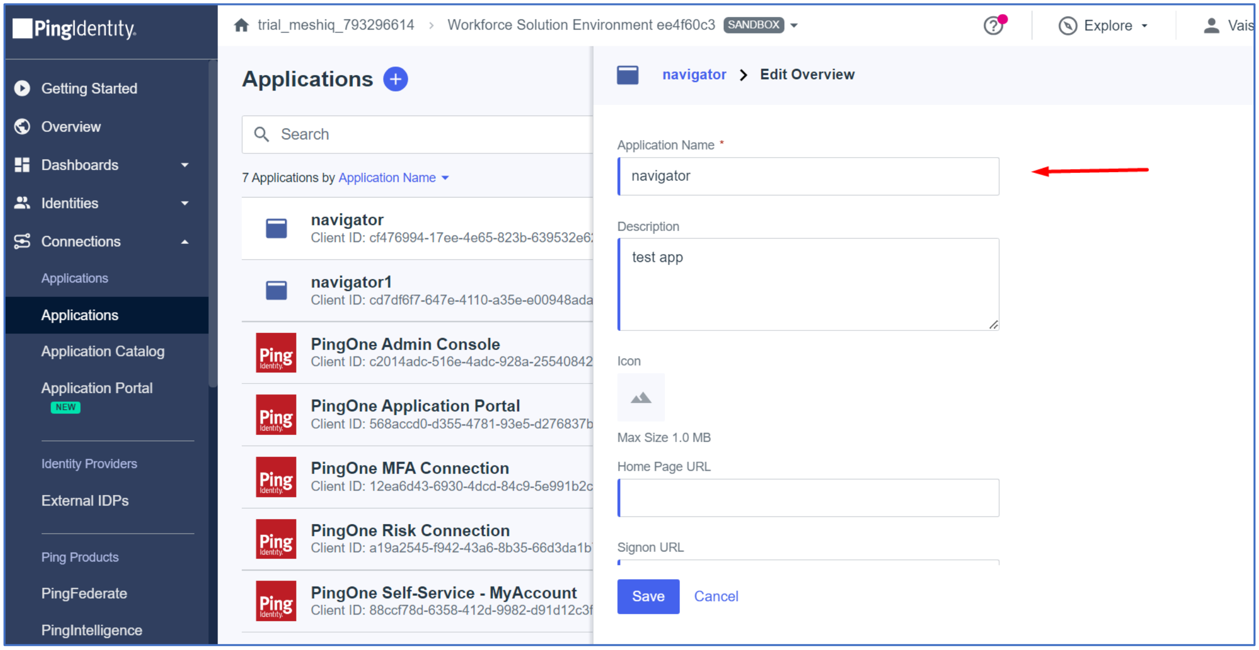
Table 4 ACS URL Parts

Part of URL	Explanation	Provided by:
https://	The URL must use the secure HTTPS protocol.	N/A
ip:port/	This is the customer's IP address and port.	Customer
navigator-server/ssologin/navigator	Subdirectory and path. The last part of the ACS URL path (navigator) is the Entity ID.	meshIQ

5.2 Create and configure the navigator application

1. In the PingOne console menu, select **Connections > Applications**.
2. Click ⊕ to add a new application.

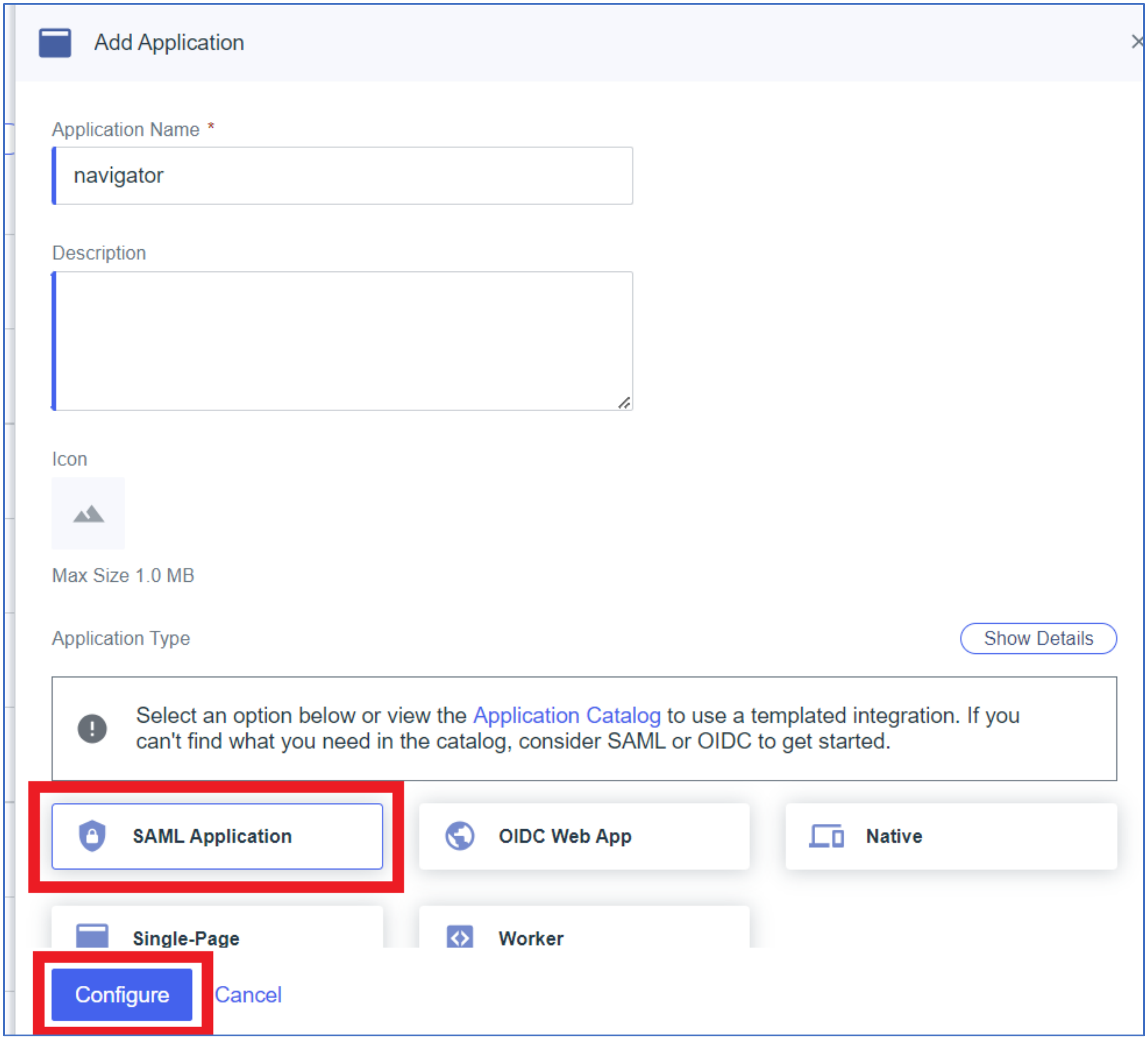
3. Enter "navigator" for the **Application Name**.


PingIdentity.
trial_meshiq_793296614 > Workforce Solution Environment ee4f60c3 SANDBOX
Explore
Vais
Getting Started
Overview
Dashboards
Identities
Connections
Applications
Applications
Application Catalog
Application Portal NEW
Identity Providers
External IDPs
Ping Products
PingFederate
PingIntelligence
Applications
Search
7 Applications by Application Name
navigator
Client ID: cf476994-17ee-4e65-823b-639532e6
navigator1
Client ID: cd7df6f7-647e-4110-a35e-e00948ada
PingOne Admin Console
Client ID: c2014adc-516e-4adc-928a-25540842
PingOne Application Portal
Client ID: 568accd0-d355-4781-93e5-d276837b
PingOne MFA Connection
Client ID: 12ea6d43-6930-4dcd-84c9-5e991b2c
PingOne Risk Connection
Client ID: a19a2545-f942-43a6-8b35-66d3da1b
PingOne Self-Service - MyAccount
Client ID: 88ccf78d-6358-412d-9982-d91d12c3f
navigator > Edit Overview
Icon
Max Size 1.0 MB
Home Page URL
Signon URL
Save
Cancel

Application Name *: navigator

Description: test app

4. Select the **SAML Application** option.



Add Application

Application Name *

navigator

Description

Icon

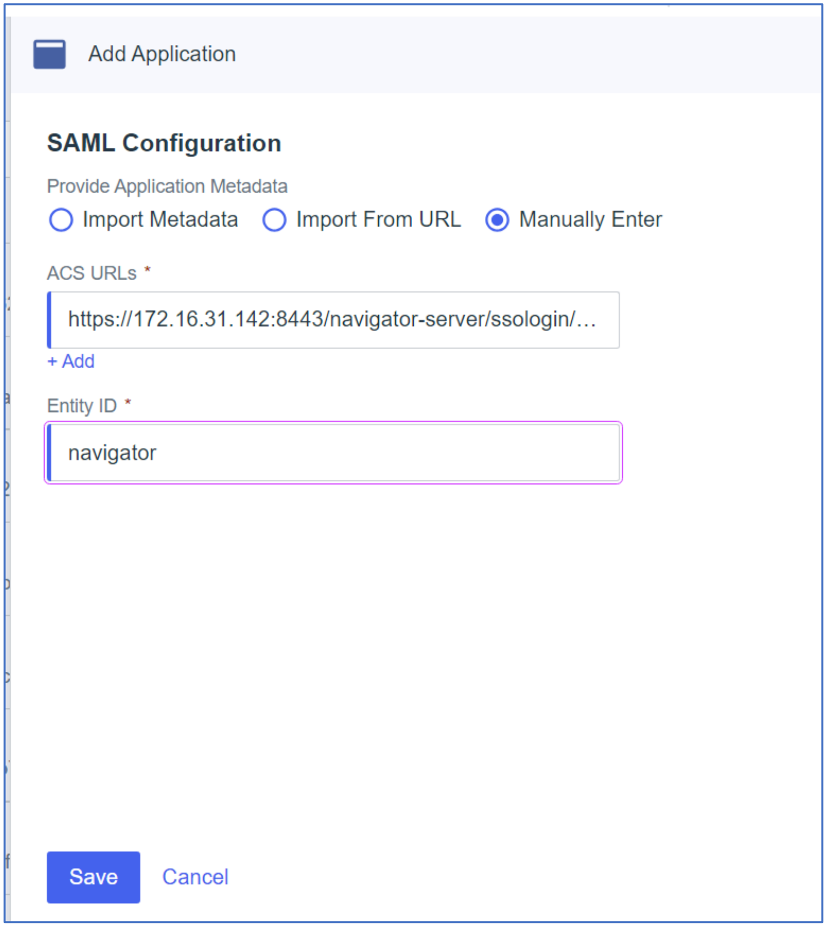
Max Size 1.0 MB

Application Type

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.

5. Click **Configure** to open SAML configuration.
6. In the SAML configuration, under Provide Application Metadata, select the **Manually Enter** option button. Add the **ACL URL** (described earlier in the *ACS URL* section).

7. Enter "navigator" for the **Entity ID**. The Entity ID is the last part of the ACS URL path. For example: navigator-server/ssologin/**navigator**.



Add Application

SAML Configuration

Provide Application Metadata

○ Import Metadata ○ Import From URL ● Manually Enter

ACS URLs *

https://172.16.31.142:8443/navigator-server/ssologin/…

Entity ID *

navigator

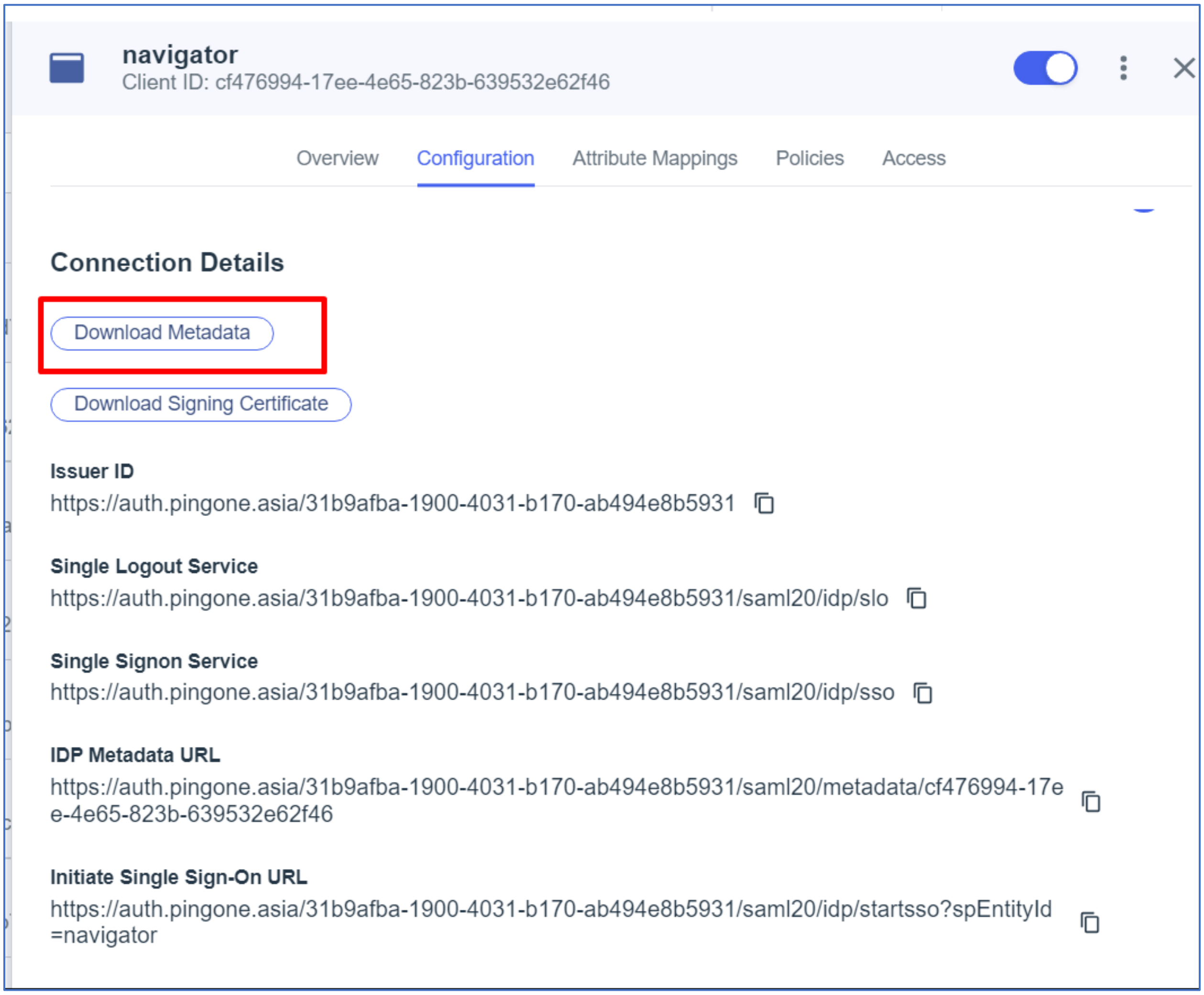
8. Click **Save**.

9. Go to the Configuration tab of the application.

10. Click **Download Metadata** to download a file containing the metadata that you will use to configure the apwmq_samlsso.xml file.

5.3 Configure the apwmq_samlsso.xml file

1. Using the information on the Configuration tab and the downloaded metadata, refer to the table below to configure apwmq_samlsso.xml:



navigator
Client ID: cf476994-17ee-4e65-823b-639532e62f46

Connection Details

Issuer ID
https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931

Single Logout Service
https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931/saml20/idp/slo

Single Signon Service
https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931/saml20/idp/sso

IDP Metadata URL
https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931/saml20/metadata/cf476994-17ee-4e65-823b-639532e62f46

Initiate Single Sign-On URL
https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931/saml20/idp/startsso?spEntityId=navigator

Table 5 PingOne Parameter Mapping

PingOne Console Connection Details page	XML Parameter
Issuer ID	Used for idpEntityId *https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931* Also used in the service URLs.
Single Logout Service	Used for idpSloServiceUrl

Table 5 PingOne Parameter Mapping

PingOne Console Connection Details page	XML Parameter
	Example: https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931/saml20/idp/slo
Single Signon Service	Used for idpSsoServiceUrl. Also used in the idpArtifactResolveServiceUrl. Example: https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931/saml20/idp/sso
IDP Metadata URL	The Url from which metadata can be downloaded. (Opening this URL performs the same action as the Download Metadata link.) Example: https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931/saml20/metadata/cf476994-17ee-4e65-823b-639532e62f46
Initiate Single Sign-On URL	The Single Sign-On URL is the URL to which users are redirected after they provide their username and password for their chosen identity provider. Example: https://auth.pingone.asia/31b9afba-1900-4031-b170-ab494e8b5931/saml20/idp/startsso?spEntityId=navigator
<ds:X509Certificate> (See downloaded metadata)	Used for idpSignCert.

2. Add two more properties in the apwmq_samlsso.xml file. These are required for the PingOne identity provider only. (They are not used by other identity providers.)

   <protocolPostBinding>true</protocolPostBinding>

   <contextComparison>none</contextComparison>

NOTE

The contextComparison value of "none" removes entity id conflicts, preventing an INVALID ACS URL error.

5.4 Sample apwmq_samlsso.xml file using Ping

```
<!-- SAML SSO handlers configurations  -->
<configs>


<!-- ping SAML SSO handler configuration -->
```

```
    <config>
        <!-- Unique name to select required handler, User defined -->
            <name>navigator</name>
        <!-- Description to show on link or button, User defined -->
            <descr>Login via ping SSO</descr>
        <!-- Position, User defined -->
            <position>2</position>
        <!-- Service Provider client ID, issuer on authentication request, User
                        defined (must be same as on IdP) -->
            <spEntityId> navigator</spEntityId>
        <!-- Service Provider certificate will be used to sign requests or decrypt
                        assertion, User defined (must be same as on IdP) -->


        <!-- Identity Provider entityID, From IdP metadata [EntityDescriptor >
                        entityID] -->
            <idpEntityId>https://auth.pingone.asia/31b9afba-1900-4031-b170-
ab494e8b5931</idpEntityId>
        <!-- Identity Provider SSO service URL, From IdP metadata [EntityDescriptor
                        > IDPSSODescriptor > SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->
            <idpSsoServiceUrl>https://auth.pingone.asia/31b9afba-1900-4031-b170-
ab494e8b5931/saml20/idp/sso
            </idpSsoServiceUrl>
        <!-- Identity Provider SSO artifact resolve URL, From IdP metadata [EntityDescriptor
                        > IDPSSODescriptor > ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"] -->
            <idpArtifactResolveServiceUrl>https://auth.pingone.asia/31b9afba-1900-4031-
b170-ab494e8b5931/saml20/idp/sso
            </idpArtifactResolveServiceUrl>
        <!-- Identity Provider SLO service URL, From IdP metadata [EntityDescriptor
                        > IDPSSODescriptor > SSingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"] -->
            <idpSloServiceUrl>https://auth.pingone.asia/31b9afba-1900-4031-b170-
ab494e8b5931/saml20/idp/slo
            </idpSloServiceUrl>
        <!-- Identity Provider certificate will be used to validate signatures,
                        From IdP metadata [EntityDescriptor > IDPSSODescriptor > KeyDescriptor use="signing"
                > KeyInfo > X509Data > X509Certificate] -->
```

```
<idpSignCert>

MIIDrjCCApagAwIBAgIGAYqTP6JpMA0GCSqGSIb3DQEBCwUAMIGXMQswCQYDVQQGEwJVU
zEWMBQGA1UECgwNUGluZyBJZGVudGl0eTEWMBQGA1UECwwNUGluZyBJZGVudGl0eTFYM
FYGA1UEAwxPUGluZ09uZSBTU08gQ2VydGlmaWNhdGUgZm9yIFdvcmtmb3JjZSBTb2x1dGlv
biBFbnZpcm9ubWVudCBlZTRmNjBjMyBlbnZpcm9ubWVudDAeFw0yMzA5MTQxMDMyMTVa
Fw0yNDA5MTMxMDMyMTVaMIGXMQswCQYDVQQGEwJVUzEWMBQGA1UECgwNUGluZyBJ
ZGVudGl0eTEWMBQGA1UECwwNUGluZyBJZGVudGl0eTFYMFYGA1UEAwxPUGluZ09uZSBTU
08gQ2VydGlmaWNhdGUgZm9yIFdvcmtmb3JjZSBTb2x1dGlvbiBFbnZpcm9ubWVudCBlZTRm
NjBjMyBlbnZpcm9ubWVudDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1i4Q
O5bil5lpggldWl80bV4RSUuaZi/saDnL5ULwmFk2l2noBIFCasAVhw8N9UdhVouO3gQyexdgDe
QeE0XaAPC23QLB/g0E9hxjYJbxOrA7efKnkDHIBCIrtDJfoqX0tmyTxSBg4Ci13NAi9ODjeJ+gG9q
ynUKTpfPN/rCwifaN+8yKEVsVVnKUBmjIqtRGIf1A6NRE8Mw9NBk1hHE6fi8YHbnCnY0noSygC
JLgP4g+NM47u1Ph1NMoepLNJ/lF0ZYTBbjOm0uTHTORkxBBgYFBw1tTEvSCAGiRkgQxNL6Q2
ec0ZtXE4h/lMiN5bySvp7BOJcGBsxSKtLODu4LgMCAwEAATANBgkqhkiG9w0BAQsFAAOCAQE
ArGRww/reXNEPS31c5PEInD5a/NHbLaGXHxfz058eon5i8QJ/HTV5x8WwAfVMlcccyVgVeLaqU
dhC3B1UVAPepkKL4doTqXj/KgAt5bx6GKSRSd0USftLLZFR0ZvVag4V0hHJNqekM+/s/ZPU+2S
6PRJS2WwY5qotHpcfHCt0luDMasOQMWcA/2S8O15RF6WQHLlOspfzT8f6/qVZF3A9+O6h9lIG
Xy+zvpCHVD9tZbahKFXbq2bJoSV+qWxlfOj1j2bivMQg81i00MnjSdzeR9ksem/yizBa142FqQNs
n1N0lLDIxLpNtWskwJR+JvP1L1f0hbgrKxavIiSb7N5mpA==

</idpSignCert>

          <!-- Service Provider must sign authentication request, User defined -->

            <authnRequestSigned>true</authnRequestSigned>

          <!-- Service Provider must sign artifact resolve request, User defined -->

            <resolveArtifactRequestSigned>true</resolveArtifactRequestSigned>

          <!-- Service Provider must sign logout request, User defined -->

            <logoutRequestSigned>true</logoutRequestSigned>

          <!-- Image can be added /image/path/img.* By default it will display an icon -->

          <!-- <buttonIcon>image.png</buttonIcon>-->

          <!-- true or false. If true, the protocol changes from the default HTTP Artifact Binding to the HTTP POST
Binding uri. -->

            <protocolPostBinding>true</protocolPostBinding>

          <!-- changes the comparison type, can be "none", "minimum"(default one), "maximum", "exact",
"better".-->

            <contextComparison>none</contextComparison>

            <buttonText>ping login</buttonText>

            <buttonColor>#ffffff</buttonColor>

      </config>

</configs>
```

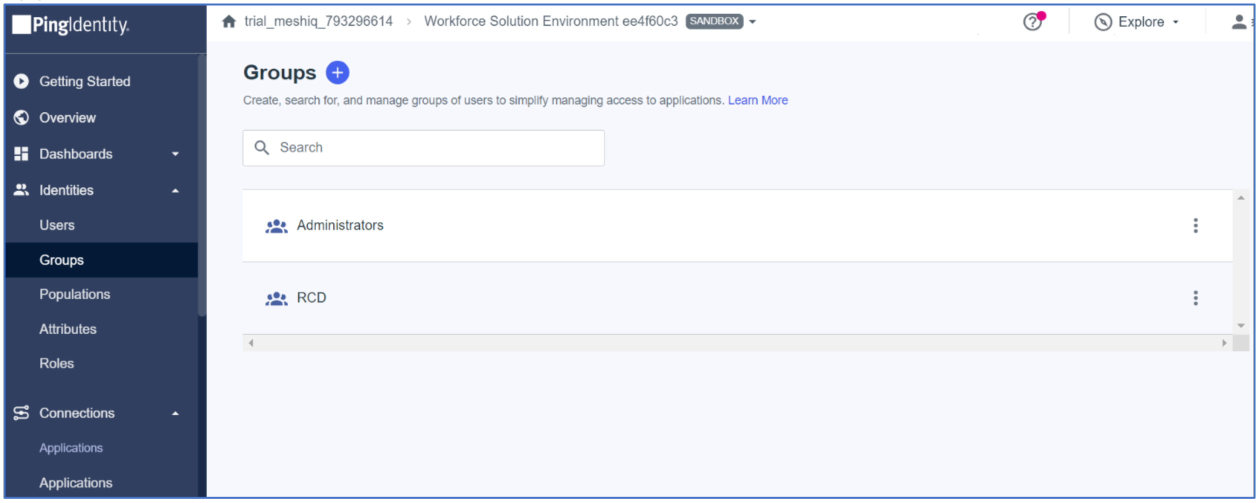
5.5 Groups and users

The next step is to define groups and users.

You can manage user groups in PingOne. Create a group in PingOne that has the same name as an existing Enterprise Manager group. Assign a user to it. When PingOne is used for the identity provider at login, the user is created in Enterprise Manager and assigned to the same-named Enterprise Manager group.

5.5.1 Add a group

1. On the PingOne console menu, select Identities > Groups.
2. Click ⊕ to add a group.
3. Define the group which is present in Enterprise Manager and meshIQ's security application.



Groups ⊕

Create, search for, and manage groups of users to simplify managing access to applications. Learn More

Administrators

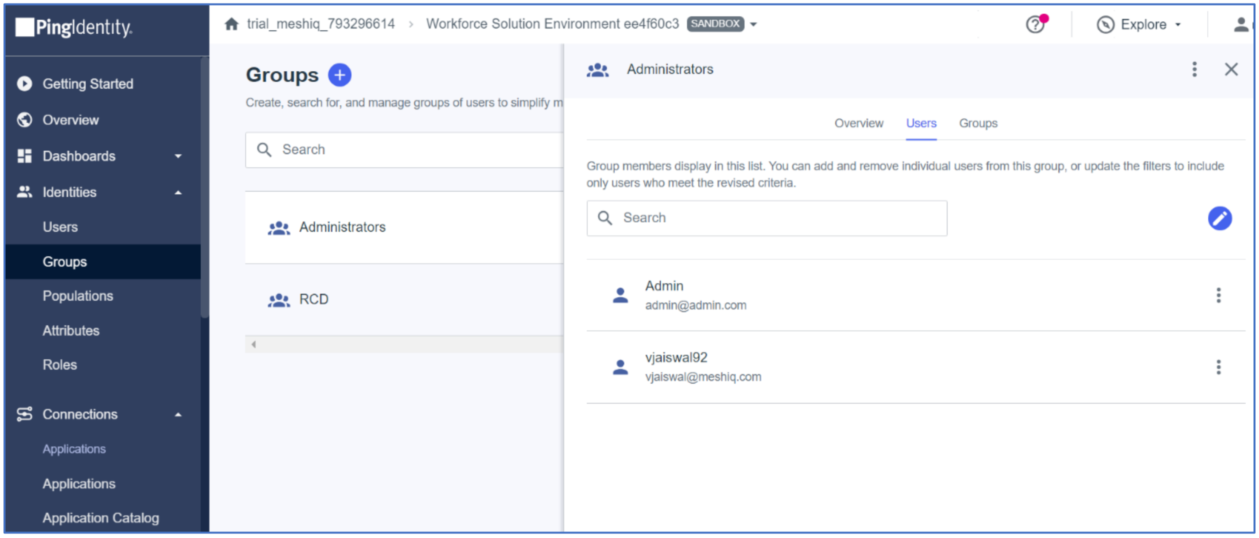
RCD

4. In Enterprise Manager, make sure that users are defined and assigned to this group.

5.5.2 Add users to a PingOne group

To view the current members of a group:

1. On the PingOne console menu, select **Identities > Groups**.
2. Click a group and select the Users tab:



Group members display in this list. You can add and remove individual users from this group, or update the filters to include only users who meet the revised criteria.

Admin
admin@admin.com

vjaiswal92
vjaiswal@meshiq.com

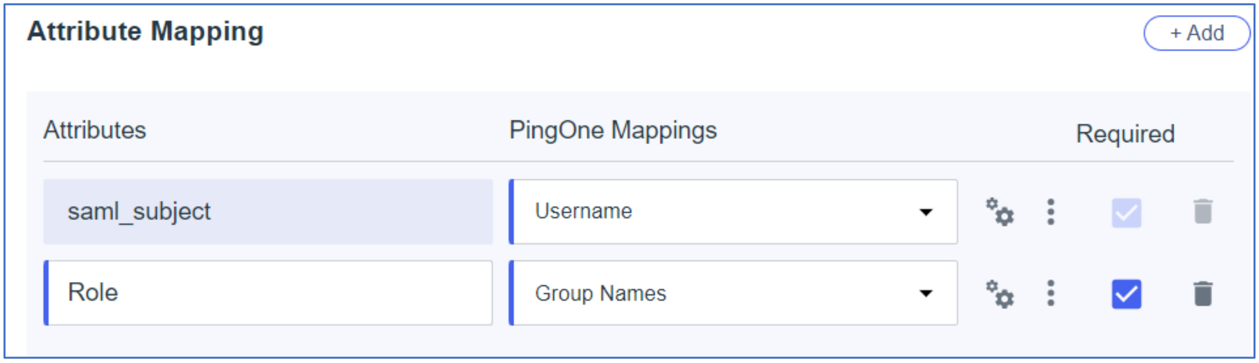
To add additional users, do one of the following:

- **From Groups:** Click ✎ on the Users tab, then select **Add/Remove Users** from the pop-up menu. Select the check boxes of the users you want to add to the group.
- **From Users:** On the PingOne console menu, select **Identities > Users**. Select a user to edit it. Select the Groups tab. Click ✎. Select the groups to which you want to add the user.

5.6 Application configuration for users and groups

5.6.1 Map SAML to PingOne attributes

1. On the PingOne console menu, select **Connections > Applications**.
2. Select the Navigator application and select the Attribute Mappings tab to map SAML attributes to PingOne attributes.
3. Click ✎ to edit the mappings.

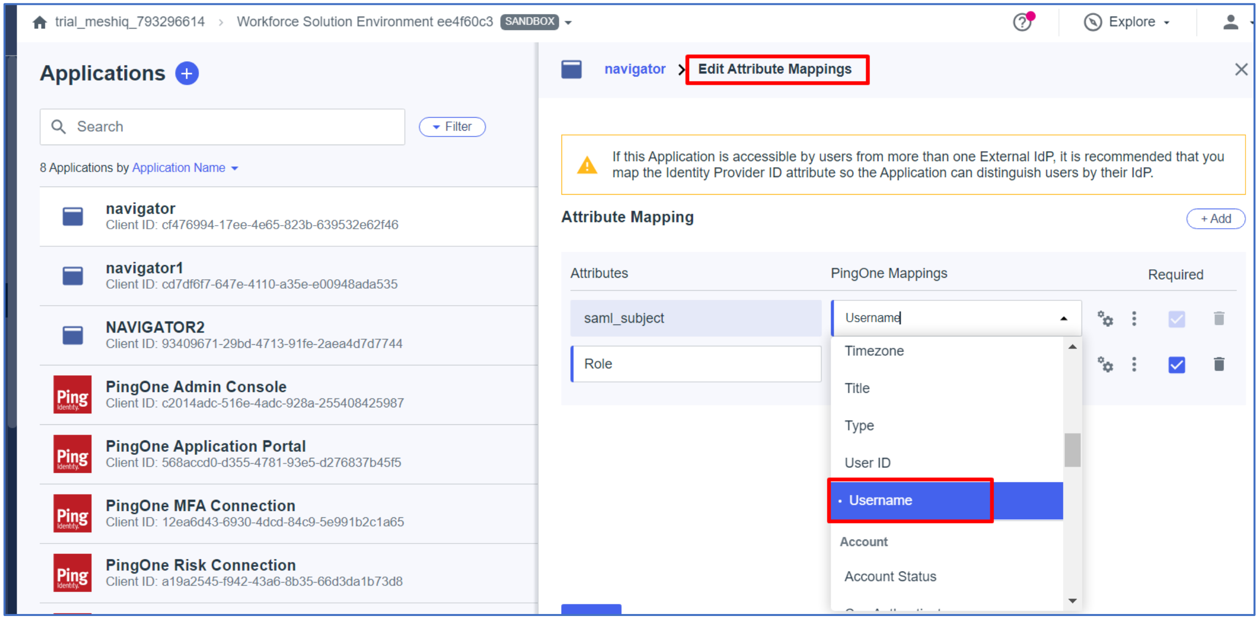


Attribute Mapping

+ Add

Attributes	PingOne Mappings	Required
saml_subject	Username	☑
Role	Group Names	☑

4. By default, saml_subject is mapped to User ID. However, since User ID values are not generated in a format that makes them easy to recognize, the best practice is to map the saml_subject SAML attribute to the PingOne Username.



trial_meshiq_793296614 › Workforce Solution Environment ee4f60c3 SANDBOX

Explore

Applications +

Search

Filter

8 Applications by Application Name

navigator
Client ID: cf476994-17ee-4e65-823b-639532e62f46

navigator1
Client ID: cd7df6f7-647e-4110-a35e-e00948ada535

NAVIGATOR2
Client ID: 93409671-29bd-4713-91fe-2aea4d7d7744

PingOne Admin Console
Client ID: c2014adc-516e-4adc-928a-255408425987

PingOne Application Portal
Client ID: 568accd0-d355-4781-93e5-d276837b45f5

PingOne MFA Connection
Client ID: 12ea6d43-6930-4dcd-84c9-5e991b2c1a65

PingOne Risk Connection
Client ID: a19a2545-f942-43a6-8b35-66d3da1b73d8

navigator > Edit Attribute Mappings

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.

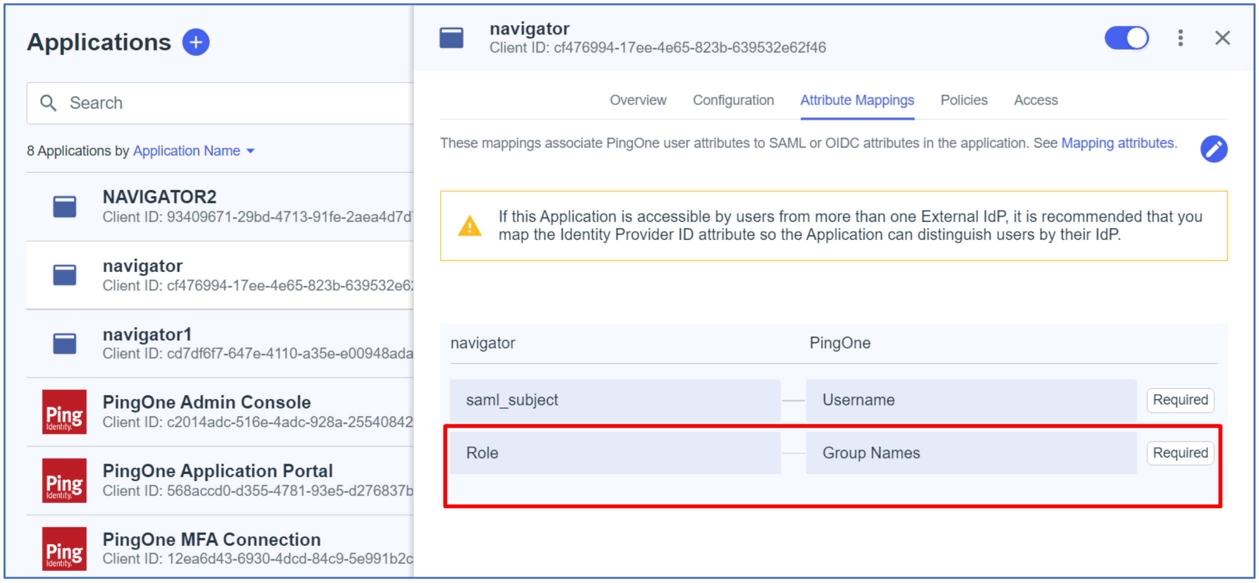
Attribute Mapping

+ Add

Attributes	PingOne Mappings	Required
saml_subject	Username	☑
Role		☑

5. Mark saml_subject and Role as Required fields. Select the **Required** check box to define the attribute as required for the application.
6. Enter “Role” in the second row under Attributes, and select **Group Names** from the PingOne Mappings list.

7. Click **Save** to return to the Attribute mappings tab.



Applications ⊕

Search

8 Applications by Application Name ▾

NAVIGATOR2
Client ID: 93409671-29bd-4713-91fe-2aea4d7d

navigator
Client ID: cf476994-17ee-4e65-823b-639532e6

navigator1
Client ID: cd7df6f7-647e-4110-a35e-e00948ada

PingOne Admin Console
Client ID: c2014adc-516e-4adc-928a-25540842

PingOne Application Portal
Client ID: 568accd0-d355-4781-93e5-d276837b

PingOne MFA Connection
Client ID: 12ea6d43-6930-4dcd-84c9-5e991b2c

navigator
Client ID: cf476994-17ee-4e65-823b-639532e62f46

Overview | Configuration | Attribute Mappings | Policies | Access

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.

navigator	PingOne	
saml_subject	Username	Required
Role	Group Names	Required

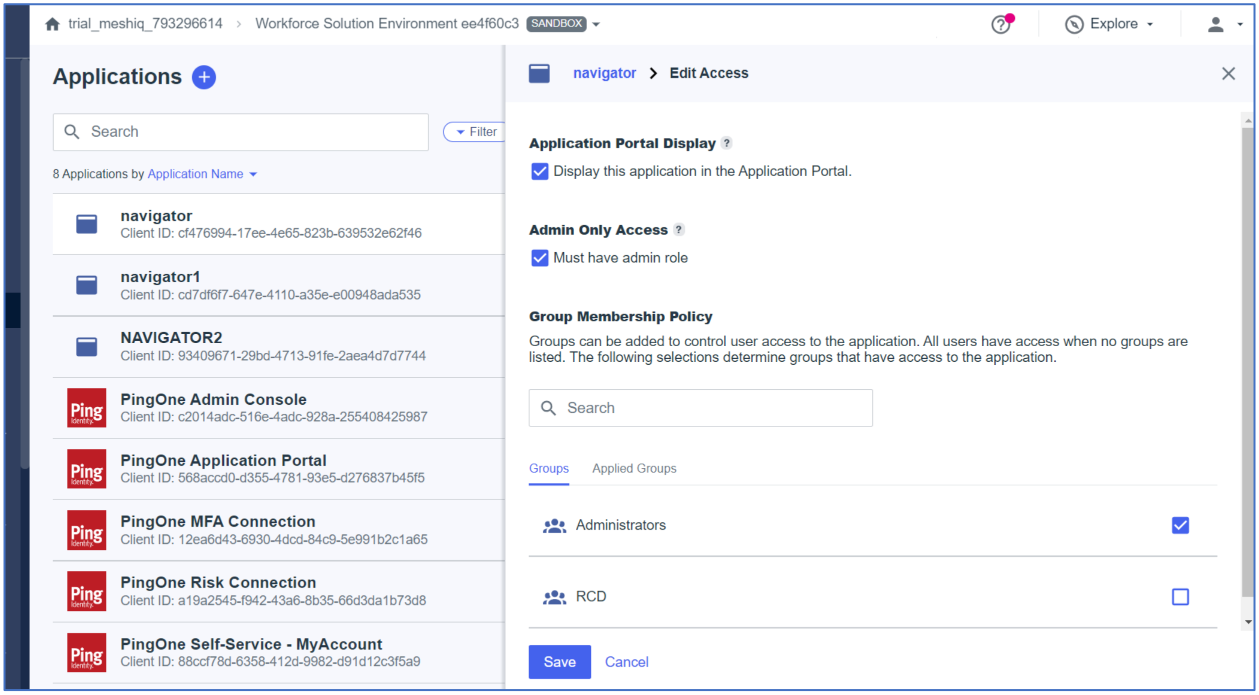
5.6.2 Provide application access to groups

1. If you are not already working on the application, select **Connections > Applications** on the PingOne console menu.

2. Select the Navigator application and select the Access tab.

3. Click ✎ to edit access settings for the application.

4. Provide access to one or more groups by selecting the check box next to each one. To view a list of the selected groups only, click **Applied Groups** above the list.



trial_meshiq_793296614 › Workforce Solution Environment ee4f60c3 SANDBOX ▾ | Explore ▾

Applications ⊕

Search | Filter

8 Applications by Application Name ▾

navigator
Client ID: cf476994-17ee-4e65-823b-639532e62f46

navigator1
Client ID: cd7df6f7-647e-4110-a35e-e00948ada535

NAVIGATOR2
Client ID: 93409671-29bd-4713-91fe-2aea4d7d7744

PingOne Admin Console
Client ID: c2014adc-516e-4adc-928a-255408425987

PingOne Application Portal
Client ID: 568accd0-d355-4781-93e5-d276837b45f5

PingOne MFA Connection
Client ID: 12ea6d43-6930-4dcd-84c9-5e991b2c1a65

PingOne Risk Connection
Client ID: a19a2545-f942-43a6-8b35-66d3da1b73d8

PingOne Self-Service - MyAccount
Client ID: 88ccf78d-6358-412d-9982-d91d12c3f5a9

navigator › 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

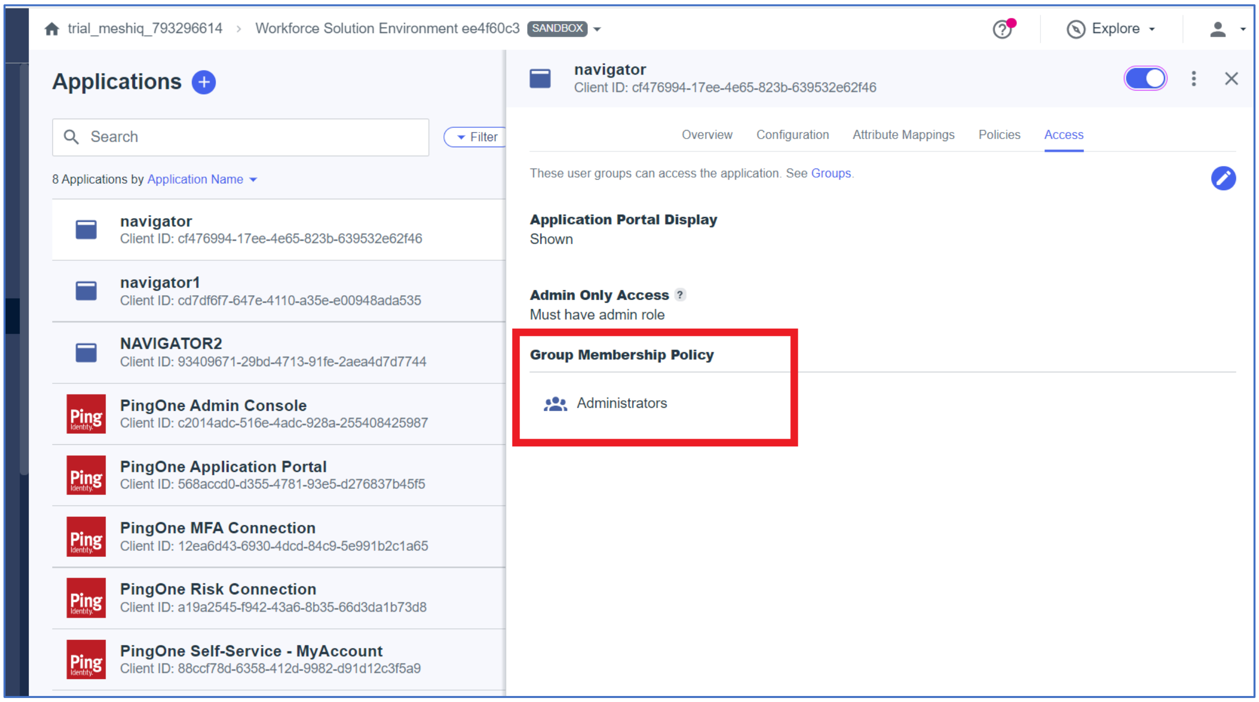
Groups | Applied Groups

Administrators ☑

RCD □

Save | Cancel

5. Click **Save** to return to the Access tab.



trial_meshiq_793296614 › Workforce Solution Environment ee4f60c3 SANDBOX
Explore
Applications
Search
Filter
8 Applications by Application Name
Overview
Configuration
Attribute Mappings
Policies
Access

navigator
Client ID: cf476994-17ee-4e65-823b-639532e62f46

navigator1
Client ID: cd7df6f7-647e-4110-a35e-e00948ada535

NAVIGATOR2
Client ID: 93409671-29bd-4713-91fe-2aea4d7d7744

PingOne Admin Console
Client ID: c2014adc-516e-4adc-928a-255408425987

PingOne Application Portal
Client ID: 568accd0-d355-4781-93e5-d276837b45f5

PingOne MFA Connection
Client ID: 12ea6d43-6930-4dcd-84c9-5e991b2c1a65

PingOne Risk Connection
Client ID: a19a2545-f942-43a6-8b35-66d3da1b73d8

PingOne Self-Service - MyAccount
Client ID: 88ccf78d-6358-412d-9982-d91d12c3f5a9

navigator
Client ID: cf476994-17ee-4e65-823b-639532e62f46

These user groups can access the application. See Groups.

Application Portal Display
Shown

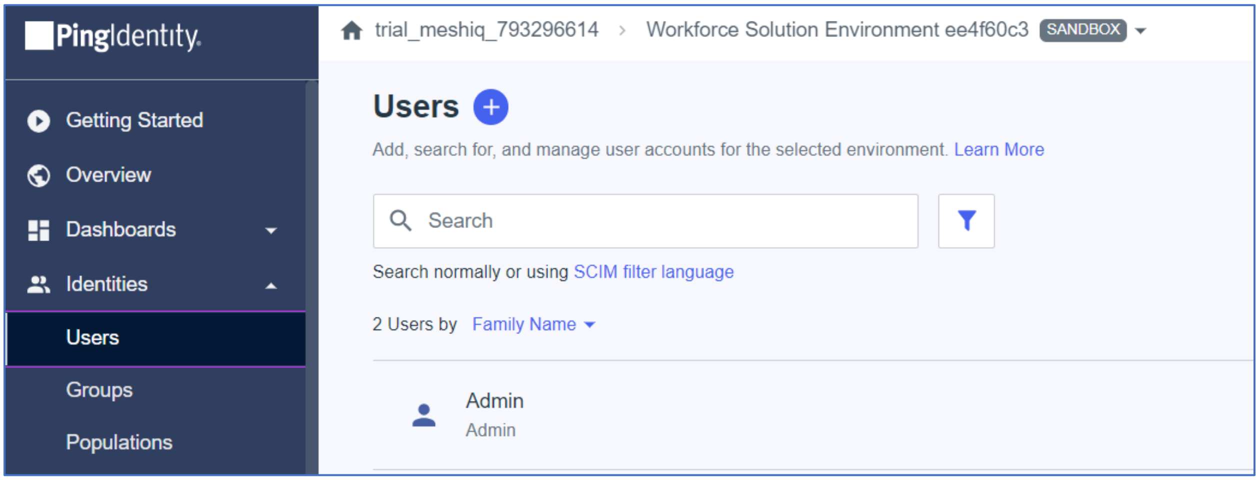
Admin Only Access
Must have admin role

Group Membership Policy
Administrators

5.7 Grant user roles

IMPORTANT! You must grant all users the Organization admin role.

1. On the PingOne console menu, select **Identities > Users**.
2. Select a user on the left to edit it.



Add, search for, and manage user accounts for the selected environment. Learn More

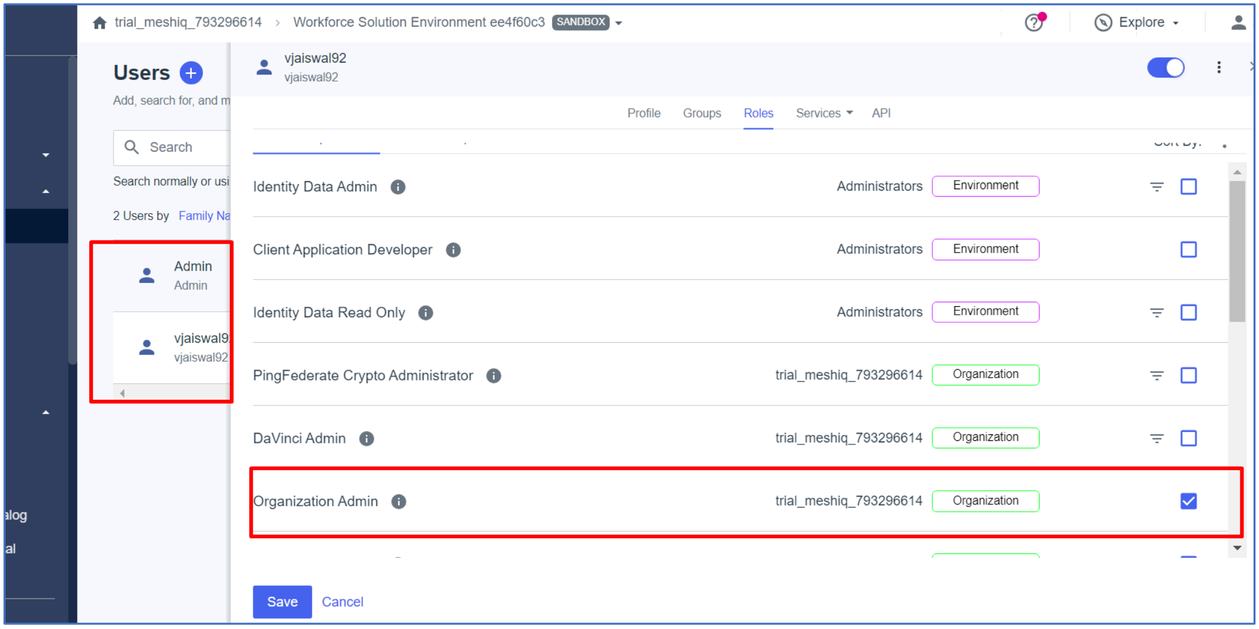
Search normally or using SCIM filter language

2 Users by Family Name

Admin
Admin

3. Select the Roles tab.

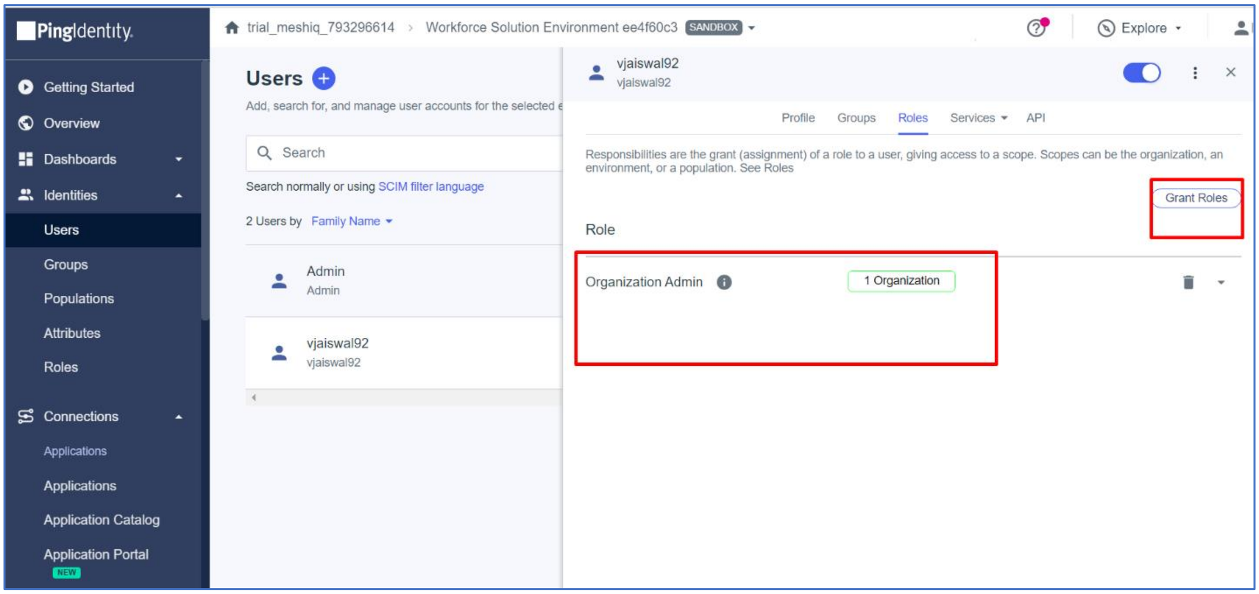
4. To add roles to the user, click **Grant roles**. Available responsibilities are listed.



Identity Data Admin	Administrators	Environment	□
Client Application Developer	Administrators	Environment	□
Identity Data Read Only	Administrators	Environment	□
PingFederate Crypto Administrator	trial_meshiq_793296614	Organization	□
DaVinci Admin	trial_meshiq_793296614	Organization	□
Organization Admin	trial_meshiq_793296614	Organization	☑

5. Select the Organization Admin responsibility. To view a list of responsibilities that have already been granted, select Granted responsibilities.

6. Click **Save** to return to the Roles tab.



Responsibilities are the grant (assignment) of a role to a user, giving access to a scope. Scopes can be the organization, an environment, or a population. See Roles

Role	
Organization Admin	1 Organization

Chapter 6: Final Steps

Once you have prepared your configuration file, you are ready to complete the SSO configuration and test Single Sign On.

6.1 Complete SSO Configuration

To complete your SSO configuration, you must perform the following two steps:

1. Place the SSO configuration file (xray_samlsso.xml or apwmq_samlsso.xml) in the expected system location, which is the Tomcat config directory. For example:

    $CATALINA_HOME/conf/xray_samlsso.xml

    $CATALINA_HOME/conf/apwmq_samlsso.xml

2. Identify the SSO Configuration file in the context.xml file.
    a. In the $APIN_HOME/AutoPilotM6/apache-tomcat/conf directory, right-click context.xml and select **Edit** from the menu to open it in a text editor.
    b. Locate the lines of code labeled <!--samlsso configuration file -->. This section indicates the location of the Tomcat samlsso configuration file.
    c. Uncomment the line underneath the samlsso configuration file label. (Remove the preceding “<!--" and the following “-->” characters.) After you perform this step, the lines of code should look like the example below:

XRay

```
<!--samlsso configuration file -->

<Parameter name=”xray.samlsso.manager.config”
value=”${Catalina_home}/conf/xray_samlsso.xml”/>
```

Or if xray.samlsso.manager.config parameter not found:

```
<!--samlsso configuration file -->

<Parameter name=”samlsso.manager.config”
value=”${Catalina_home}/conf/xray_samlsso.xml”/>
```

Navigator

```
<!--samlsso configuration file -->

<Parameter name=”apwmq.samlsso.manager.config”
value=”${Catalina_home}/conf/apwmq_samlsso.xml”/>
```

6.2 Test Single Sign On

⚠ **IMPORTANT!**

After any changes to the Tomcat samlsso configuration files, you must restart Apache Tomcat before testing Single Sign On.

If you have made any changes to the samlsso configuration files, restart Apache Tomcat. Then test Single Sign On by going to the application's login page and attempting to log in using one of the user accounts you added.