Jenkins - SAML Integration

1.Background

This section aims at providing a detailed description on integrating Jenkins and Okta and configure SAML for setting up SSO for the users along with configuring user account provisioning for Jenkins.

The purpose of integrating Okta and Jenkins is to allow the users to have Single Sign-on setup(SSO) so that the users can access the Jenkins from Okta in one single login. Configuring user provisioning helps to manage all user attributes and group memberships from Okta.

2.Prerequisites

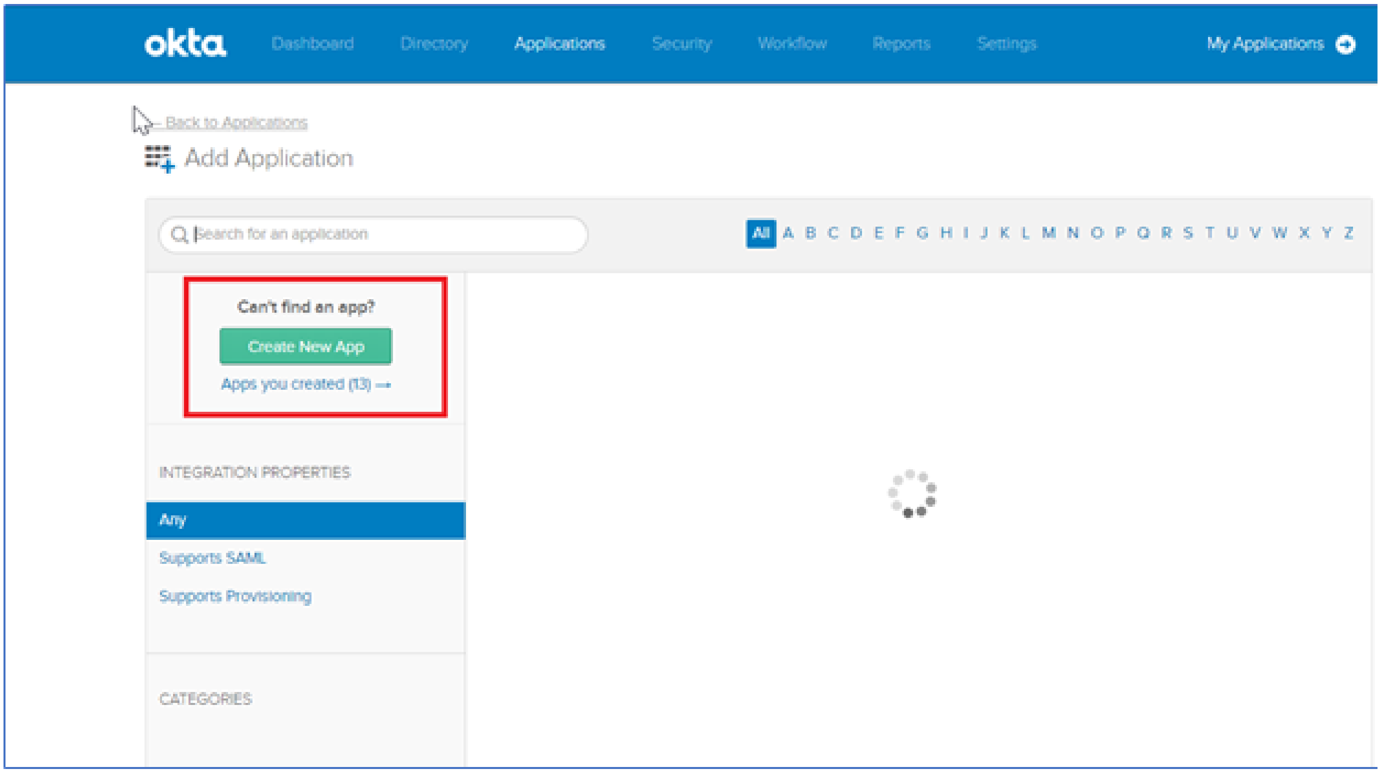
- Administrator account in Jenkins and SAML plugin needs to be installed.
- Administrator account in Okta

3. Okta Configuration Settings

Step 1: Log in to your Okta organization as a user with administrative privileges.

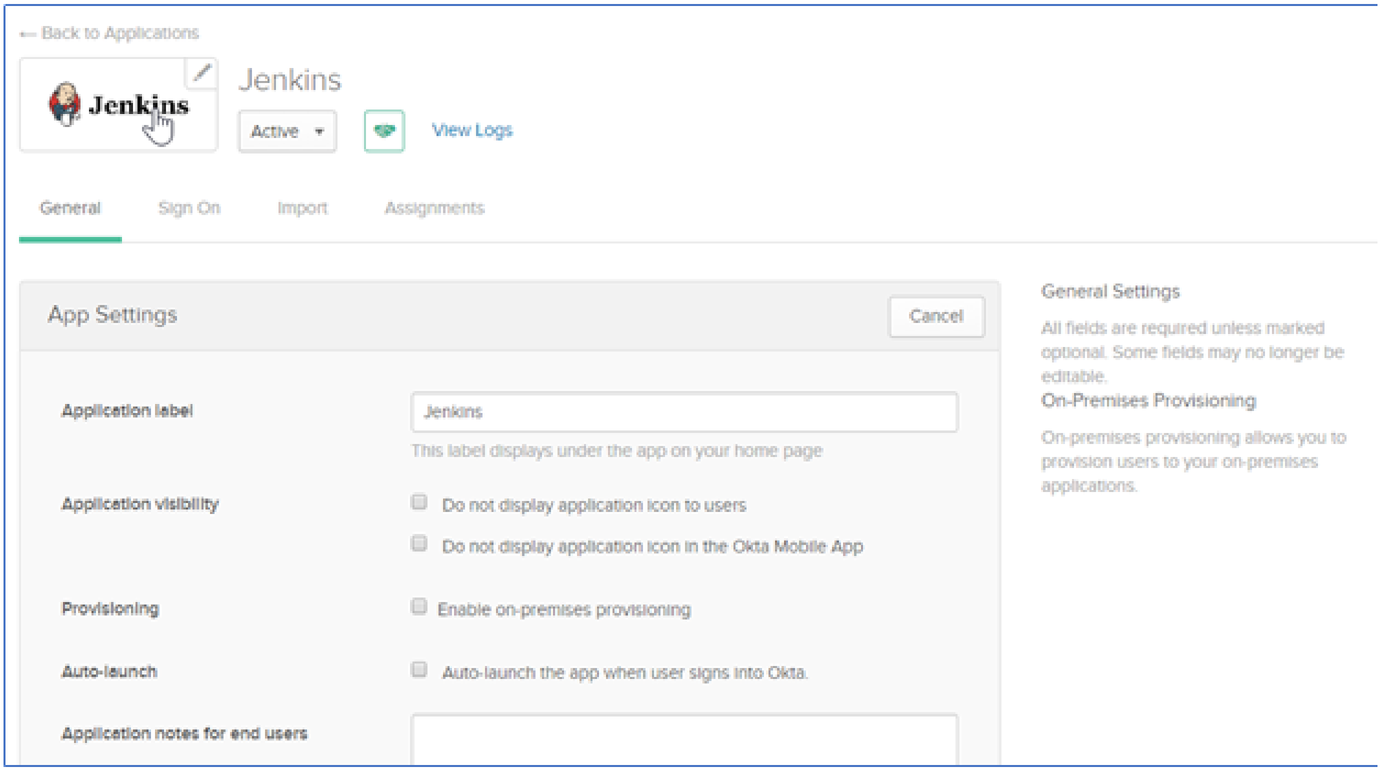
Step 2: Click on the Applications link in the upper navigation bar.

Step 3: Click on the green **Create New App** button.



Step 4: In the dialog that opens, select the "**SAML 2.0**" option, then click the green **Create** button.

Step 5: In General Settings", label the application name appropriately in the **Application label** field, then click the green Next button.



App Settings

Application label: Jenkins

This label displays under the app on your home page

Application visibility:
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile App

Provisioning: □ Enable on-premises provisioning

Auto-launch: □ Auto-launch the app when user signs into Okta.

Application notes for end users:

General Settings

All fields are required unless marked optional. Some fields may no longer be editable.

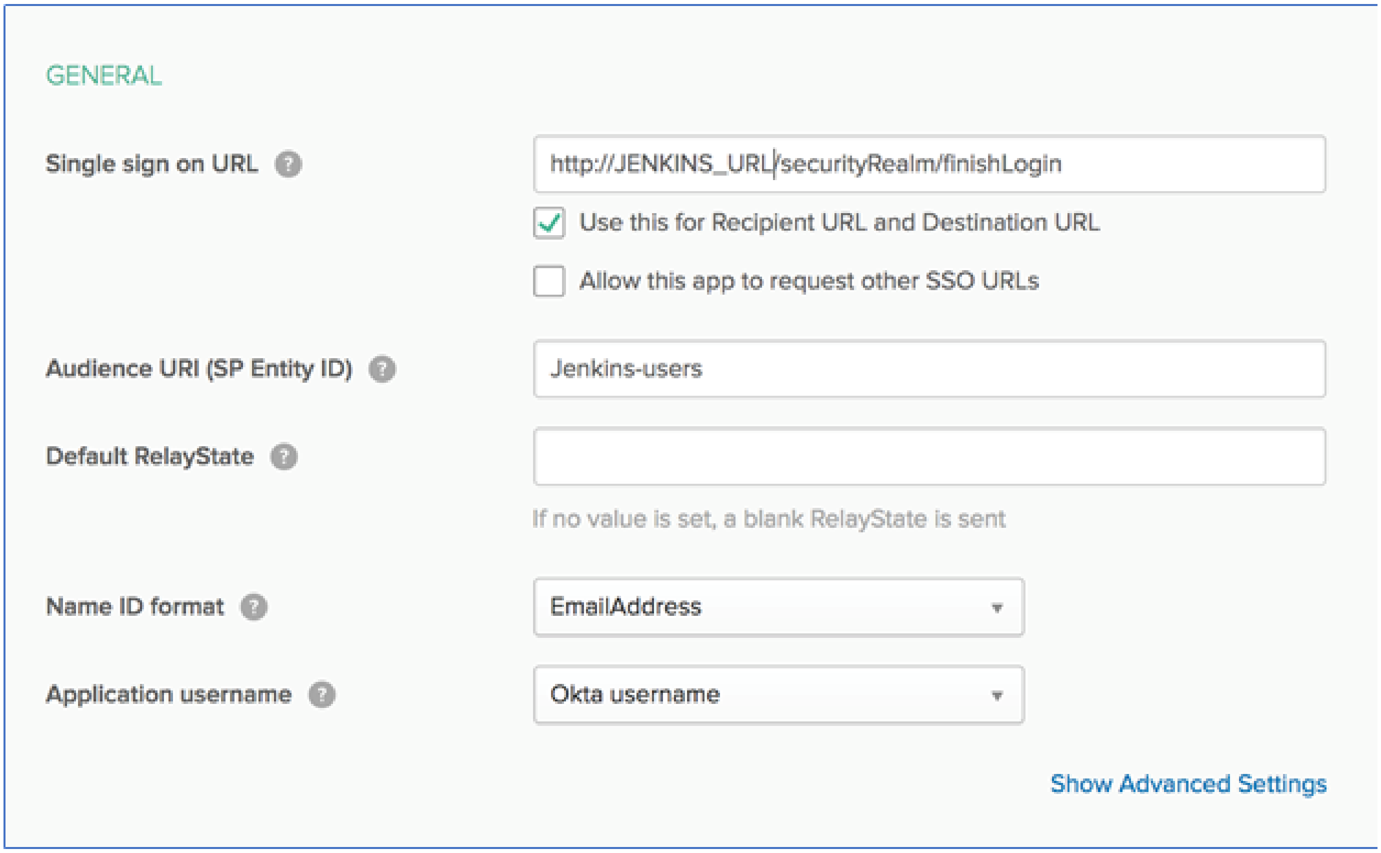
On-Premises Provisioning

On-premises provisioning allows you to provision users to your on-premises applications.

Step 6: Navigate to Sign on settings and enter "**Single sign on URL**" and "**Audience URI** (SP Entity ID)" in the below format before configuring Jenkins which will be modified later.

Example format of the Single Sign On URL: **http(s)://$Jenkins_URL/securityRealm/finishLogin**

- The **NameID format** can be set to EmailAddress, and the Application Username should be set to Okta User Name.



GENERAL

Single sign on URL: http://JENKINS_URL/securityRealm/finishLogin

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): Jenkins-users

Default RelayState:

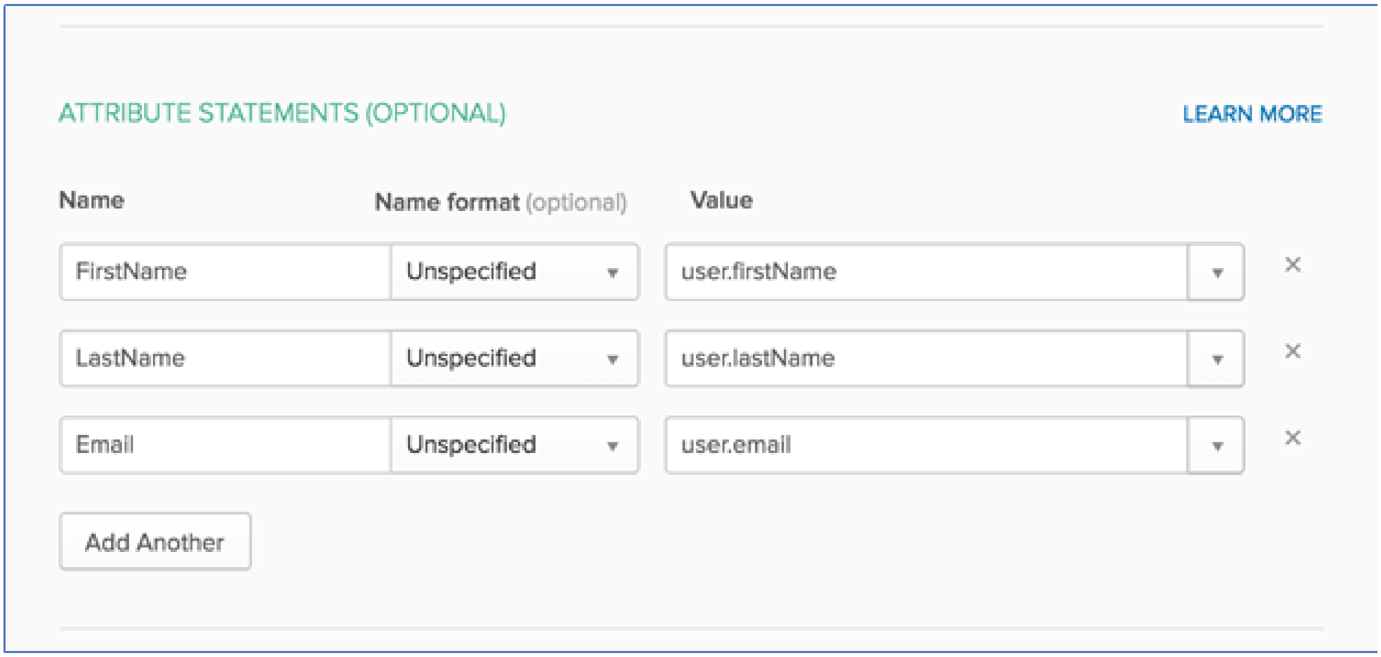
If no value is set, a blank RelayState is sent

Name ID format: EmailAddress ▾

Application username: Okta username ▾

Step 7: In the "Attribute Statements" section, add three attribute statements:

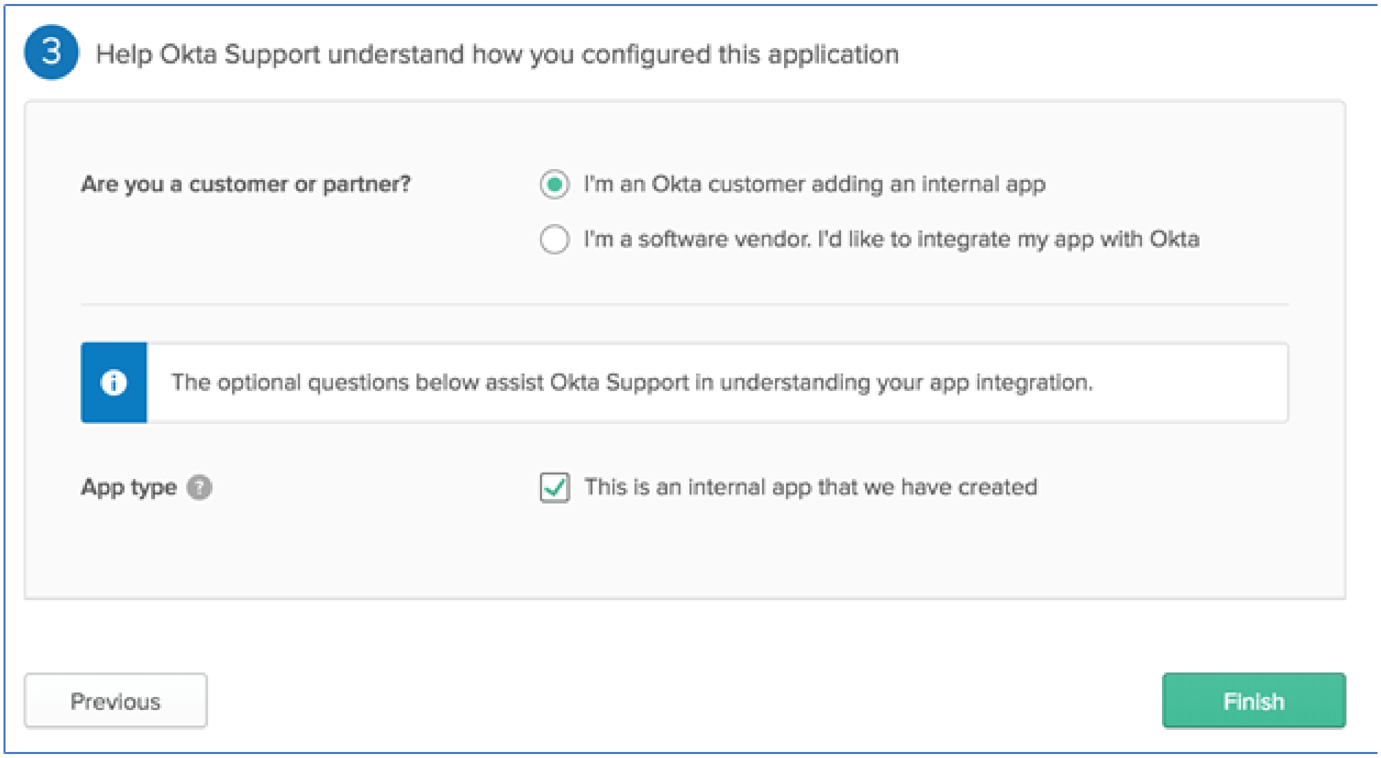
- "FirstName" set to "user.firstName"
- "LastName" set to "user.lastName"
- "Email" set to "user.email" Then click **Next** to continue.



ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Value
FirstName	Unspecified	user.firstName
LastName	Unspecified	user.lastName
Email	Unspecified	user.email

Step 8: In "**Feedback**", select "I'm an Okta customer adding an internal app", and "This is an internal app that we have created," then click **Finish** .



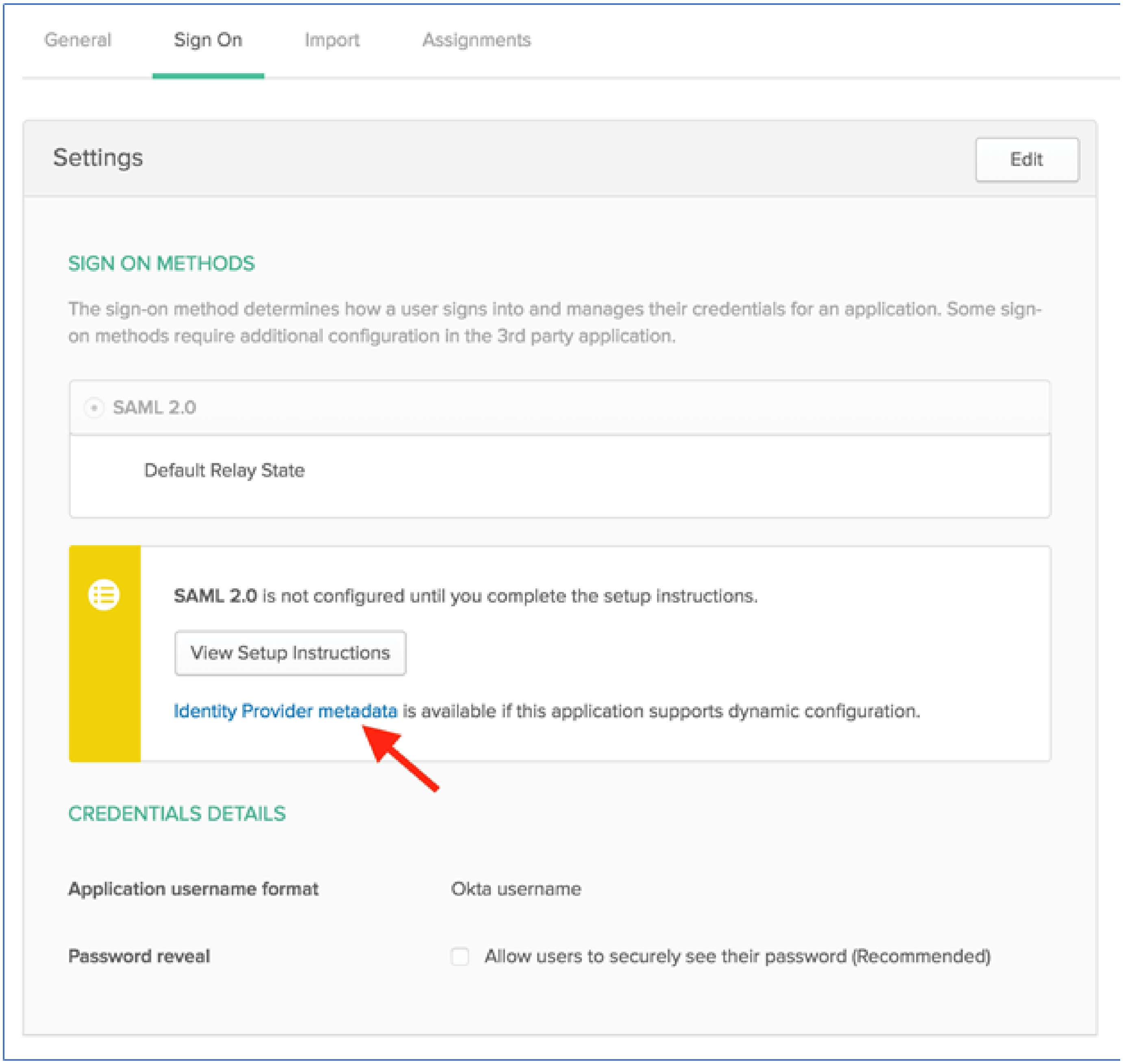
3 Help Okta Support understand how you configured this application

Are you a customer or partner?
● I'm an Okta customer adding an internal app
○ I'm a software vendor. I'd like to integrate my app with Okta

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

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

Step 9: The **Sign On** section of your newly created "SAML Application" application appears. Keep this page open it a separate tab or browser window. You will return to this page after configuration in Jenkins.



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.

● SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

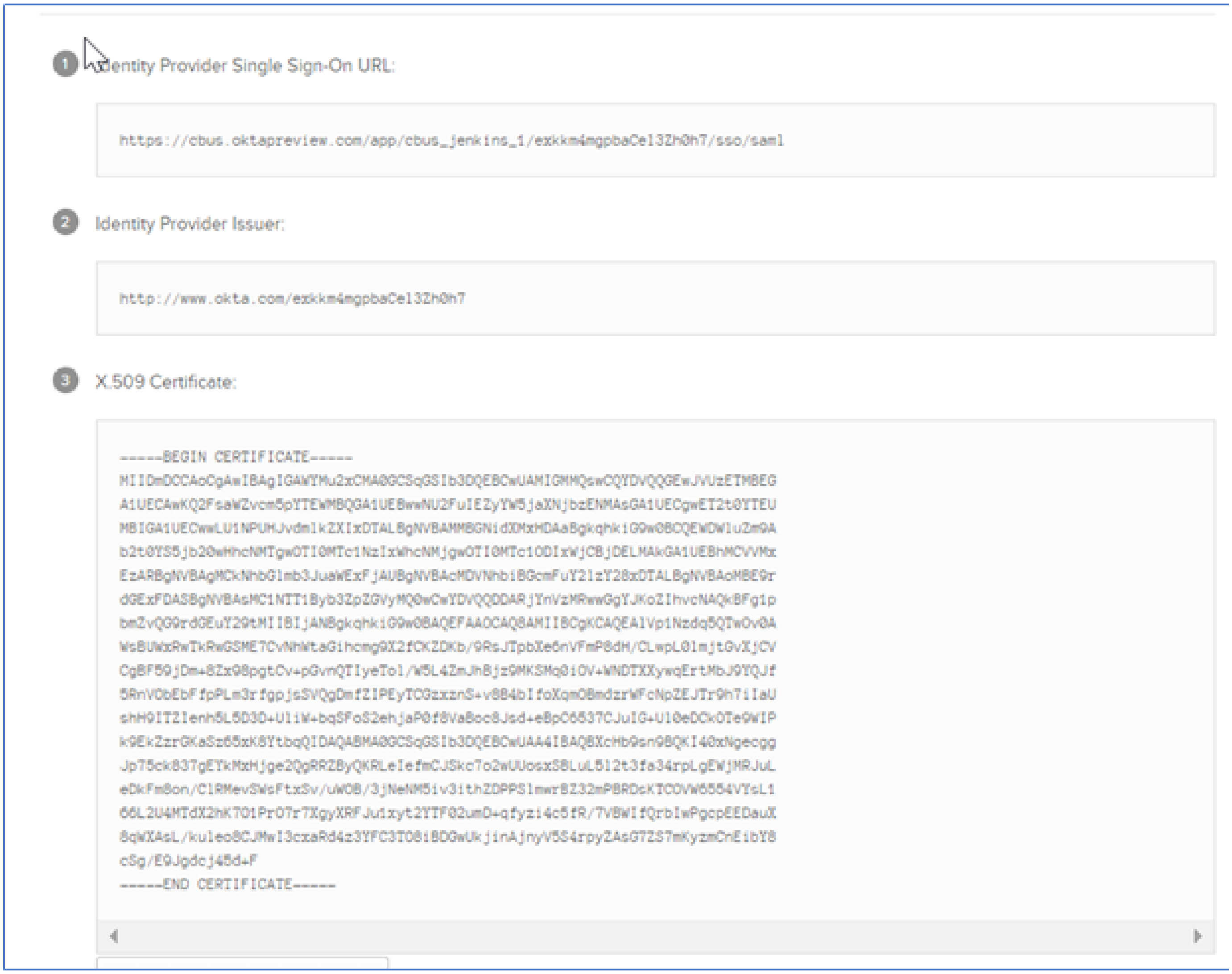
Identity Provider metadata is available if this application supports dynamic configuration.

CREDENTIALS DETAILS

Application username format	Okta username
Password reveal	□ Allow users to securely see their password (Recommended)

Step 10: Click on **View setup instructions** and copy the identity provider metadata. To copy that link, right-click on the **Identity Provider metadata** link and select Copy.

Step 11: In the instructions page, you will see these:



1 Identity Provider Single Sign-On URL:

```
https://cbus.oktapreview.com/app/cbus_jenkins_1/exkkm4mgpbaCe13Zh0h7/sso/saml
```

2 Identity Provider Issuer:

```
http://www.okta.com/exkkm4mgpbaCe13Zh0h7
```

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDmDCCAoCgAwIBAgIGAWYMu2xCMA0GCSqGSIb3DQEBCwUAMIGMMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxDTALBgNVBAMMBGNidXMxHDAaBgkqhkiG9w0BCQEWDWluZm9A
b2t0YS5jb20wHhcNMTgwOTI0MTc1NzIxWhcNMjgwOTI0MTc1ODIxWjCBjDELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTALBgNVBAoMBE9r
dGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMQ0wCwYDVQQDDARjYnVzMRwwGgYJKoZIhvcNAQkBFg1p
bm2vQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlVp1Nzdq5QTwOv0A
WsBUWxRwTkRwGSME7CvNhWtaGihcmg9X2fCKZDKb/9RsJTpbXe6nVFmP8dH/CLwpL01mjtGvXjCV
CgBF59jDm+8Zx98pgtCv+pGvnQTIyeTol/W5L4ZmJhBjz9MKSMq0iOV+WNDTXXywqErtMbJ9YQJf
5RnVObEbFfpPLm3rfgpjsSVQgDmfZIPEyTCGzxznS+v884bIfoXqmOBmdzrWFcNpZEJTr9h7iIaU
shH9ITZIenh5L5D3D+U1iW+bqSFoS2ehjaP0f8VaBoc8Jsd+eBpC6537CJuIG+U10eDCkOTe9WIP
k9EkZzrGKaSz65xK8YtbqQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBXcHb9sn9BQKI40xNgecgg
Jp75ck837gEYkMxHjge2QgRRZByQKRLeIefmCJSkc7o2wUUosxS8LuL5l2t3fa34rpLgEWjMRJuL
eDkFm8on/C1RMevSWsFtxSv/uWOB/3jNeNM5iv3ithZDPPS1mwrBZ32mPBRDsKTCOVW6554VYsL1
66L2U4MTdX2hK7O1PrO7r7XgyXRFJu1xyt2YTF02umD+qfyzi4c5fR/7VBWIfQrbIwPgcpEEDauX
8qWXAsL/kuleo8CJMwI3cxaRd4z3YFC3TO8iBDGwUkjinAjnyV5S4rpyZAsG72S7mKyzmCnEibY8
cSg/E9Jgdcj45d+F
-----END CERTIFICATE-----
```

4. Install the SAML plugin

Step 1: Login to Jenkins.

Step 2: Click on Manage Jenkins => Manage plugins

Step 3: Select the Available Tab

Step 4: Search for SAML plugin and select the check-box;

Step 5: Click on "Download now and install after restart"

Step 6: Watch the installation progress under the updateCenter view from Jenkins

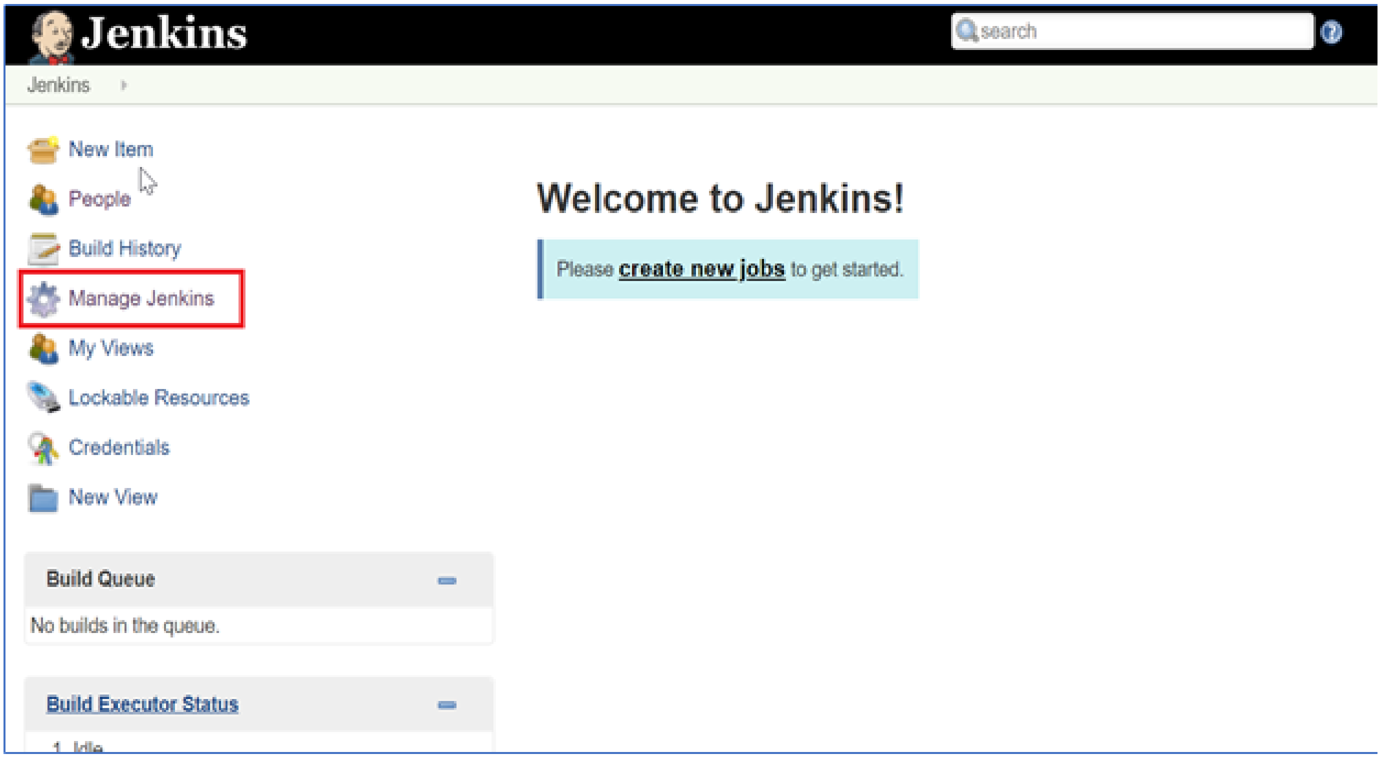
5. Jenkins Configuration Settings

- Configure plugin settings
- Hit Save

You'll also need to turn on authorization for the SAML settings to take effect. As long as the anonymous user can take all actions, Jenkins won't try to log the user in.

Step 1: Login to Jenkins using administrator account.

Step 2: Click on **Manage Jenkins**.

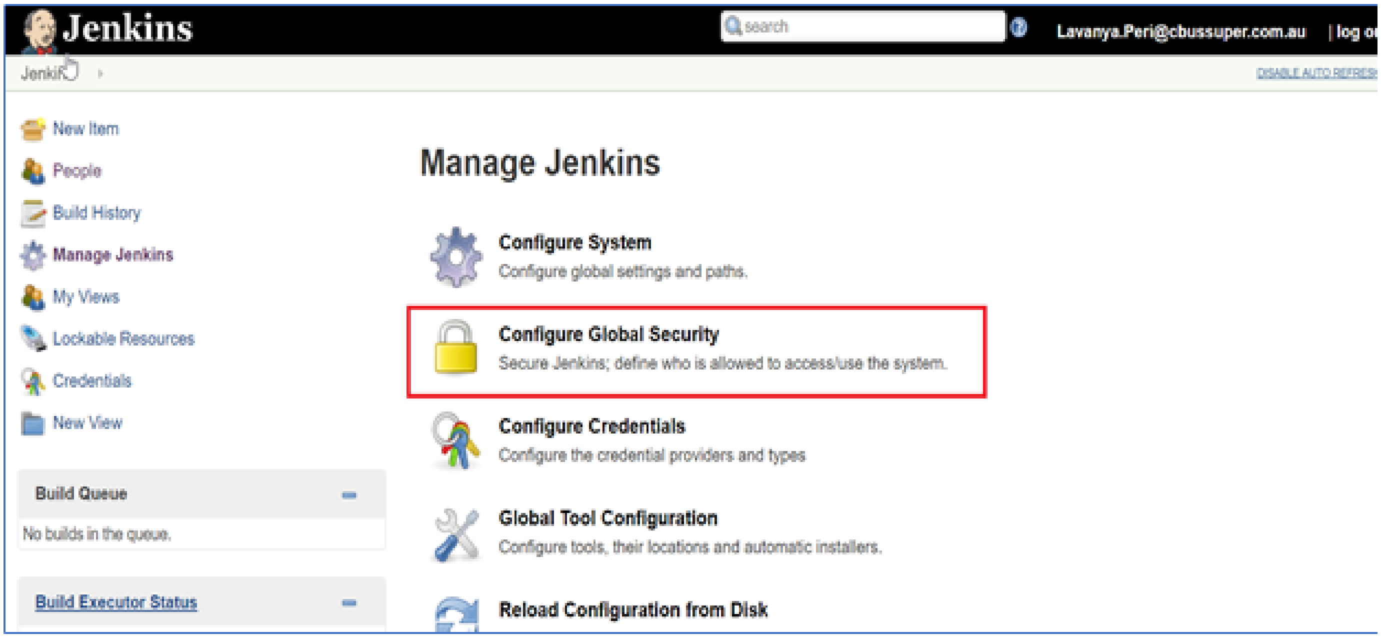


Welcome to Jenkins!

Please **create new jobs** to get started.

No builds in the queue.

Step 3: Go to **Configure Global Security**.



Manage Jenkins

Configure System
Configure global settings and paths.

Configure Global Security
Secure Jenkins; define who is allowed to access/use the system.

Configure Credentials
Configure the credential providers and types

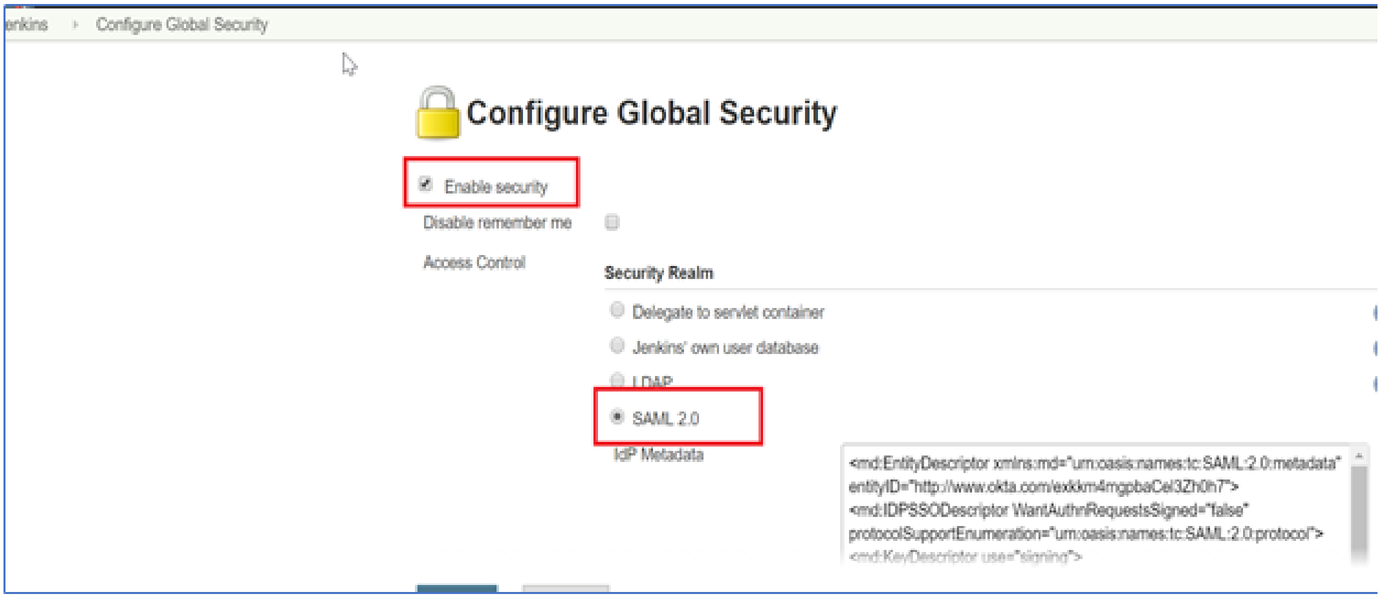
Global Tool Configuration
Configure tools, their locations and automatic installers.

Reload Configuration from Disk

No builds in the queue.

Step 4: Check **Enable security**.

Step 5: Select **SAML 2.0.**



enkins › Configure Global Security

Configure Global Security

☑ Enable security

Disable remember me ☐

Access Control

Security Realm

○ Delegate to servlet container

○ Jenkins' own user database

○ LDAP

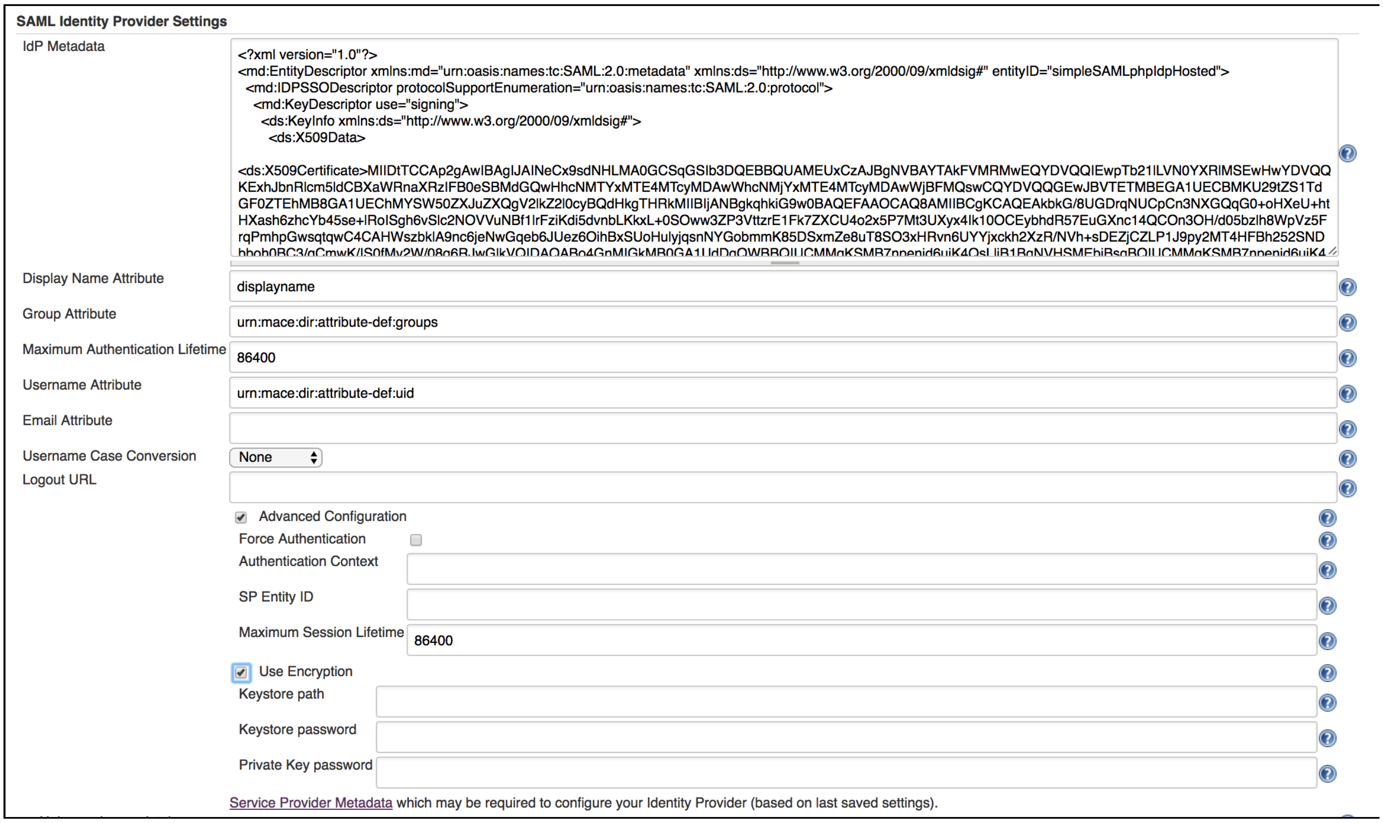
● SAML 2.0

IdP Metadata

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exkkm4mgpbaCel3Zh0h7">
<md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
```

Step 6: Configure plugin settings and hit save.

You'll also need to turn on authorization for the SAML settings to take effect. As long as the anonymous user can take all actions, Jenkins won't try to log the user in.



SAML Identity Provider Settings

IdP Metadata

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="simpleSAMLphpIdpHosted">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>

<ds:X509Certificate>MIIDtTCCAp2gAwIBAgIJAINeCx9sdNHLMA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNVBAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMSEwHwYDVQQ
KExhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwHhcNMTYxMTE4MTcyMDAwWhcNMjYxMTE4MTcyMDAwWjBFMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1Td
GF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkbkG/8UGDrqNUCpCn3NXGQqG0+oHXeU+ht
HXash6zhcYb45se+lRoISgh6vSlc2NOVVuNBf1lrFziKdi5dvnbLKkxL+0SOww3ZP3VttzrE1Fk7ZXCU4o2x5P7Mt3UXyx4Ik10OCEybhdR57EuGXnc14QCOn3OH/d05bzlh8WpVz5F
rqPmhpGwsqtqwC4CAHWszbklA9nc6jeNwGqeb6JUez6OihBxSUoHulyjqsnNYGobmmK85DSxmZe8uT8SO3xHRvn6UYYjxckh2XzR/NVh+sDEZjCZLP1J9py2MT4HFBh252SND
bhoh0BC3/qCmwK/lS0fMv2W/08q6BJwGlkVQIDAQABo4GnMIGkMB0GA1UdDgQWBBQIUCMMqKSMB7npenid6uiK4QsLjiB1BgNVHSMEbjBsgBQIUCMMqKSMB7npenid6uiK4
```

Display Name Attribute: displayname

Group Attribute: urn:mace:dir:attribute-def:groups

Maximum Authentication Lifetime: 86400

Username Attribute: urn:mace:dir:attribute-def:uid

Email Attribute:

Username Case Conversion: None

Logout URL:

☑ Advanced Configuration

Force Authentication ☐

Authentication Context:

SP Entity ID:

Maximum Session Lifetime: 86400

☑ Use Encryption

Keystore path:

Keystore password:

Private Key password:

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

Configuring plugin settings

- **Metadata**
  - **IdP Metadata** - Identity Provider Metadata in XML format. Usually, identity providers that support SAML expose metadata in XML form by public URL. This metadata should be downloaded and copy-pasted to this field (not need if you have set the IdP Metadata URL).
  - **IdP Metadata URL** - The Identity Provider metadata file source URL (not need if you have set the IdP Metadata).

- **Refresh Period** - The period of minutes we will wait until refresh the IdP Metadata. Set it to 0 to not update the metadata.

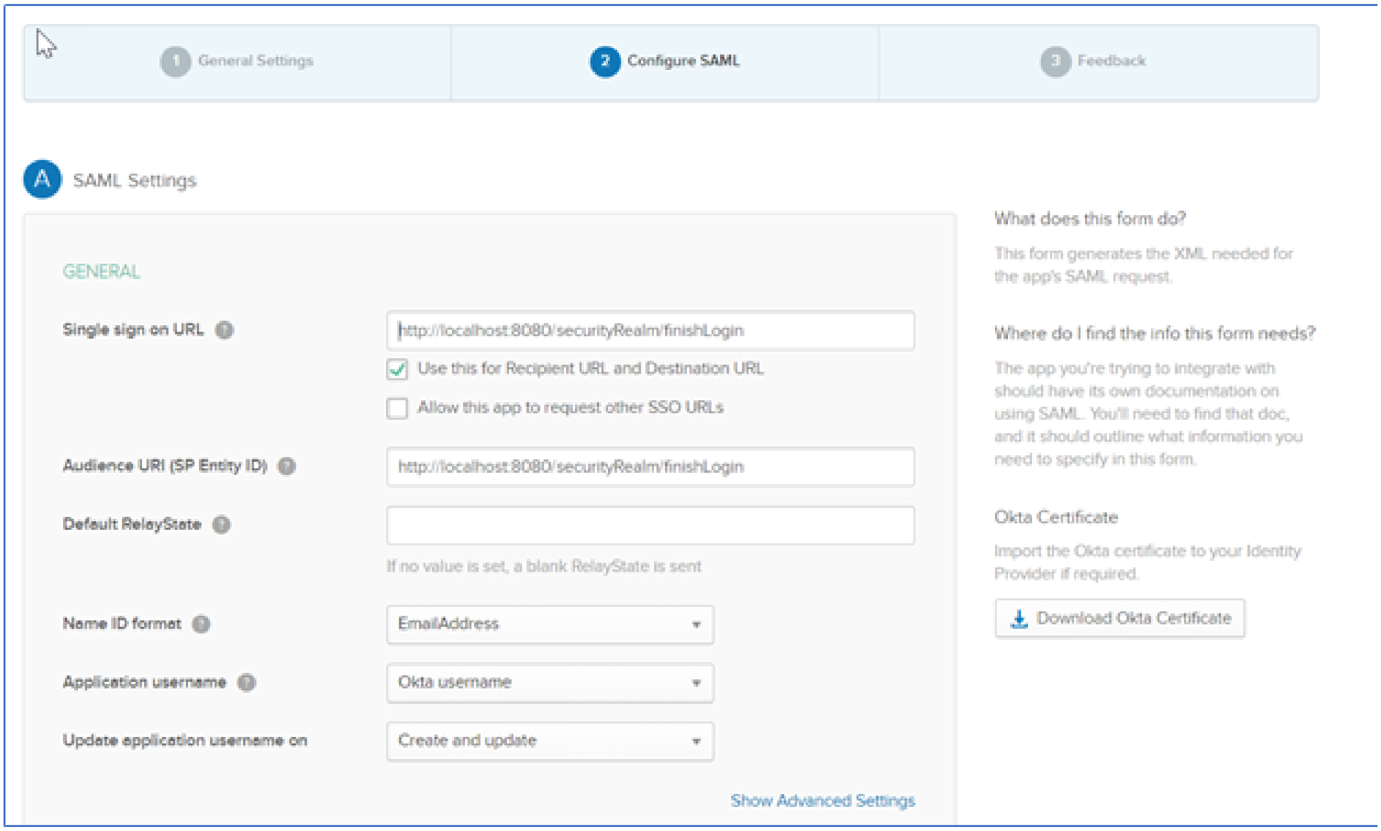
- **Display Name Attribute** - Name of the attribute that carries the display name (optional). If not specified, the username is used.
- **Group Attribute** - Name of the attribute that carries user groups (optional)**. This attribute must have separate AttributeValue elements per role (so for example, they can't be concatenated to a single string). In Okta's case, set this value to "Group" - this is case sensitive.**
- **Maximum Authentication Lifetime** - Number of seconds since the user was authenticated in IdP while his authentication is considering as active. If you often get "No valid subject assertion found in response" or "Authentication issue instant is too old or in the future" then most probably you need to increase this value. Set this setting to value greater than the session lifetime on IdP Default is 24h * 60 min * 60 sec = 86400
- **Username Attribute** - Name of the attribute that carries user name which will be used as the Jenkins ID (optional). If not specified, the SAML profile ID will be used.
- **Email Attribute** - Fill name of email attribute in SAML response.
- **Username Case Conversion** - The ID returned from SAML is used as the username for Authorization, which is usually case sensitive. To make it easier to match with user definition in the policy, the returned value can be converted. **Caution!** Be aware of case in Authorization strategy as you may lose access rights if they do not match
    - None - will not change return value (default)
    - Lowercase - convert to lowercase
    - Uppercase - convert to uppercase
- **Data Binding Method** - SAML Plugin supports two method of redirection binding HTTP-Redirect and HTTP-POST, by default HTTP-Redirect is used. Check supported binding redirection types of your IdP.
    - urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
    - urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
- **Logout URL** - The url of your Identity Provider where you want to be redirected once logout.
- **Advanced Configuration** - You could enable this options to use SAML ForceAuthn to force logins at our IdP, AuthnContextClassRef to override the default authentication mechanism, and force multi-factor authentication; you also could set the sessions on Jenkins to be shorter than those on your IdP.
    - **Force Authentication** - Whether to request the SAML IdP to force (re)authentication of the user, rather than allowing an existing session with the IdP to be reused. Off by default
    - **Authentication Context** - If this field is not empty, request that the SAML IdP uses a specific authentication context, rather than its default. Check with the IdP administrators to find out which authentication contexts are available
    - **SP Entity ID** - If this field is not empty, it overrides the default Entity ID for this Service Provider. Service Provider Entity IDs are usually a URL, like ***http://jenkins.example.org/securityRealm/finishLogin***.
- **Encryption** - If your provider requires encryption, you can specify the keystore details here that should be used.
    - **Keystore path** - The path to the keystore file created with the keygen command.
    - **Key Alias** - The alias used in the -alias argument of the keytool< command.
    - **Keystore password** - The password used in the -storepass argument of the keytool command.
    - **Private Key password** - The password used in the -keypass argument of keytool.
    - **Disable Signature Redirect Binding Auth Request** - Disable signature of the Redirect Binding Auth Request (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect), It is not possible to disable the signature in HTTP-POST binding.

The attribute is sometimes called a claim, and for some IdPs it has a fixed structure, e.g. a URI. So in some documentation, you might see the term URI of the claim instead of the name of the attribute.

5. Configuring Identity Provider (IdP)

On the IdP side, you need to specify the location in Jenkins which accepts the HTTP POST with the authentication data (SAML response). This is [URL of Jenkins]/securityRealm/finishLogin. This Jenkins URL it is obtained from "Jenkins URL" field on Configure System, if you use a load balancer or reverse proxy or another kind of redirection in the middle check that the real URL it is configured on Configure System, if not the SAML Response will be not valid. So for example ***https://jenkins.example.com/securityRealm/finishLogin***.

You also need to specify the **entity ID** (sometimes called **Audience**), by default, this is the same URL, on advanced settings you can configure it.



A SAML Settings

GENERAL

Single sign on URL: http://localhost:8080/securityRealm/finishLogin

☑ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): http://localhost:8080/securityRealm/finishLogin

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: EmailAddress

Application username: Okta username

Update application username on: Create and update

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.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

6. Configuring groups security

If your IdP provides the group(s) a user belongs to via an attribute of the SAML response, you can use this to configure role-based security with the Role Strategy Plugin.

- Go to "Configure Global Security"
- Check "Role-Based Strategy" in Authorization section
- Hit Save
- Go to "Manage and Assign Roles" => "Manage Roles". Here you define roles, which have permissions.
- Configure "Project roles" section with roles that match your needs. These roles can be named anything you like.
- Hit Save
- Go to "Manage and Assign Roles" => "Assign Roles". Here you attach the SAML-provided groups to the roles you defined in the previous step.
- In "User/group to add" you enter the name of the SAML group you want to attach to a role. (Group names are case sensitive)
- Once a group is added, you can attach it to one or more roles.
- Hit save.

7. Backup files considerations

If you do not configure encryption settings The plugin creates a key pair automatically and stores them in "JENKINS_HOME/saml-jenkins-keystore.jks", then store the data related into "JENKINS_HOME/saml-jenkins-keystore.xml", you can grab the public key from "JENKINS_HOME/saml-sp-metadata.xml".

If you configured the encryption settings, you only have to copy the key store and the config files (you should maintain the secrets also). The default key store is "JENKINS_HOME/saml-jenkins-keystore.jks" the configuration is in "JENKINS_HOME/saml-jenkins-keystore.xml" some data is encrypted, so it is not for manual manage, and it only is valid for a Jenkins with the same JENKINS_HOME/secrets.

You need the following files to restore the SAML configuration

JENKINS_HOME/config.xml JENKINS_HOME/saml-jenkins-keystore.jks JENKINS_HOME/saml-jenkins-keystore.xml JENKINS_HOME/saml-ipd-metadata.xml JENKINS_HOME/saml-sp-metadata.xml Also you need the same secret.key, if not the configuration is impossible to unencrypt but in any case, you use to make a backup of your full JENKINS_HOME to make your Jenkins instance work properly (not only SAML Plugin), I recommend you to take a look at this CloudBees KB.