Graphite 8 SSO Setup Guide

Overview

Summary

Graphite integrates with single sign-on (SSO) providers to offer a common authentication scheme for users in an organization. Integration is achieved using the SAML 2.0 specification, and this document provides a step-by-step guide to setting up SSO with Okta, OneLogin, and Azure Active Directory.

Pre-Requisites

This document assumes that your Graphite 8 instance is set up and configured to use the standard Graphite authentication method, with at least one active administrator account. Otherwise, prior to setting up SSO, please refer to the *Graphite 8 Deployment Guide* to set up your Graphite 8 instance.

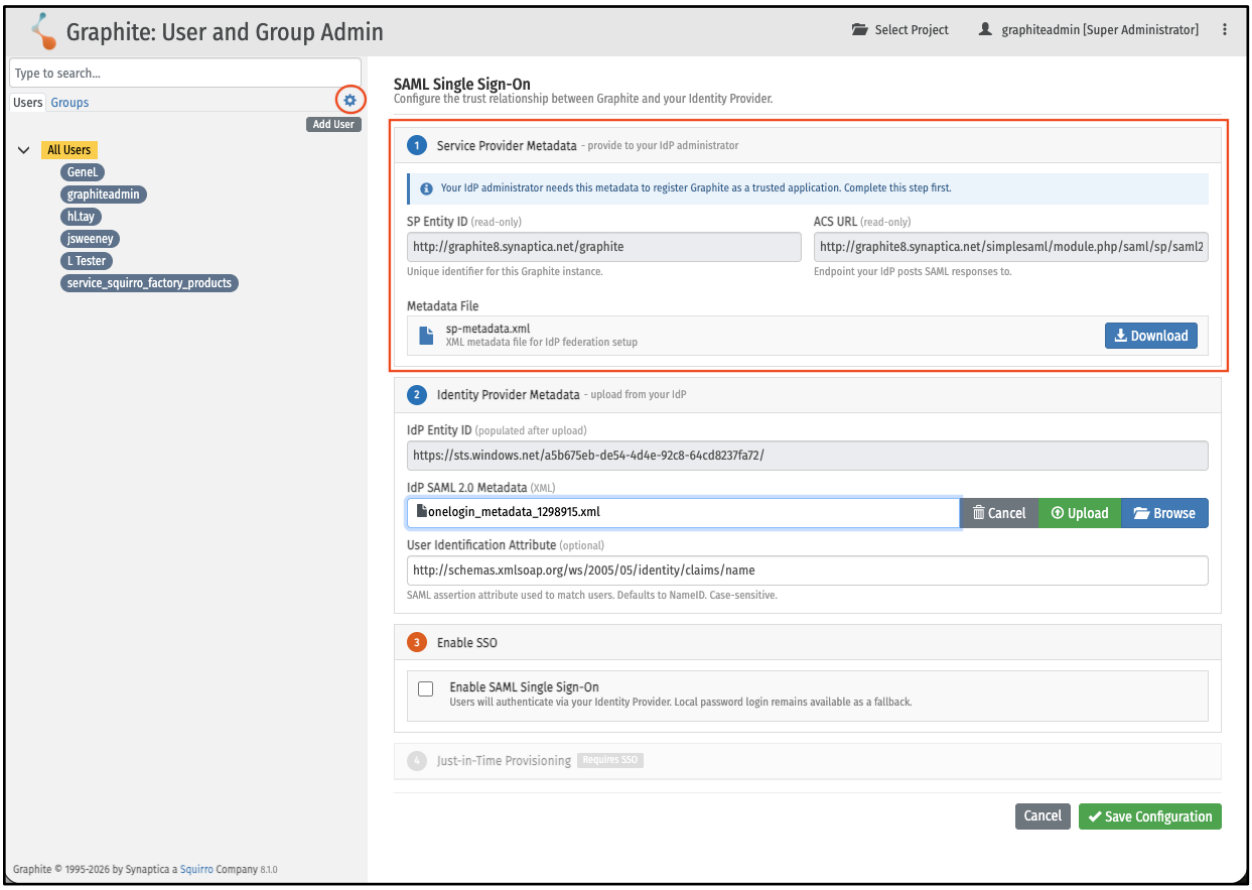
Modifying the Apache Web Server Configuration

In order to support SSO, the following lines should be added to the Apache configuration file (generally, located in `/etc/httpd/conf/httpd.conf`). Replace demo.synaptica.net with the fully qualified domain name of your Graphite 8 instance, and adjust the directory path according to your configuration.

Alias `/simplesaml /var/www/html/demo.synaptica.net/simplesamlphp/www`

Configuring SSO in User Admin

When preparing to add Graphite as a service provider application in your SSO provider, please launch *User and Group Admin* in Graphite. Click on the *gear* icon on the top left to display the information you need to supply to your SSO provider. Leave the window open so you can conveniently copy and paste the service provider information into your SSO provider configuration screen, or click on the *Download* button to download the metadata file and upload it to the SSO provider.

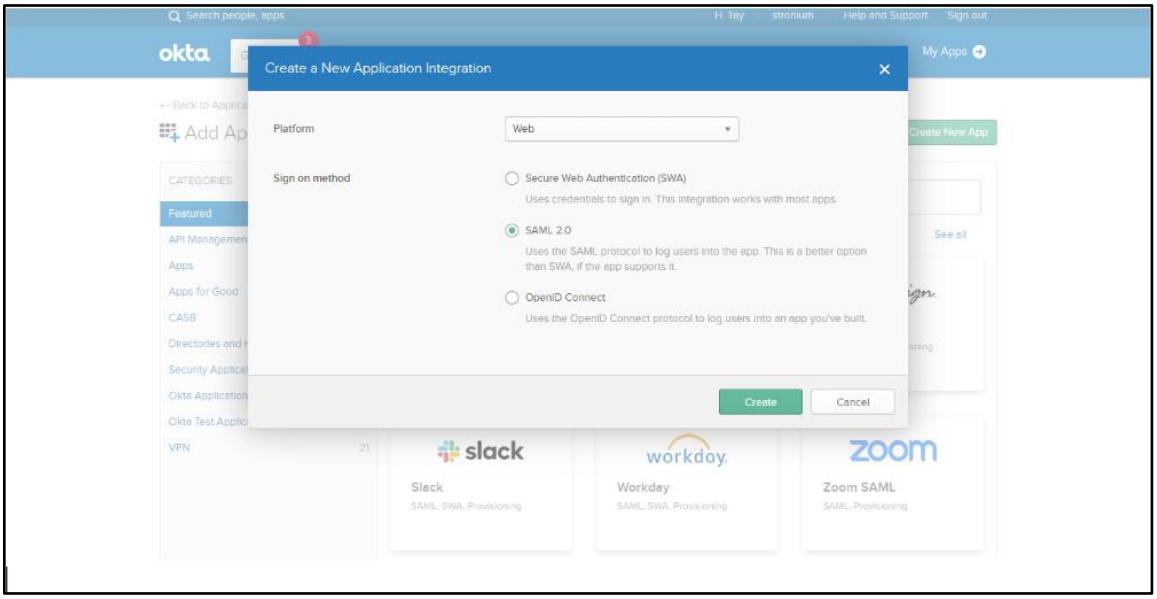


The next sections provide step-by-step guidance on setting up Graphite as a service provider in each respective SSO provider. You may refer to the section relevant to your SSO provider, and skip to the section, *Completing the Setup of SSO in Graphite*.

Setting Up Graphite in Okta

Create New App in Okta

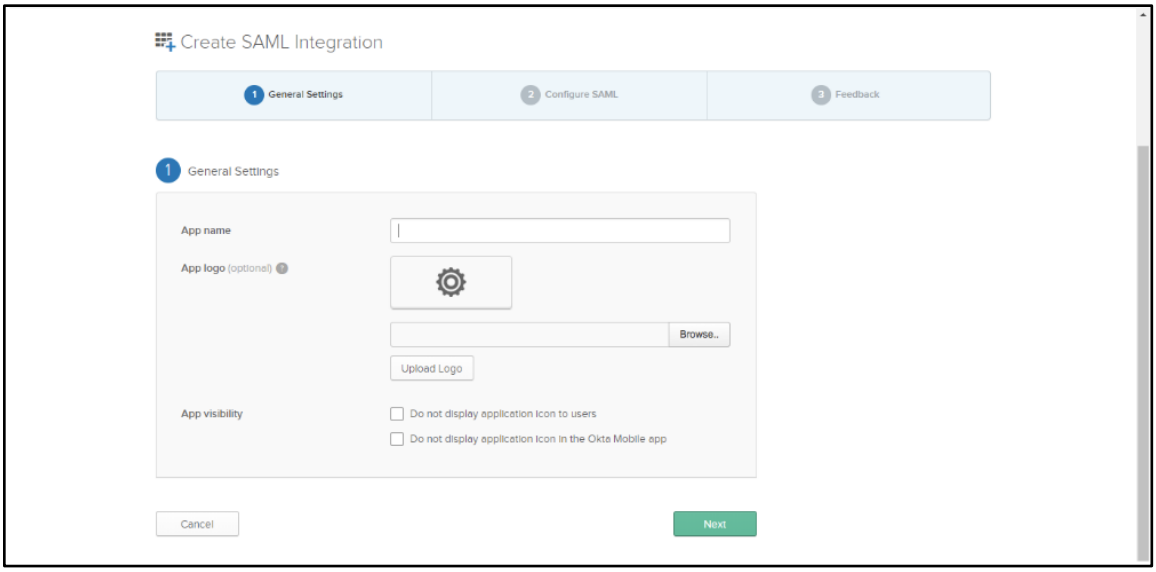
1. Verify that you are using the Admin Console. If you are using the Developer Console, you need to switch over to the Admin Console. If you see Developer Console in the top left corner of your console, click it, then click Classic UI to switch.
2. In the Admin Console, go to Applications > Applications.
3. Click Add Application.
4. Click Create New App.
5. To create a SAML integration, select Web as the Platform and SAML 2.0 as the *Sign-on method*.
6. Click Create.



Step 1 – General Settings

1. App name — Specify a name identifier for your integration.
   Note: The name can only consist of UTF-8, 3-byte characters.
2. App logo (optional) — Add a logo to accompany your integration in the Okta org.
3. App visibility — Choose whether to hide your integration from your end-users' homepage, and to hide your integration from the Okta Mobile apps store on your

end-users' devices.



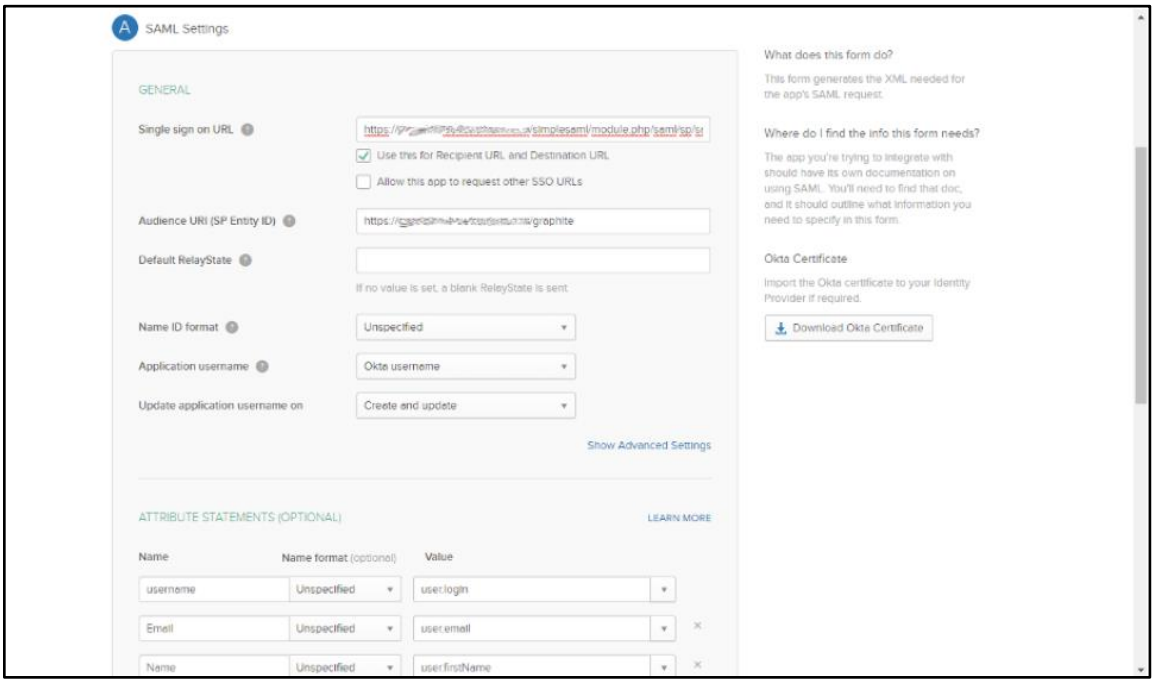
Step 2 – Configure SAML

A SAML 2.0 configuration requires a combination of information from both your org and the target app, Graphite.

1. Single sign-on URL — The location where the SAML assertion is sent with a POST operation. This URL is required and serves as the default ACS URL value for the Service Provider (SP). This URL is always used for IdP-initiated sign-on requests. You can copy and paste the value located in the *Graphite SAML 2.0 Service Provider Information* pop-up dialog as described in the previous section of this document, e.g. https://demo.synaptica.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
2. Use this for Recipient URL and Destination URL — Select this check box for Graphite.
3. Allow this app to request other SSO URLs — Leave this unchecked for Graphite.
4. Audience URI (SP Entity ID) — The intended audience of the SAML assertion. This is usually the Entity ID of your application, and in the case of Graphite, you should copy the value under *Audience Restriction* in the *Graphite SAML 2.0 Service Provider Information* pop-up, e.g. https://demo.synaptica.net/graphite
5. Default RelayState — Not required for Graphite.
6. Name ID format — You may use the default (Unspecified) setting for Graphite.
7. Application username — This field denotes the username in Okta that matches exactly the username in Graphite. You may use the following settings:

a. Okta username (default)
b. If email is used as the username in Graphite, you can specify the email attribute as the authentication ID in Okta:
    i. Name > Email (*Name format* set to *unspecified*), and select user.email as Value
    Important: For security reasons, do not use fields that can be edited by users.

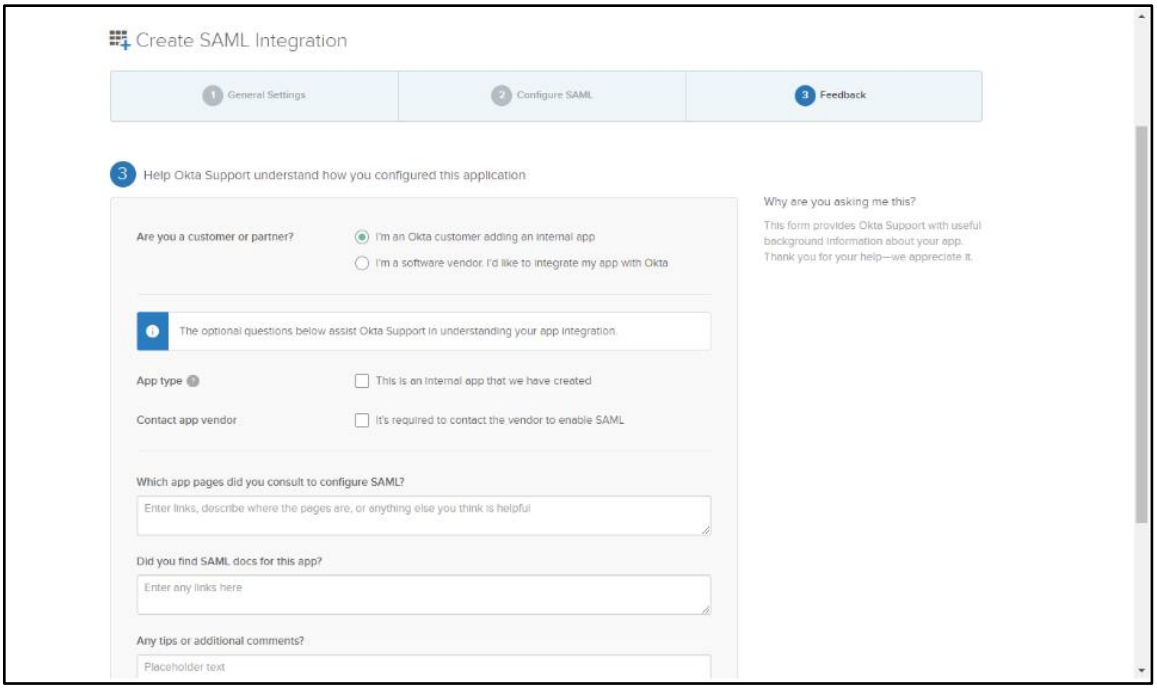
8. Show Advanced Settings – leave these as default for Graphite.
9. Attribute Statements (Optional) — Not required for Graphite.
10. Group Attribute Statements (Optional) — Not required for Graphite.
11. Click *Preview the SAML Assertion* to view the XML generated from the Configure SAML section of the SAML App Wizard.
12. Click Next to continue.



Step 3 – Feedback

If you are an Okta customer adding an integration that is intended for internal use only:

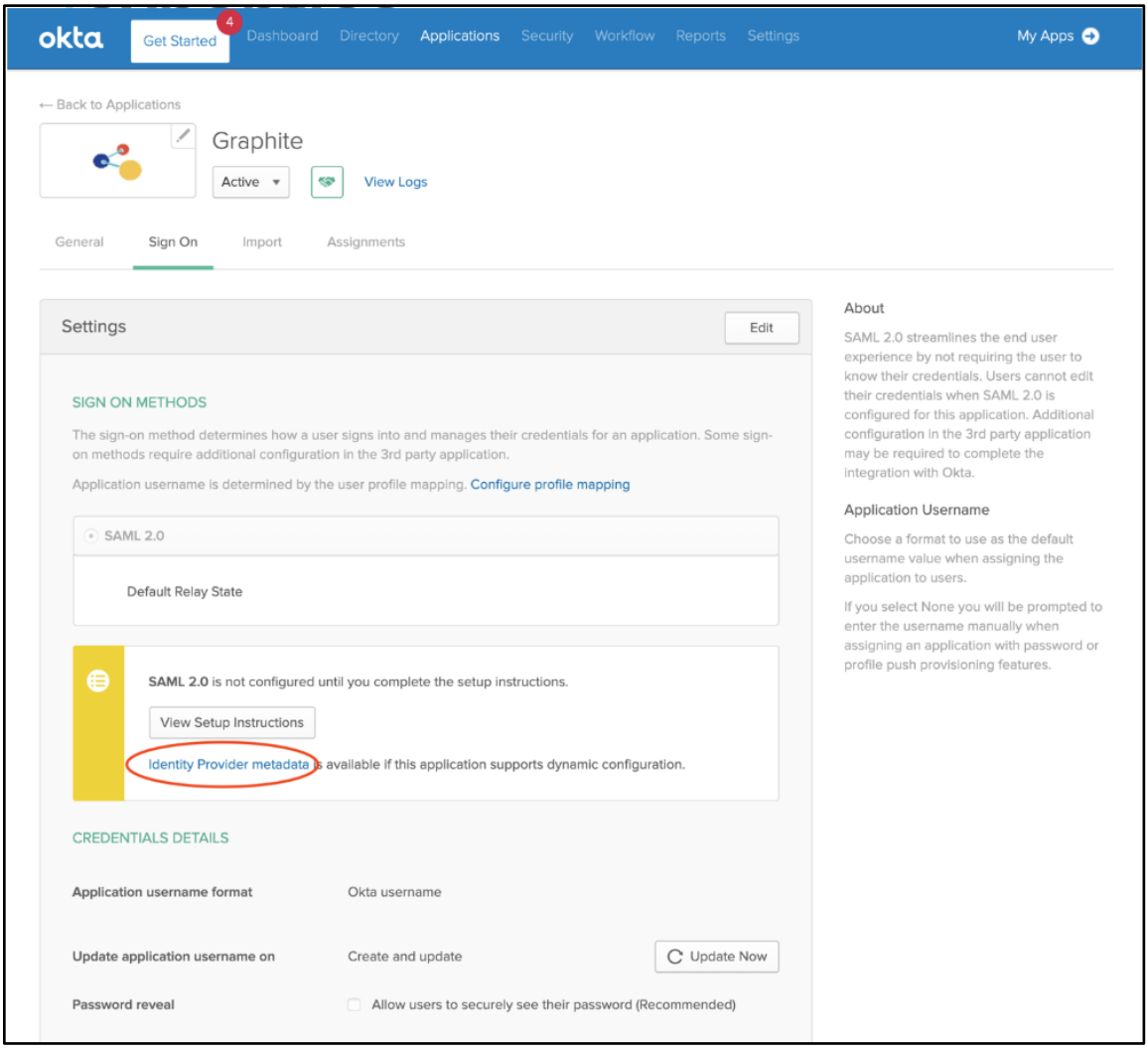
1. Select *I'm an Okta customer adding an internal app*.
2. Click Finish. Your integration is created in your Okta org.
3. The Settings page for your integration appears, where you can modify any of the parameters and assign your integration to users.



Retrieve Metadata

1. In the Admin Console, click Applications.
2. Select the Graphite app you configured.
3. Click the Sign On tab, and locate the *Identity Provider metadata* link.

4. Click the link, and save the resulting XML file to upload to Graphite later.

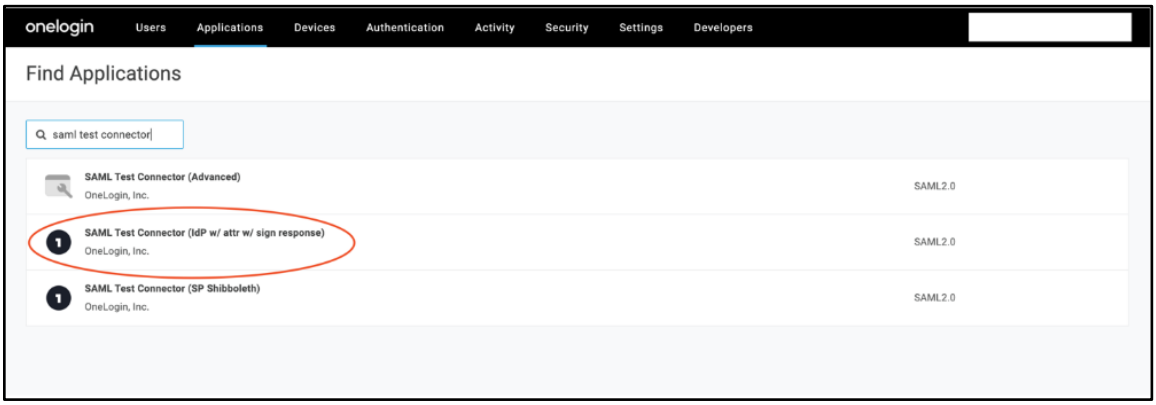


Assign Users

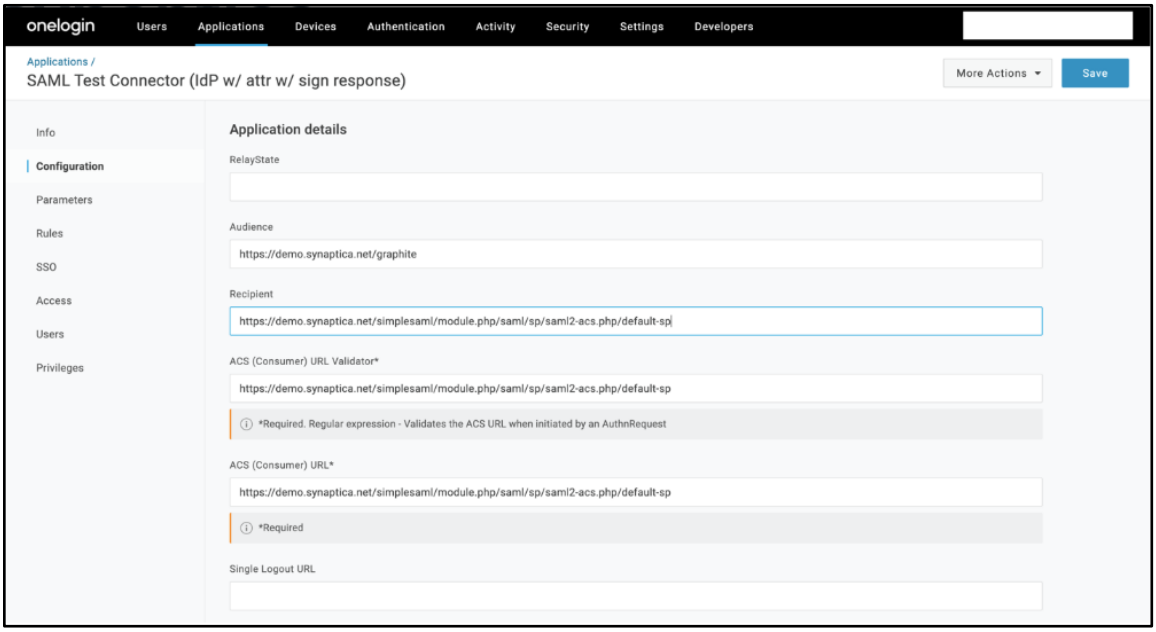
1. Click on the Assignments tab to assign users to the newly added Graphite app Okta.
2. Key in the corresponding Graphite username for each user assigned to the Graphite app in Okta. Alternatively, you can create Graphite user accounts with users' email addresses if you wish to use the default Okta username configuration.

Setting Up Graphite in OneLogin

1. Log in as the administrator in OneLogin, and click Administration.
2. Click Applications in the top menu bar, and then, Applications.
3. Click the Add App button on the top right.
4. In this example, we can use a suitable template to configure the Graphite app. In the search field key in *SAML Test Connector*, and select *SAML Test Connector (IdP w/ attr w/ sign response)*.



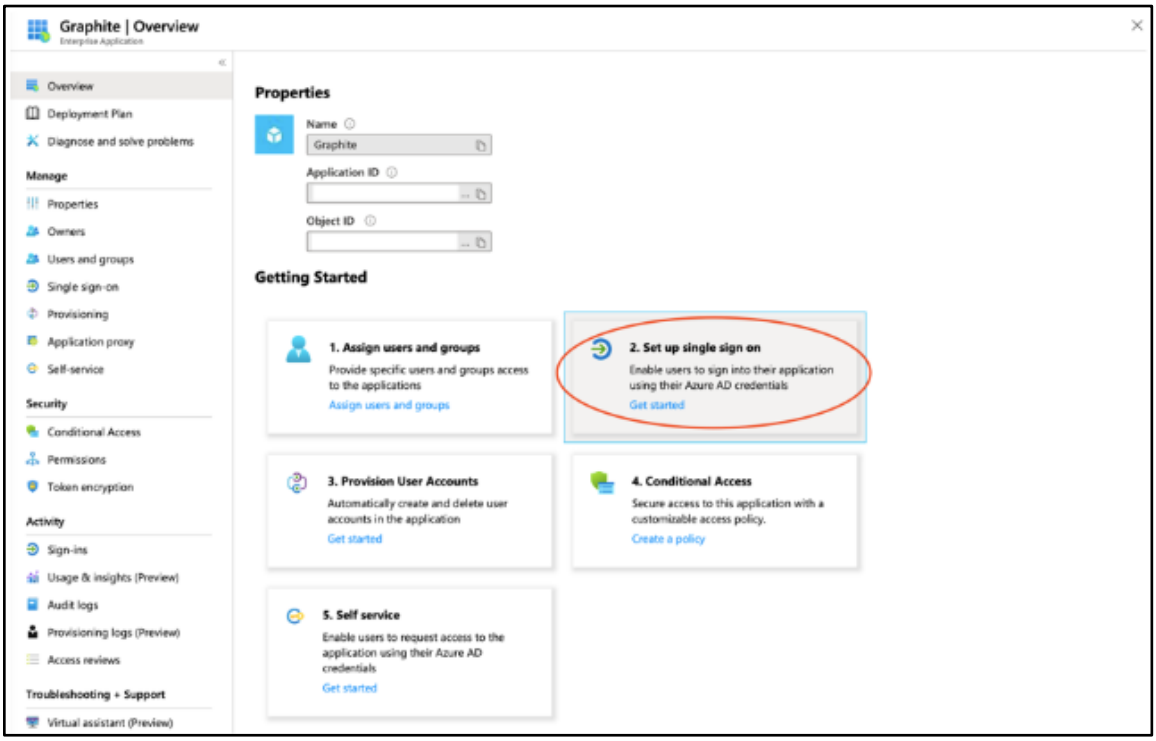
5. Click Configuration on the left column, and enter the corresponding details based on the information provided in pop-up panel in the Graphite User Admin. Please refer to the screenshot below. Click Save when done.

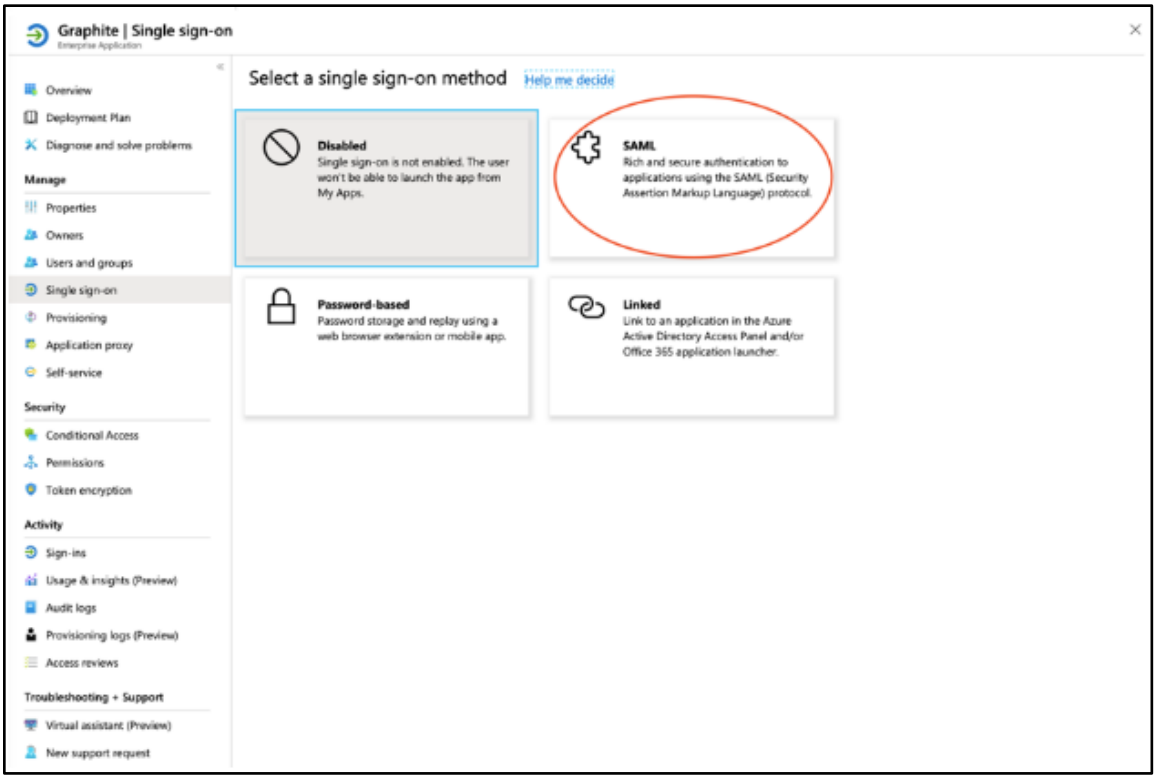


6. Download the metadata XML file by clicking *More Actions* on the top right, followed by *SAML Metadata*. This XML file will be uploaded in Graphite later.
7. Click on Users in the left navigation column to add users to the Graphite app created in OneLogin.

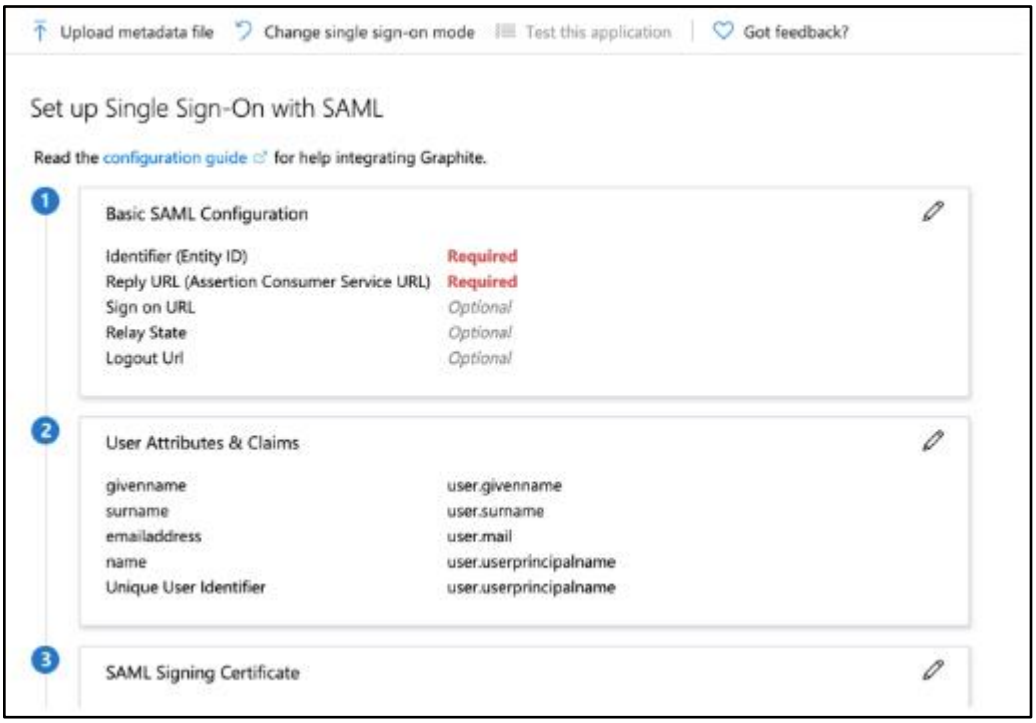
Setting Up Graphite in Azure Active Directory

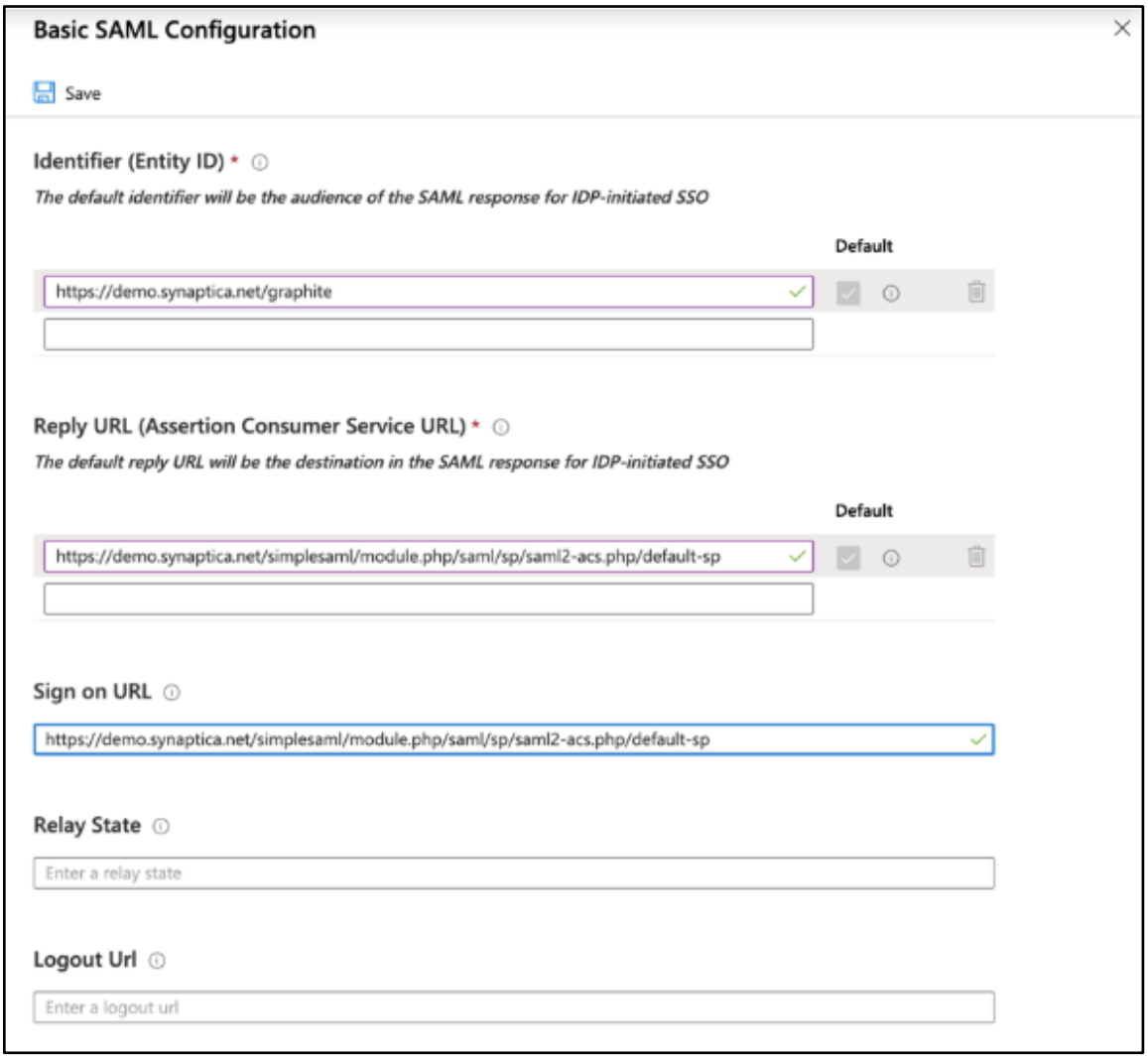
1. In the Azure Active Directory admin center, click *Enterprise applications*.
2. Click *New application* to add Graphite as a new application.
3. Click *Non-gallery application*, and enter a descriptive label for Graphite under the Name field, then click the Add button below.
4. Click *2. Set up single sign on*, followed by *SAML*, as the single sign-on method.





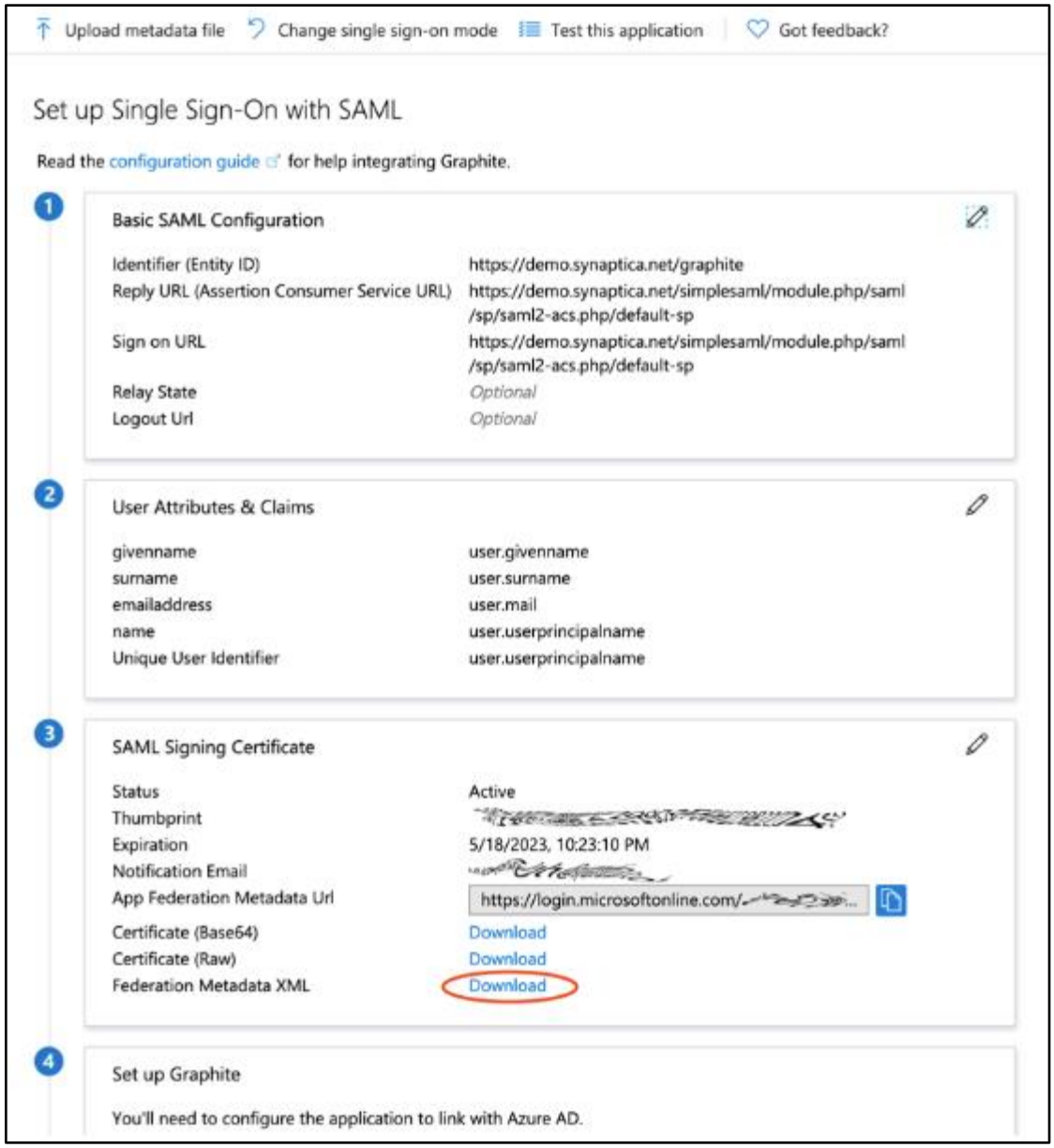
5. Click the pencil icon under *Basic SAML Configuration*, and fill out the details as shown in the example screenshot, substituting with values from the pop-up in the i icon in Graphite User Admin. Click the Save button when done.


Upload metadata file
Change single sign-on mode
Test this application
Got feedback?
Set up Single Sign-On with SAML
Read the configuration guide for help integrating Graphite.
1
Basic SAML Configuration
Identifier (Entity ID) Required
Reply URL (Assertion Consumer Service URL) Required
Sign on URL Optional
Relay State Optional
Logout Url Optional
2
User Attributes & Claims
givenname user.givenname
surname user.surname
emailaddress user.mail
name user.userprincipalname
Unique User Identifier user.userprincipalname
3
SAML Signing Certificate



6. Return to the previous screen, and click Download beside *Federation Metadata XML*, under *SAML Signing Certificate*. The resulting XML file will be uploaded in

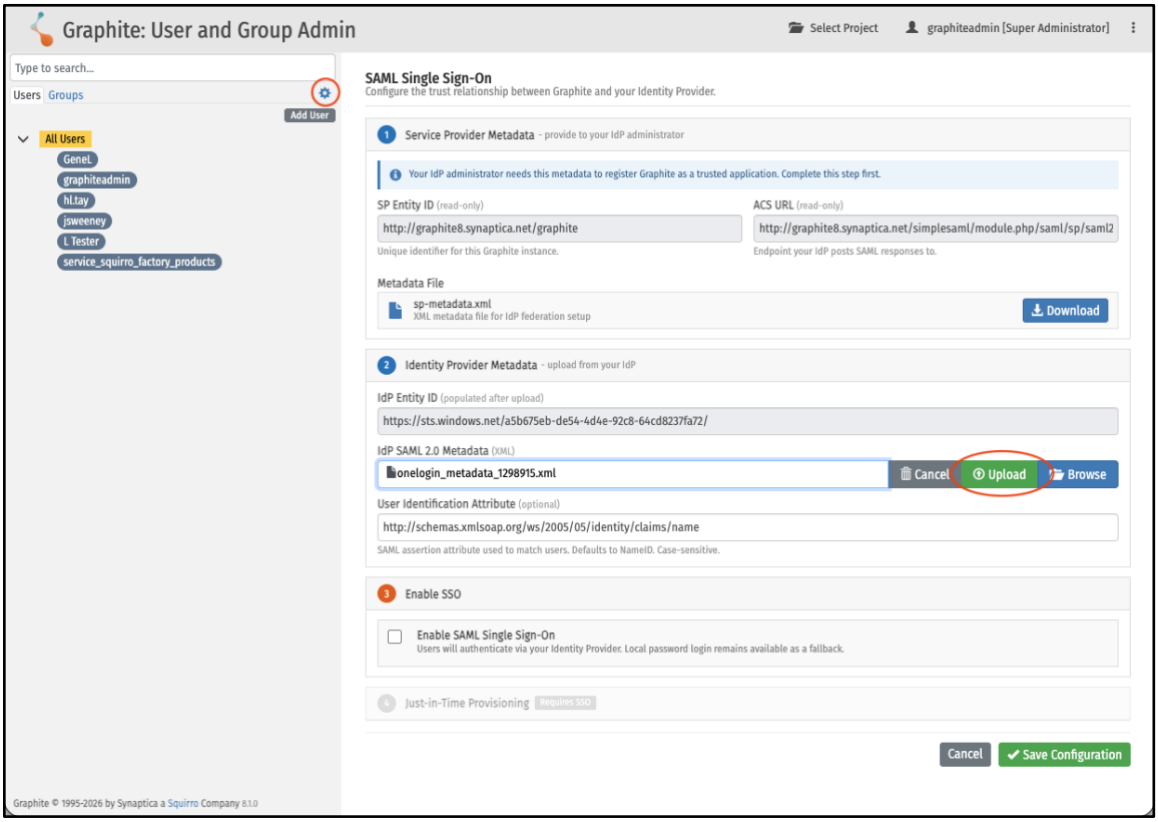
Graphite later to complete the SSO setup.



7. Return to the overview page, and select *1. Assign users and groups* to assign users to the Graphite app created in Active Directory.

Completing the Setup of SSO in Graphite

1. To set up SSO in Graphite, please log in as an administrator.
2. Go to User and Group Admin.
3. Firstly, ensure that you have a Graphite user account with a username that corresponds to your SSO credentials. This Graphite user should be an administrator, so you can continue to access Graphite after SSO is enabled.
4. Click the *gear* icon to launch the SAML Single Sign-On page as shown in the screenshot.



5. Under *Identity Provider SAML 2.0 Metadata (XML),* upload the XML file from your SSO provider.
6. Click the Submit button to apply the settings in the XML file in Graphite.
7. For Okta and OneLogin, leave the User Identification Attribute field empty to use the default NameID mapping as the username. If you are using Azure Active Directory, enter the following to use the attribute containing the Active Directory username (typically, the user's email address) in Graphite: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
8. Check Enable SAML Single Sign-On to activate SSO on the next login. Click Save Configuration to commit the changes.

9. At this stage, you may test SSO by launching another browser, or opening an Incognito browser window on your current browser, and keying in your Graphite instance URL in the address bar. Click *Sign in* on the top right to be redirected to your SSO provider login page.

Bypassing SSO

The systems administrator may allow bypassing SSO for troubleshooting. To allow bypassing of SSO, edit the file */{graphite_directory}/graphite/graphite.ini*, and set the *bypass-sso* option to *true*:

```
  ######################
# SSO configuration #
######################

[sso]
; Whether to bypass SSO and use basic authentication
; Optional
; Default = false
bypass_sso = true
```

You can then access the login screen on your Graphite instance using the nosso=1 parameter, e.g.

```
https://demo.synaptica.net/graphite/login?nosso=1
```

Caution: The SSO bypass option should only be used for troubleshooting. Enabling it negates the security benefits offered by the SSO provider for authentication since it allows local password-based authentication for all active user accounts in Graphite.

Appendix

Graphite SSO Flow