Graphite SSO Setup Guide

Software Version 6.15
Document Version 20240314

Table of Contents

Table of Contents

1 Overview **2**

1.1 Summary 2

1.2 Pre-Requisites 2

1.3 Modifying the Apache Web Server Configuration 2

1.4 Configuring SSO in User Admin 2

2 Setting Up Graphite in Okta **3**

2.1.1 Create New App in Okta 3

2.1.2 Step 1 – General Settings 3

2.1.3 Step 2 – Configure SAML 4

2.1.4 Step 3 – Feedback 5

2.2 Retrieve Metadata 6

2.3 Assign Users 7

3 Setting Up Graphite in OneLogin **8**

4 Setting Up Graphite in Azure Active Directory **10**

5 Completing the Setup of SSO in Graphite **13**

6 Bypassing SSO **13**

7 Appendix **15**

7.1 Graphite SSO Flow 15

synaptica
a squirro company

Graphite SSO Setup Guide

Software Version 6.15
Document Version 20240314

1 Overview

1.1 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.

1.2 Pre-Requisites

This document assumes that your Graphite 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 Installation and Administration Guide* to set up your Graphite instance.

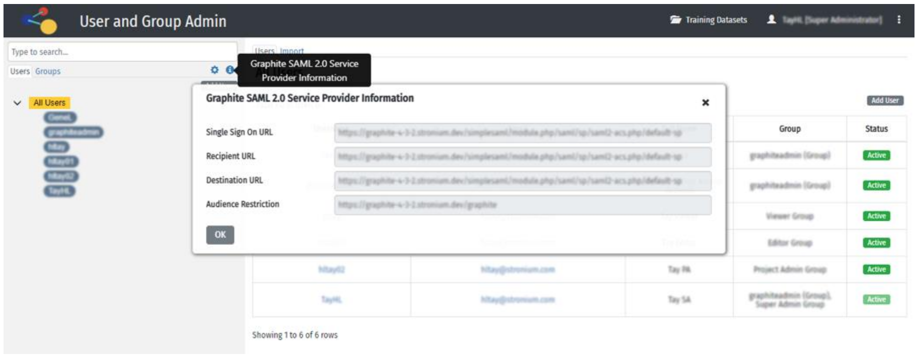
1.3 Modifying the Apache Web Server Configuration

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 instance, and adjust the directory path according to your configuration.

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

1.4 Configuring SSO in User Admin

When preparing to add Graphite as a service provider application in your SSO provider, please launch *User Admin* in Graphite. Click on the *i* 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.



Graphite SAML 2.0 Service Provider Information

Single Sign On URL: https://graphite-4-3-2.stronium.dev/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
Recipient URL: https://graphite-4-3-2.stronium.dev/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
Destination URL: https://graphite-4-3-2.stronium.dev/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
Audience Restriction: https://graphite-4-3-2.stronium.dev/graphite

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*.

2 Setting Up Graphite in Okta

2.1.1 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.

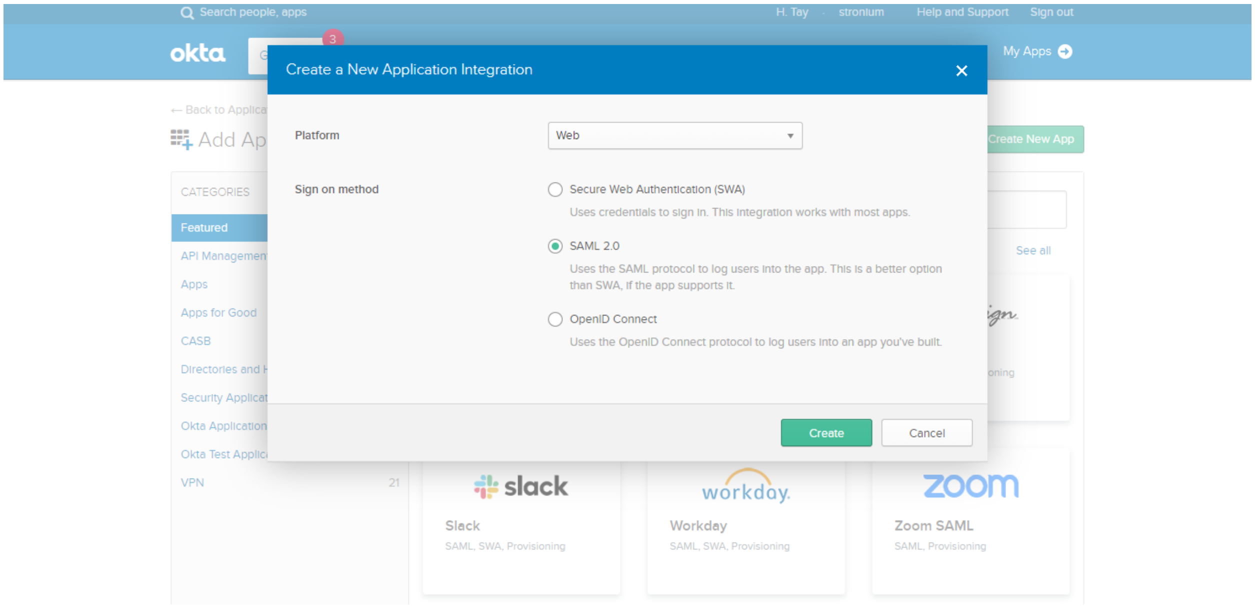
2. In the Admin Console, go to Applications > Applications.

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.



Create a New Application Integration

Platform: Web

Sign on method

○ Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.

● SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

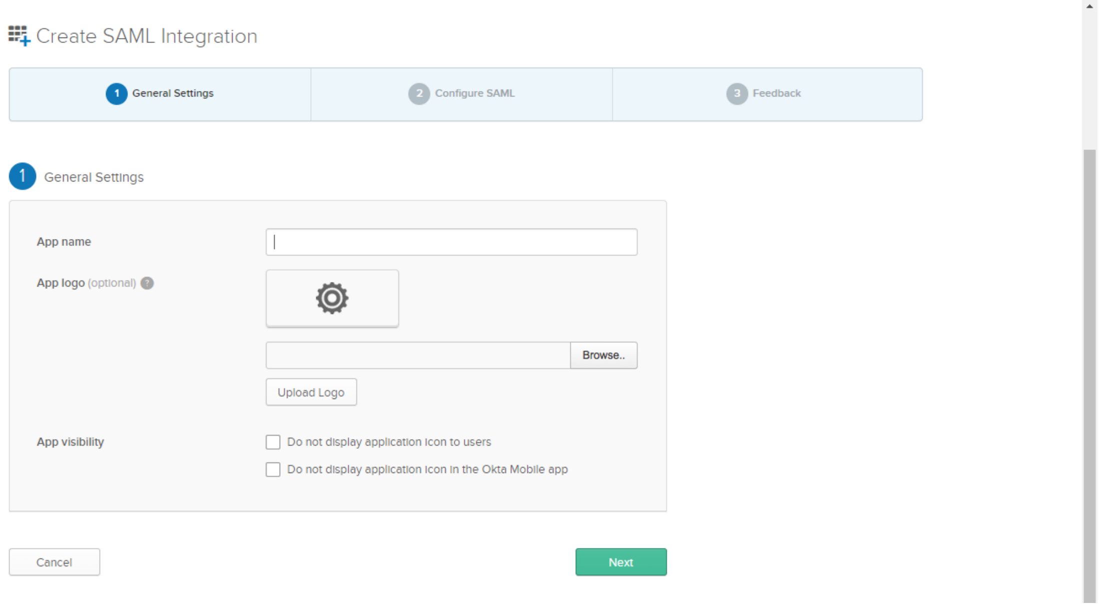
○ OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

2.1.2 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.



2.1.3 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:

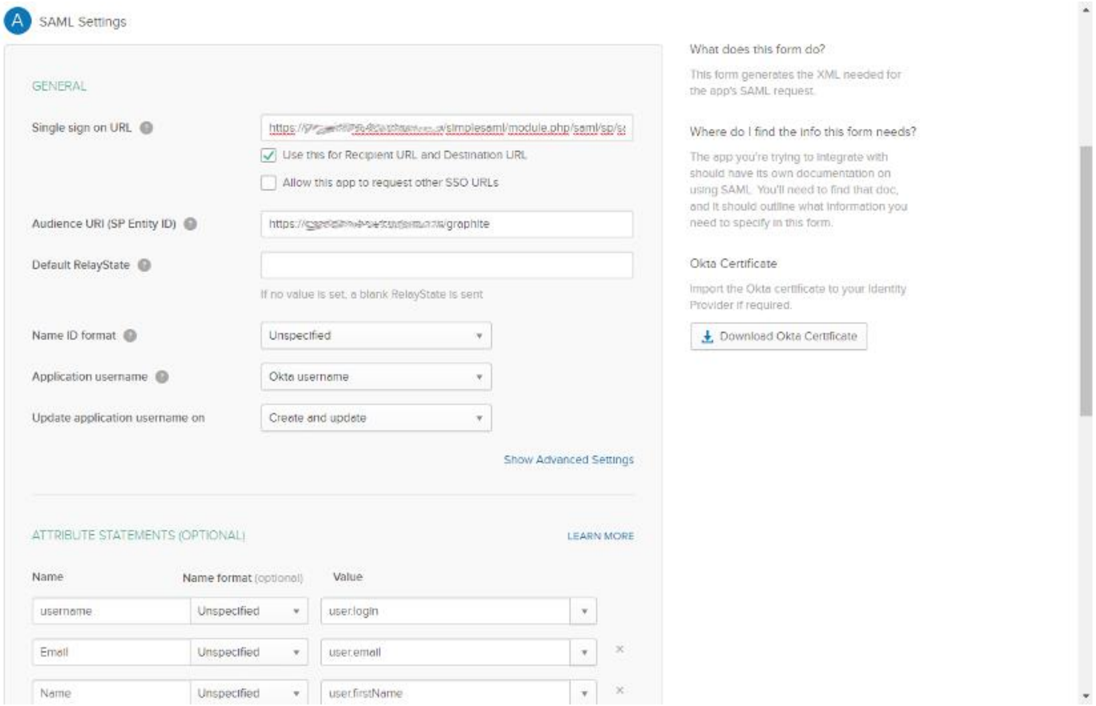
    a. Okta username (default)

   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.



GENERAL

Single sign on URL	https://[redacted]/simplesaml/module.php/saml/sp/sa
	☑ Use this for Recipient URL and Destination URL
	☐ Allow this app to request other SSO URLs
Audience URI (SP Entity ID)	https://[redacted]/graphite
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

ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Value
username	Unspecified	user.login
Email	Unspecified	user.email
Name	Unspecified	user.firstName

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

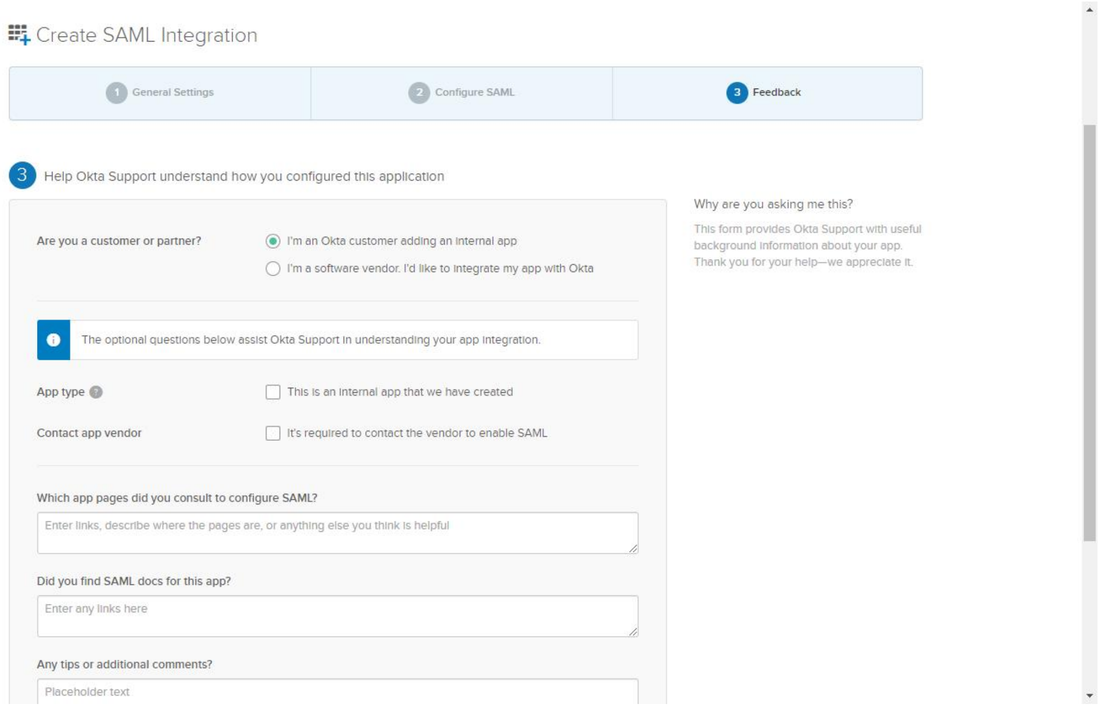
Import the Okta certificate to your Identity Provider if required.

2.1.4 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.



Create SAML Integration

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

Contact app vendor □ It's required to contact the vendor to enable SAML

Which app pages did you consult to configure SAML?
Enter links, describe where the pages are, or anything else you think is helpful

Did you find SAML docs for this app?
Enter any links here

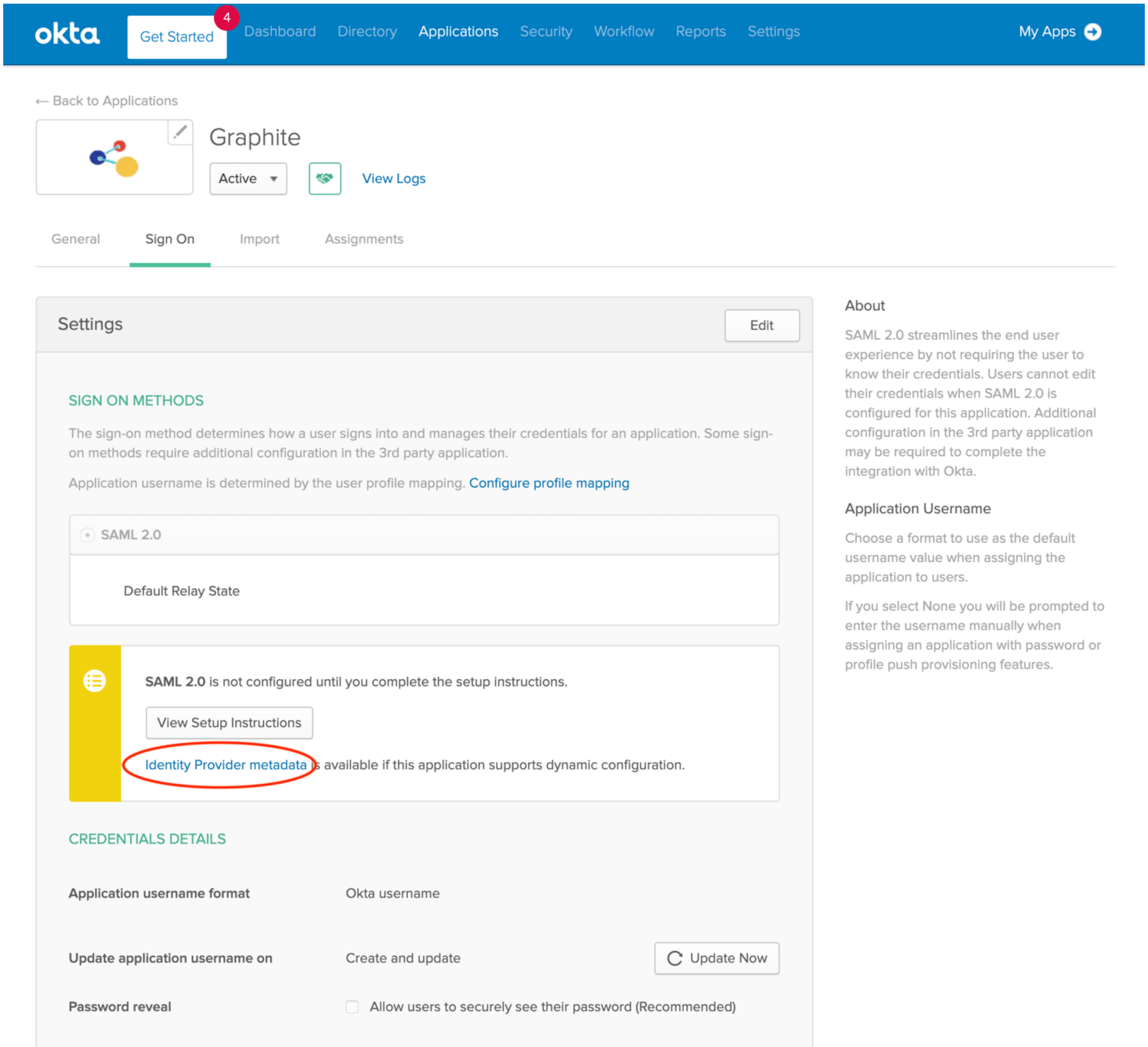
Any tips or additional comments?
Placeholder text

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.

2.2 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.



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

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
Update application username on	Create and update
Password reveal	□ Allow users to securely see their password (Recommended)

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.

2.3 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.

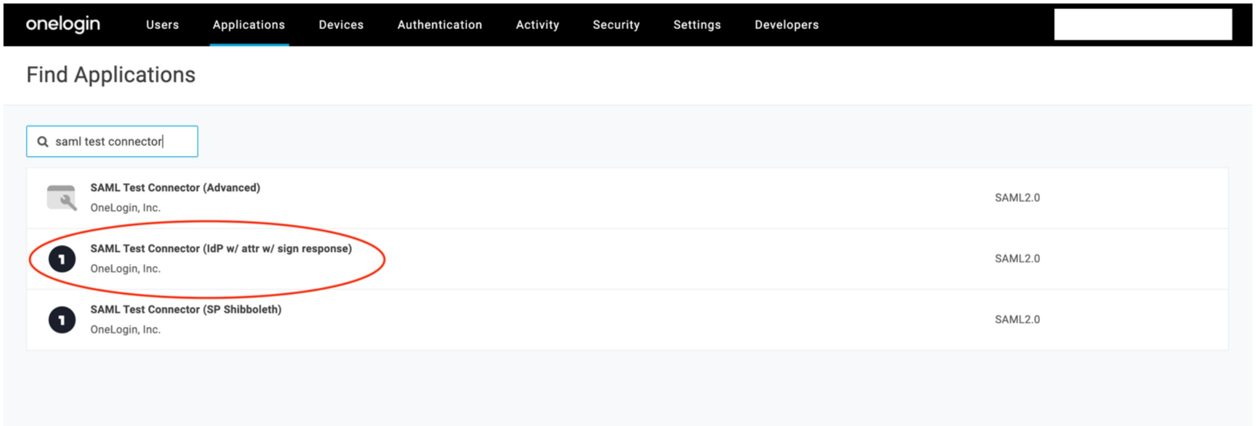
3 Setting Up Graphite in OneLogin

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)*.

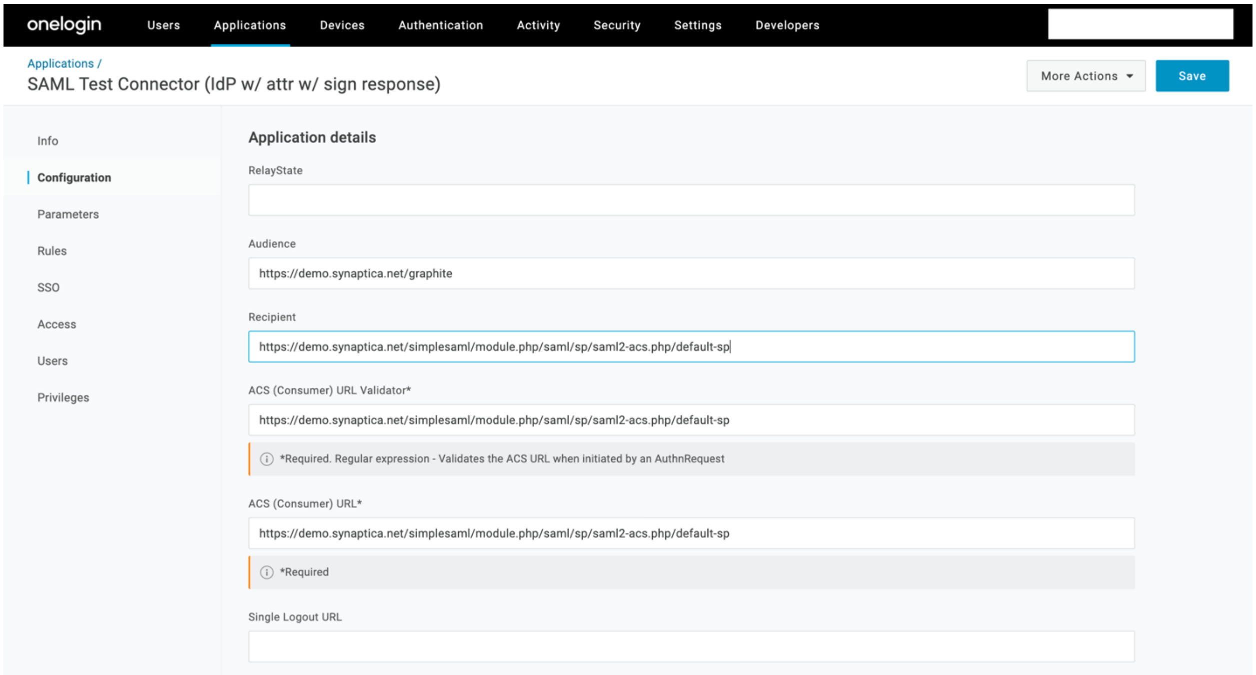


Find Applications

saml test connector

SAML Test Connector (Advanced) OneLogin, Inc.	SAML2.0
SAML Test Connector (IdP w/ attr w/ sign response) OneLogin, Inc.	SAML2.0
SAML Test Connector (SP Shibboleth) OneLogin, Inc.	SAML2.0

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.



SAML Test Connector (IdP w/ attr w/ sign response)

Application details

RelayState

Audience
https://demo.synaptica.net/graphite

Recipient
https://demo.synaptica.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

ACS (Consumer) URL Validator*
https://demo.synaptica.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
*Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest

ACS (Consumer) URL*
https://demo.synaptica.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
*Required

Single Logout URL

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.

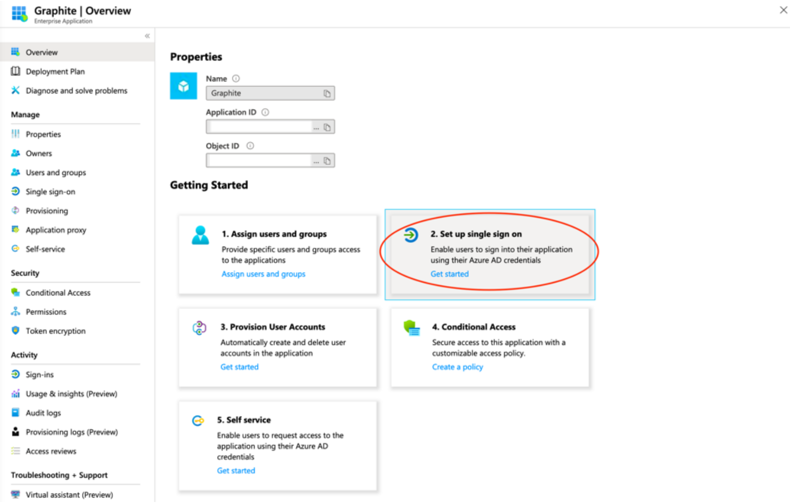
4 Setting Up Graphite in Azure Active Directory

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.



Graphite | Overview
Enterprise Application

Properties

Name: Graphite

Getting Started

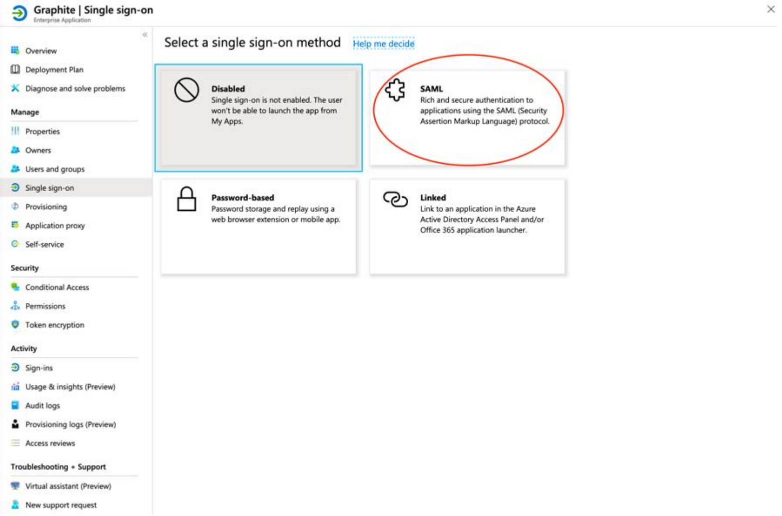
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started



Graphite | Single sign-on
Enterprise Application

Select a single sign-on method   Help me decide

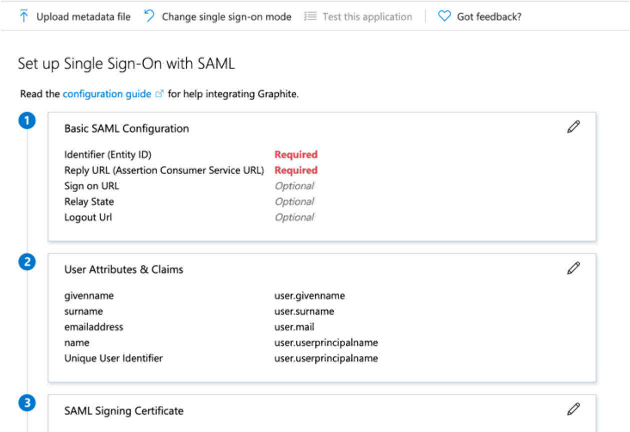
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

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.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating Graphite.

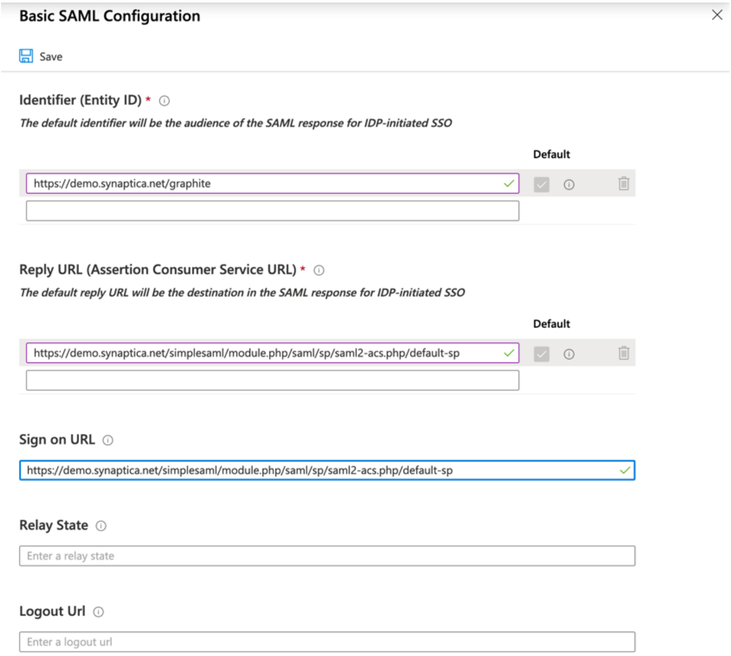
1 Basic SAML Configuration

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



Basic SAML Configuration

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

https://demo.synaptica.net/graphite

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://demo.synaptica.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

Sign on URL

https://demo.synaptica.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

Relay State

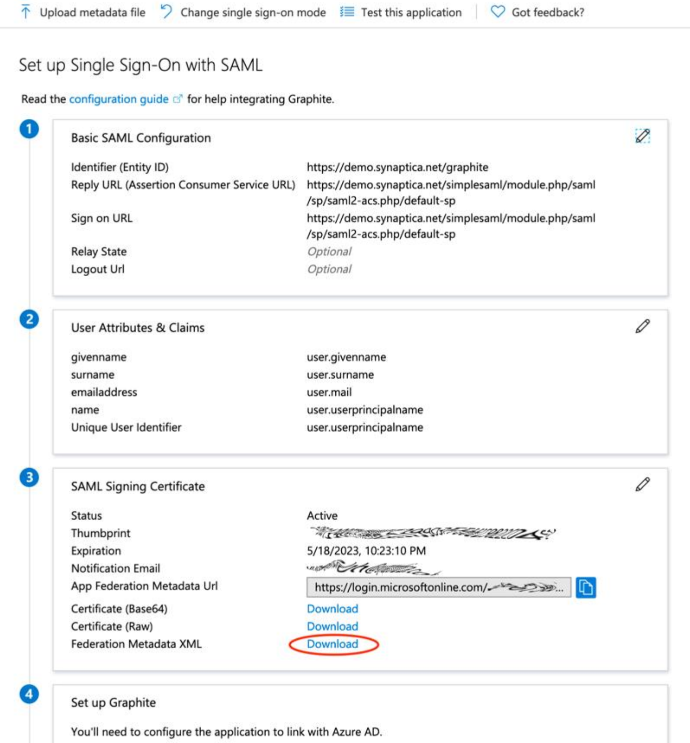
Enter a relay state

Logout Url

Enter a logout url

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.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating Graphite.

1 Basic SAML Configuration

Identifier (Entity ID)	https://demo.synaptica.net/graphite
Reply URL (Assertion Consumer Service URL)	https://demo.synaptica.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
Sign on URL	https://demo.synaptica.net/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
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

Status	Active
Thumbprint	[redacted]
Expiration	5/18/2023, 10:23:10 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/[redacted]...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Graphite

You'll need to configure the application to link with Azure AD.

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

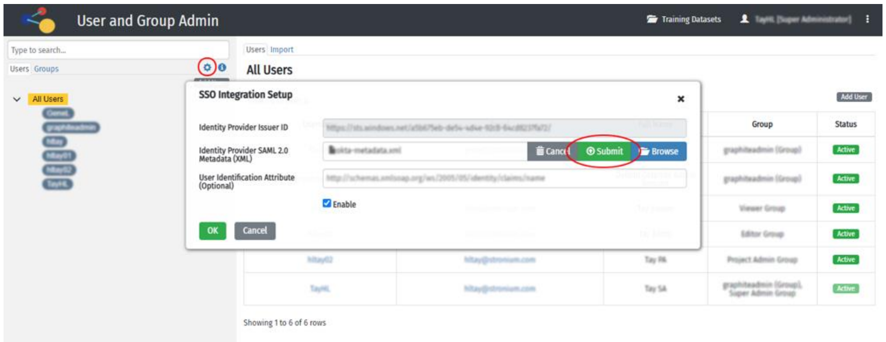
5 Completing the Setup of SSO in Graphite

1. To set up SSO in Graphite, please log in as an administrator.

2. Go to User 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 SSO Integration Setup icon as shown in the screenshot.



SSO Integration Setup

Identity Provider Issuer ID

Identity Provider SAML 2.0 Metadata (XML): okta-metadata.xml

User Identification Attribute (Optional): http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

☑ Enable

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 to activate SSO on the next login. Click OK 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.

6 Bypassing SSO

The systems administrator may allow bypassing SSO for troubleshooting. To allow bypassing of SSO, edit the file, config_graphite.php, in the tinymvc/myapp/configs directory, and set the *bypass-sso* option to *true*:

```
$graphite['bypass-sso'] = true;
```

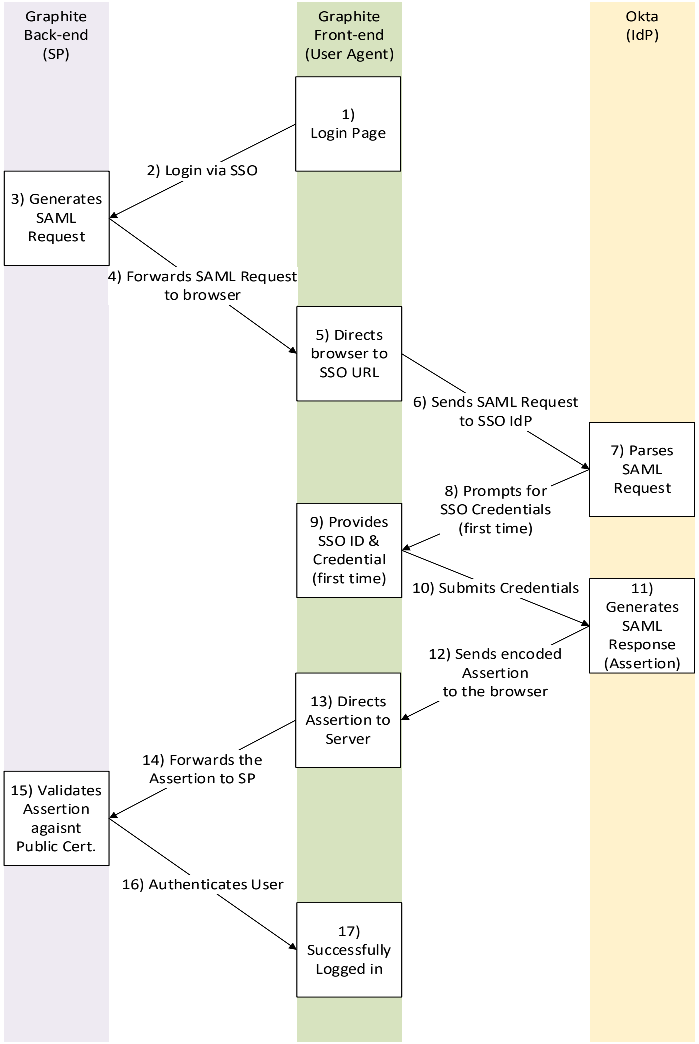
You can then access the login screen on your Graphite instance using the nosso=1 parameter, e.g.

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.

7 Appendix

7.1 Graphite SSO Flow


Graphite Back-end (SP)
Graphite Front-end (User Agent)
Okta (IdP)
1) Login Page
2) Login via SSO
3) Generates SAML Request
4) Forwards SAML Request to browser
5) Directs browser to SSO URL
6) Sends SAML Request to SSO IdP
7) Parses SAML Request
8) Prompts for SSO Credentials (first time)
9) Provides SSO ID & Credential (first time)
10) Submits Credentials
11) Generates SAML Response (Assertion)
12) Sends encoded Assertion to the browser
13) Directs Assertion to Server
14) Forwards the Assertion to SP
15) Validates Assertion agaisnt Public Cert.
16) Authenticates User
17) Successfully Logged in