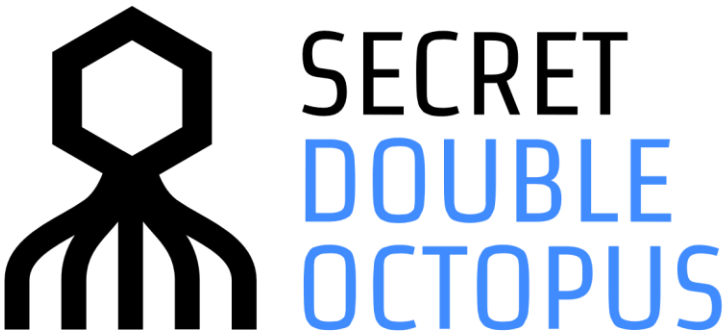
MARCH 26, 2020



How to Configure Octopus Authentication for Okta SSO Service

CONTENTS

Introduction

This document describes the configurations required for SAML 2.0 integration between the Octopus Authenticator and the Okta SSO service.

The integration process involves the following stages:

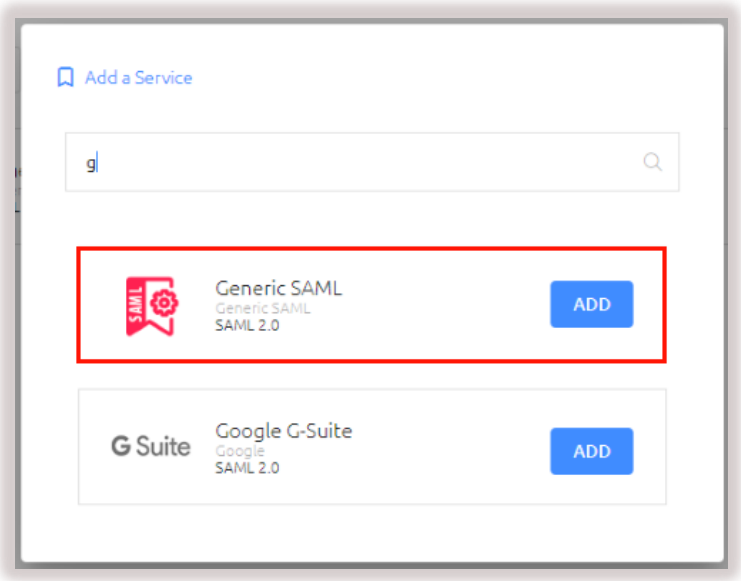
- Creating the Okta SAML Service in the Octopus Management Console
- Setting Up the Okta 3rd Party Identity Provider
- Completing Service Integration

Creating the Okta SAML Service

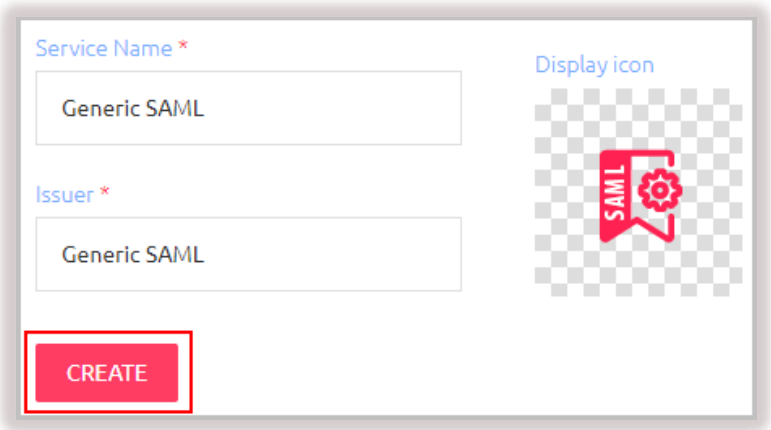
The following procedure explains how to create the required SAML service in the Octopus Management Console. The service settings will be used later when you configure the IdP setup in your Okta admin account.

To add and configure the Okta SAML service:

1. From the Octopus Management Console, open the **Services** menu and click **Add Service**. In the **Generic SAML** tile, click **Add**.

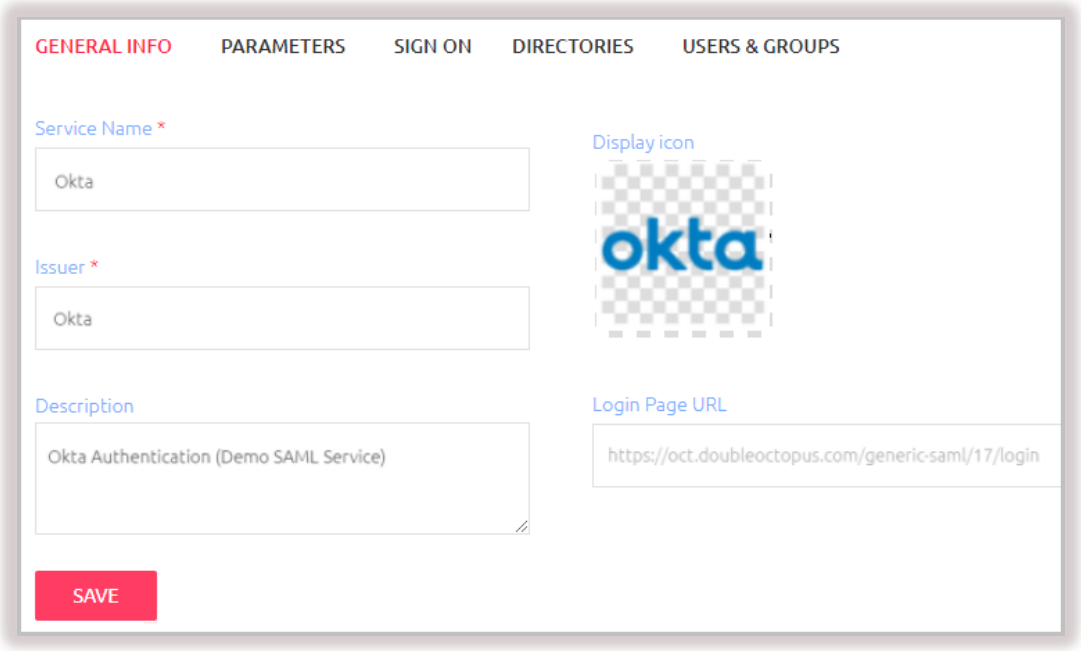


Then, in the dialog that opens, click **Create**.



2. Review and configure the following settings in the **General Info** tab:

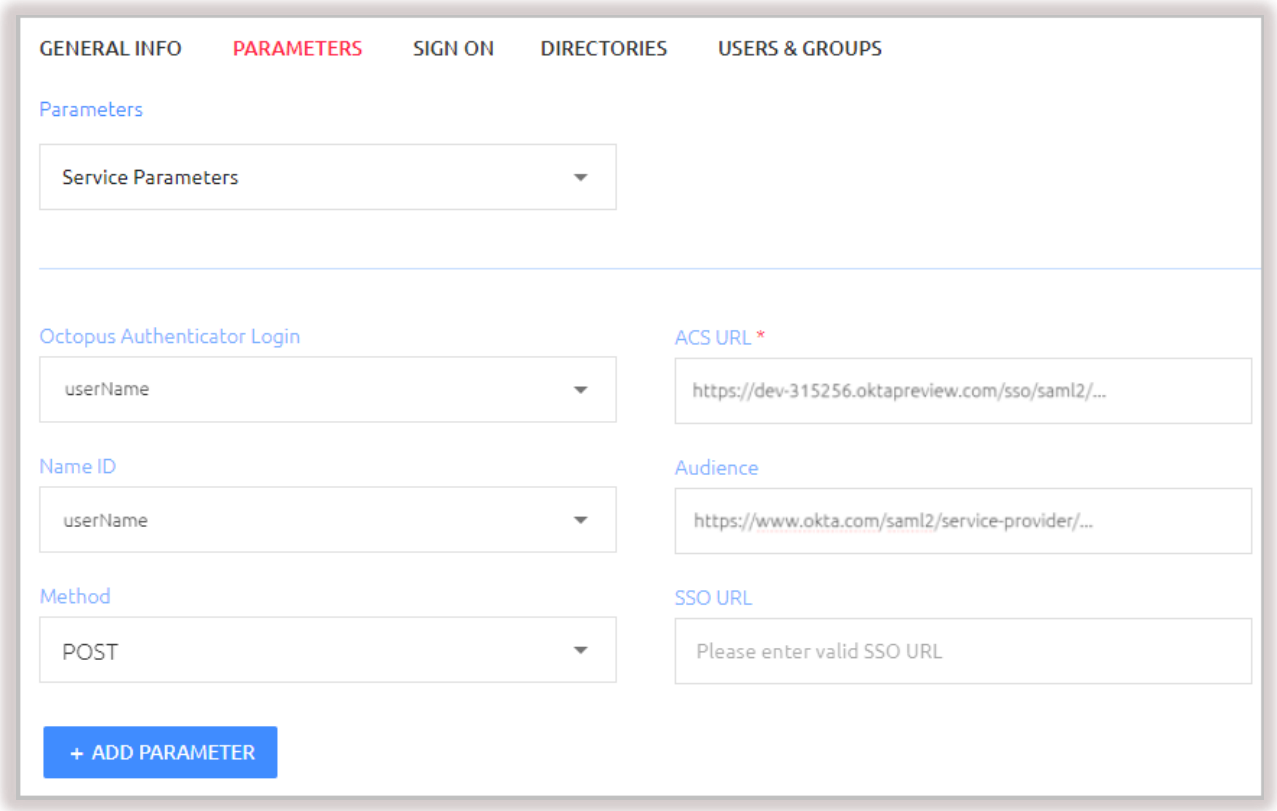
Setting	Value
Service Name	Okta
Issuer	Okta
Description	Okta authentication SAML service
Display icon	Click and upload an icon that will be displayed on the Login page for the service
Login Page URL	<https://<Enterprise Base URL>/generic-saml/<No.>/login>



3. At the bottom of the tab, click **Save**.

4. Open the **Parameters** tab and configure the following settings. You may add more parameters if you wish by clicking the **Add Parameter** button.

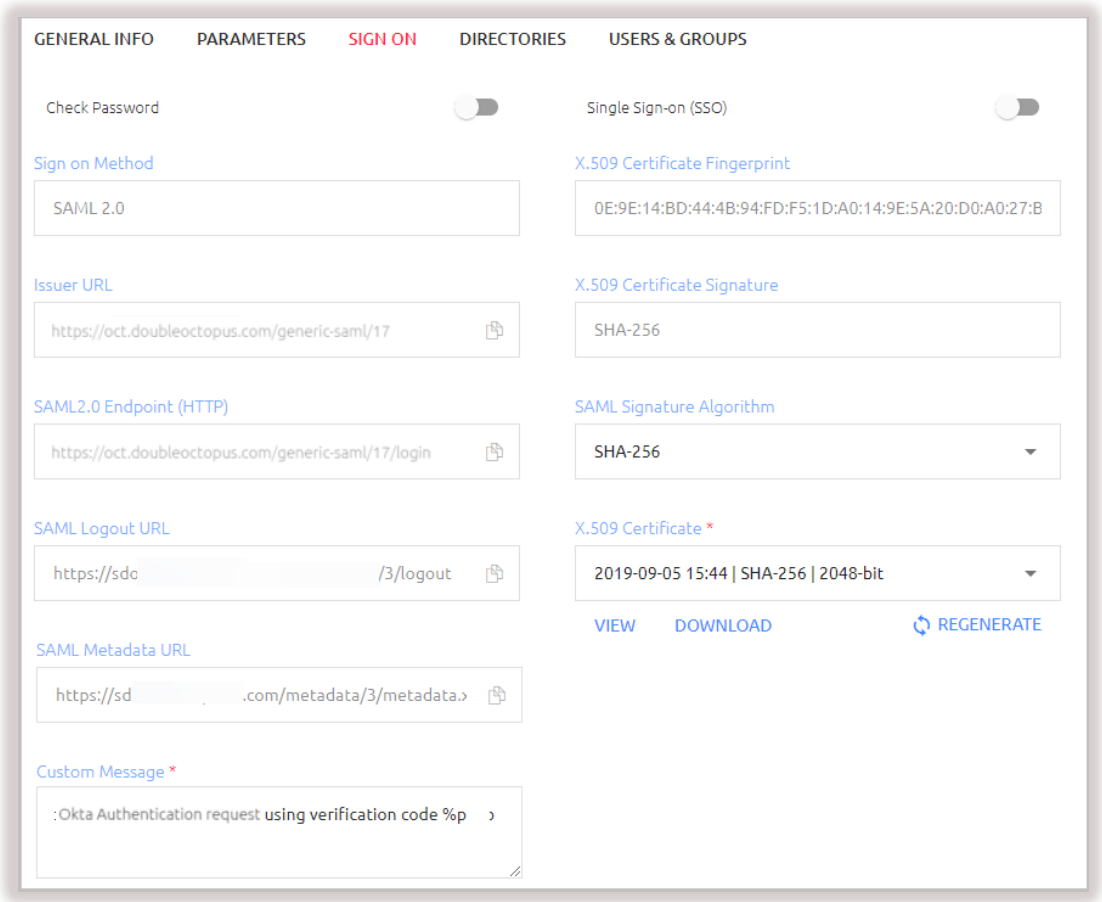
Setting	Value / Notes
Octopus Authentication Login	Login method for the Octopus Authentication Server
Name ID	Okta login username
Method	Binding mechanism for the Okta SAML request
ACS URL	Assertion Consumer Service URL for the Okta IdP
Audience	Audience URI for the Okta IdP



5. At the bottom of the tab, click **Save**.

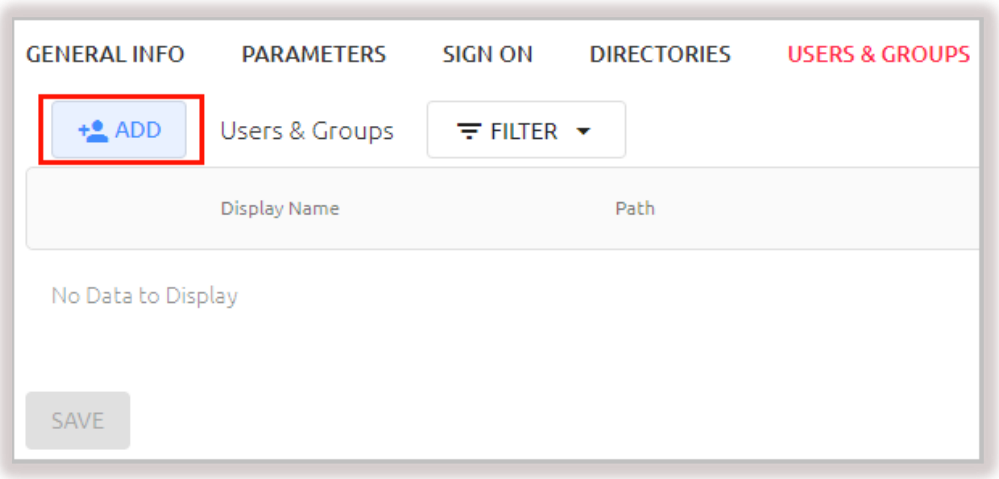
6. Open the **Sign On** tab and configure the following settings. It is recommended not to change default settings.

Setting	Value
Check Password	Disabled (default setting)
Single Sign-on (SSO)	Disabled (default setting)
Sign on Method	SAML 2.0
Issuer URL	The URL used by the service to connect to Octopus Authenticator, e.g., https://<Enterprise base URL>/ generic-saml/<No>
SAML 2.0 Endpoint (HTTP)	The URL used by the service to communicate with the SAML Login page, e.g., https://<Enterprise base URL>/generic-saml/login
SAML Signature Algorithm	SHA-256 (default)
X.509 Certificate	X.509 certificate for the Octopus Authenticator Salesforce service
Custom Message	The message that is shown to the user upon successful login. Use the %p tag to display the password in the message.



7. At the bottom of the **Sign On** tab, click **Save**.

8. Open the **Directories** tab, and select the checkbox of the directory to be integrated with the service. (Local or LDAP).
9. Open the **Users & Groups** tab and click **Add**.



A popup opens, with a list of directories displayed on the left.

10. Expand the relevant directory and select the checkboxes of the groups and users that you want to add to the service. Then, click **Done** to close the popup.

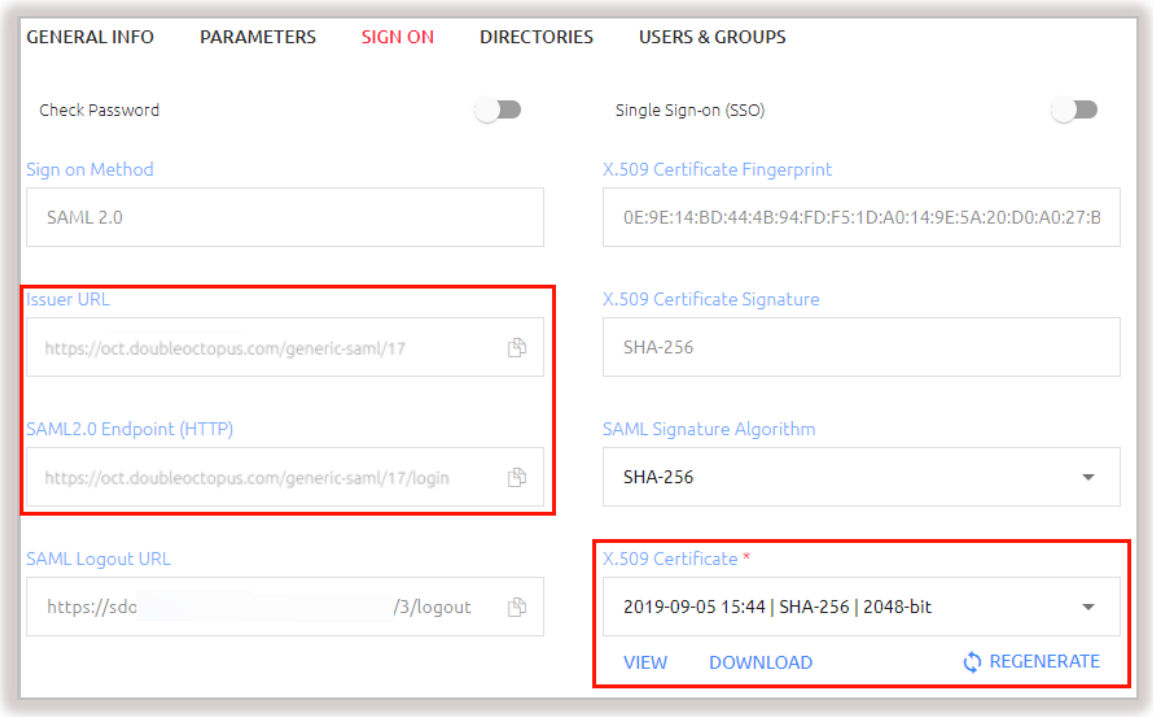
    The groups and users you selected are listed in the **Users & Groups** tab.
11. Click **Save** and publish your changes.

Setting Up the Okta 3rd Party Identity Provider

The procedure below explains how to configure the 3rd party identity provider in your Okta Admin account to support integration with Octopus Authenticator.

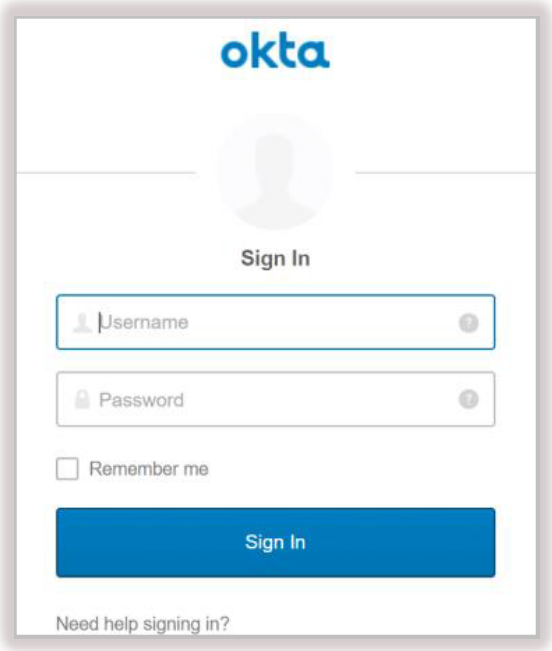
Before you begin, make sure that you have access to the following elements. They can be copied or downloaded from the **Sign On** tab of the Okta SAML service that you created in the Octopus Management Console.

- **Issuer URL:** The URL used by the Okta service to connect to Octopus Authenticator. Click the Copy icon to copy the URL.
- **SAML2.0 Endpoint (HTTP):** The Octopus Authenticator Okta Login page URL to which the Okta service provider will refer users for Octopus authentication. Click the Copy icon to copy the URL.
- **X.509 Certificate:** Click **Download** to download the **cert.pem** file. You will use the file while configuring the Okta IdP.

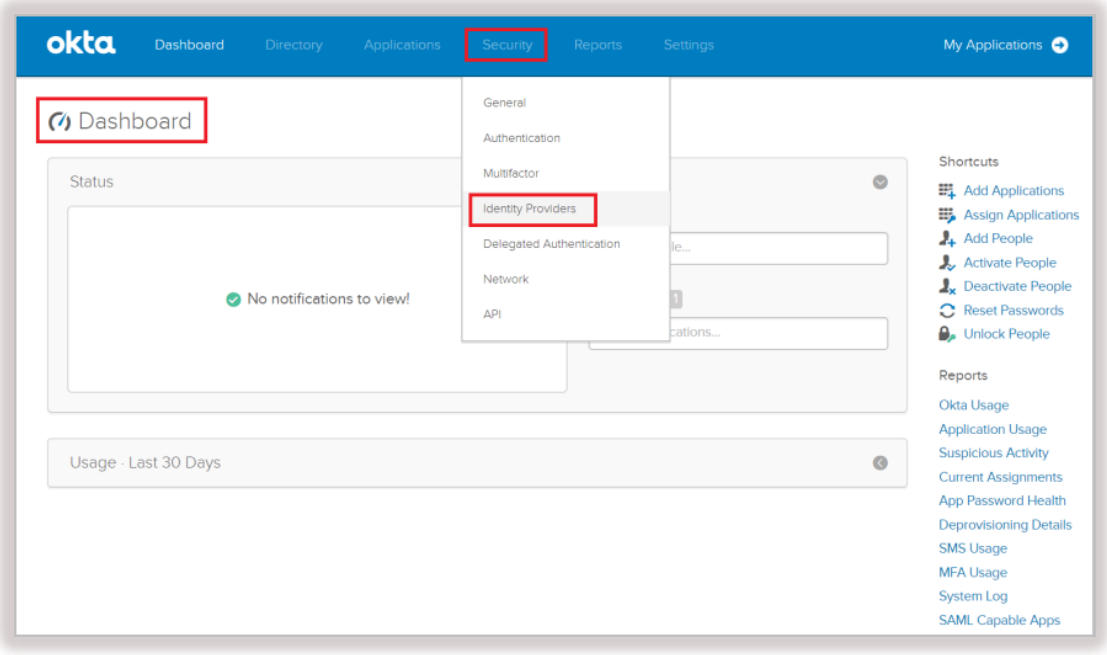


To set up the Okta 3rd party IdP:

1. Log into your Okta Admin account.



2. From the Admin Dashboard, navigate to **Security** > **Identity Providers**.

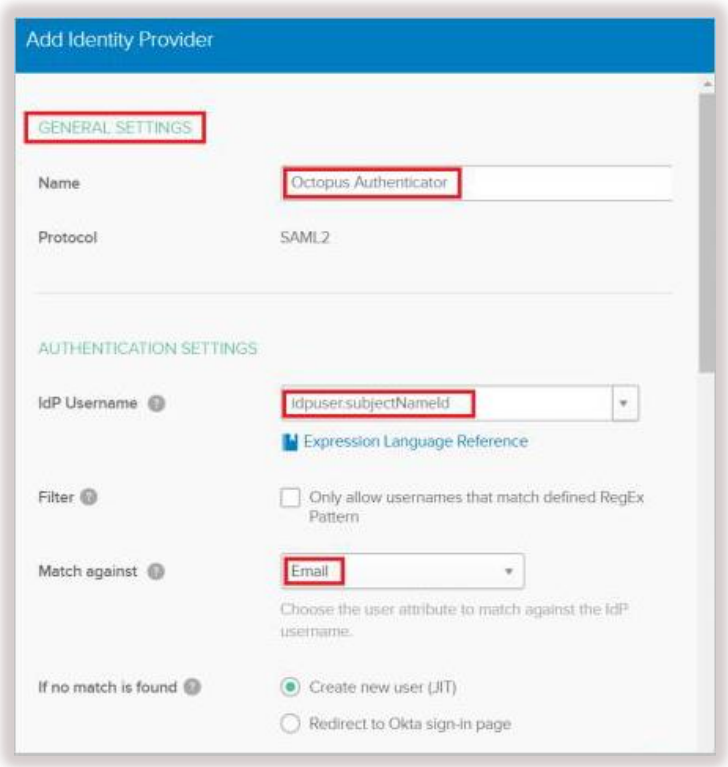


3. On the **Identity Providers** page, click **Add Identity Provider** and select **Add SAML 2.0 IdP**.

The **Add Identity Provider** dialog opens.

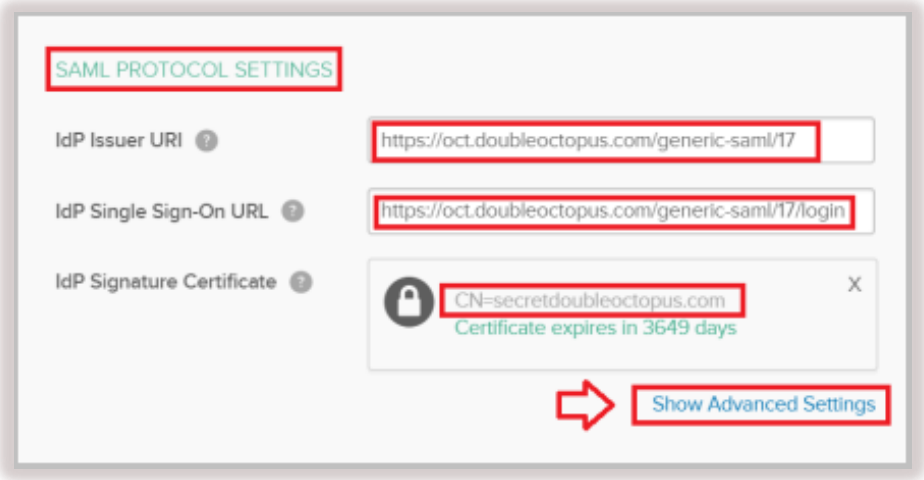
4. At the top of the dialog, configure the following settings:

Setting	Value / Notes
Name	Octopus Authenticator
IdP Username	Select **idpuser.subjectNameId** (default value)
Match against	Select **Email** (or another option, as required by your setup)



5. Scroll down to **SAML Protocol Settings**, and configure the following settings:

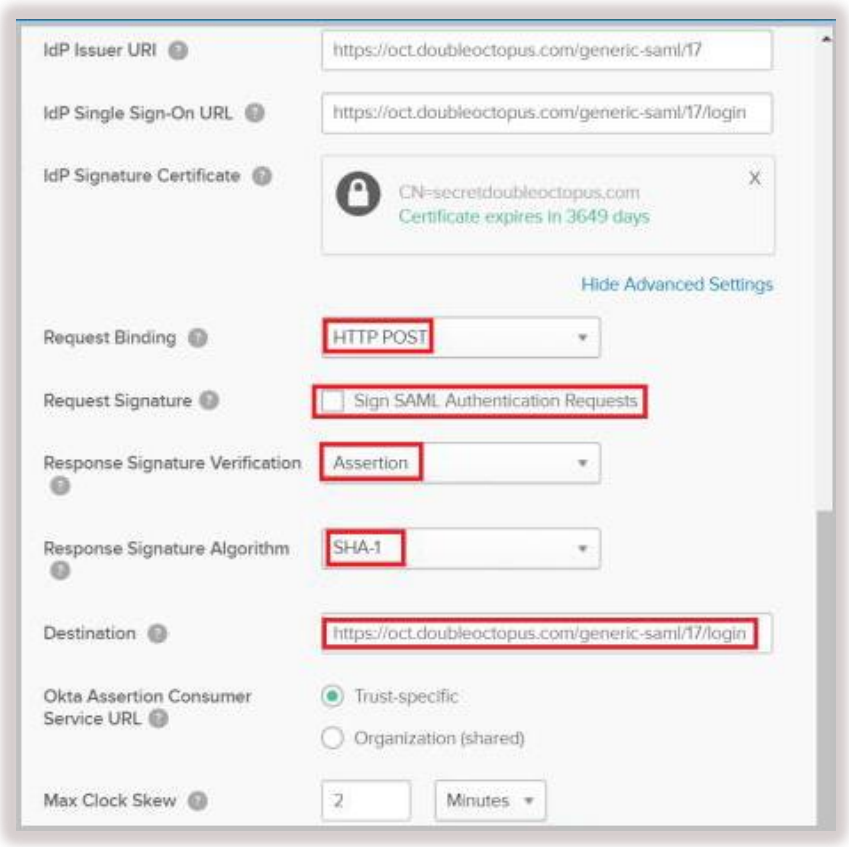
Setting	Value / Notes
IdP Issuer URI	Paste the **Issuer URL** (from the Okta SAML service in the Octopus Management Console) in the field.
IdP Single Sign-on URL	Paste the **SAML2.0 Endpoint (HTTP)** in the field.
IdP Signature Certificate	Upload the **X.509 certificate** file that you downloaded from the Okta SAML service in the Octopus Management Console.



Then, click **Show Advanced Settings**.

6. Under **Advanced Settings**, configure the following settings:

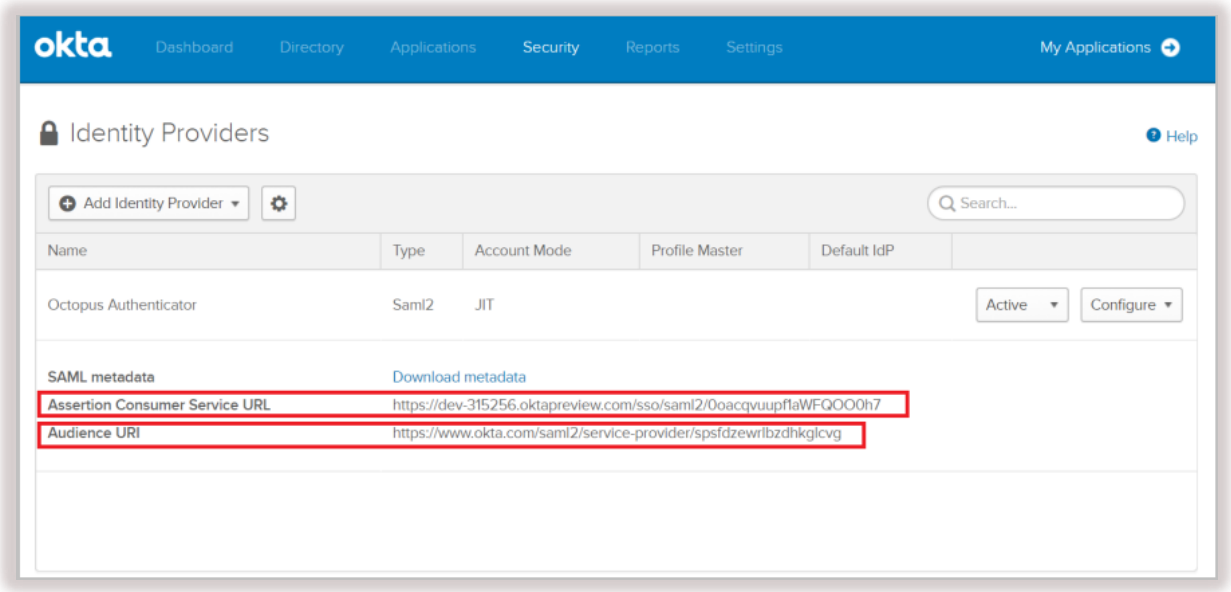
Setting	Value / Notes
Request Binding	Select **HTTP POST** or **HTTP GET**
Request Signature	Keep the checkbox *unchecked*.
Response Signature Verification	Select **Assertion**
Response Signature Algorithm	Select **SHA-1**
Destination	Paste the **SAML2.0 Endpoint (HTTP)** in the field. (Copy the value from the Okta SAML service in the Octopus Management Console.)



7. At the bottom of the page, click **Add Identity Provider**.

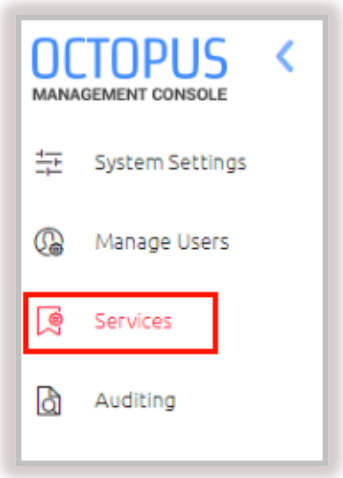
Completing Service Integration

The final phase of the integration involves copying some data from the Okta IdP into the settings of the Okta SAML service you created in the Octopus Management Console. The parameters you need to copy are shown in the following figure.



To complete service integration:

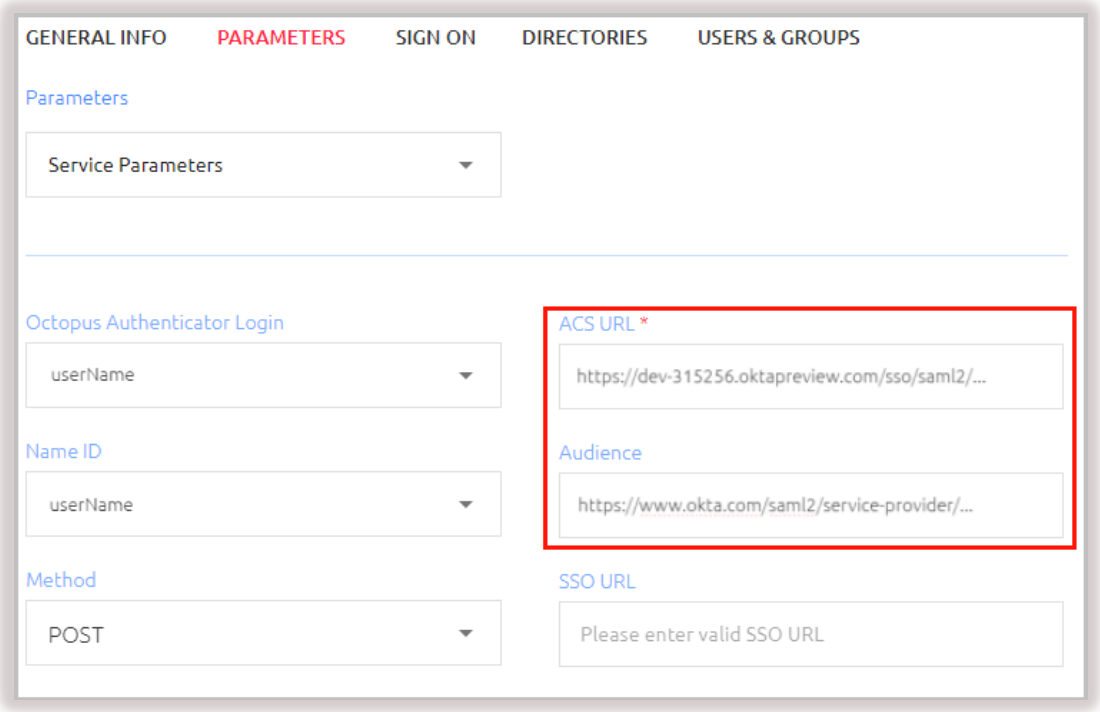
1. Log into the Octopus Management Console and open the **Services** menu.



2. In the tile of the Okta SAML service, click ✎ to display the service settings.

3. Open the **Parameters** tab and set the following parameters:

Setting	Value / Notes
ACS URL	Set the value to the **Assertion Consumer Service URL** of the Okta IdP.
Audience	Set the value to the **Audience URI** of the Okta IdP.



4. Click **Save** and then publish your changes.