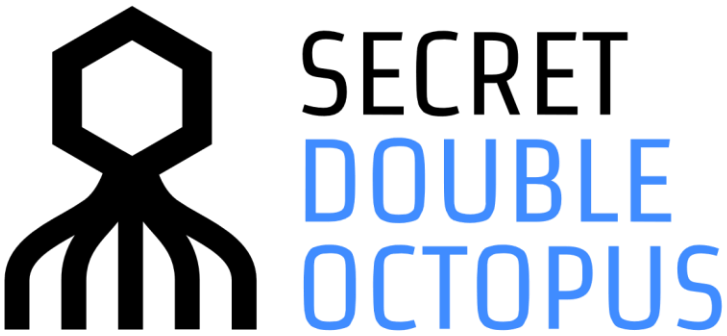
MARCH 8, 2020



Federating Okta Authentication to the Octopus Platform

CONTENTS

Introduction

Secret Double Octopus provides industry-leading security and flexibility for corporate authentication needs. Through support of the SAML2.0 protocol, Secret Double Octopus is able to integrate authentication from most corporate web-hosted platforms, including Okta.

This document describes how to federate authentication from Okta to the Secret Double Octopus authentication platform. The procedures in this guide focus on federating based on domain name. If your organization has different needs, you can select the appropriate rules as required.

This document is based on the latest release of Okta (as of February 21st, 2020) and version 4.4.0 of the Secret Double Octopus authentication platform.

Federation Overview

The following steps are required to federate authentication from Okta to the Secret Double Octopus authentication platform:

1. Creating a SAML 2.0 Service in the Octopus Management Console
2. Creating a SAML IDP in the Okta Management Platform
3. Creating an Identity Provider Routing Rule in the Okta Management Platform
4. Configuring SAML 2.0 Service Parameters in the Secret Double Octopus Platform

The following table matches SAML terminology between Okta and Secret Double Octopus:

Okta	Secret Double Octopus
IdP Issuer URI	Issuer URL
IdP Single Sign-On URL	SAML 2.0 Endpoint (HTTP)
IdP Signature Certificate	X.509 Certificate
Destination	SAML 2.0 Endpoint (HTTP)

Authentication Process Flow

The process flow for federated authentication with Okta is:

1. The user accesses the Okta portal Login page at *https://<YourDomain>.okta.com*
2. The user enters a username.

   If the username matches a rule for federated authentication, the flow continues with Step 3.

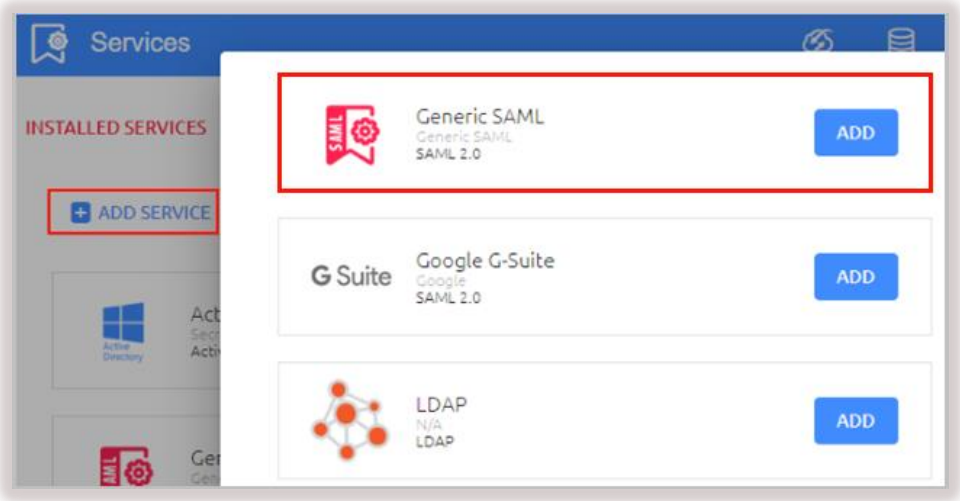
   If the username does NOT match a rule for federated authentication, the user is authenticated by Okta.
3. The user is redirected to Secret Double Octopus authentication platform.
   a. The user receives a push notification on the enrolled mobile phone (or receives a prompt for FIDO authentication).
   b. The user approves authentication.
   c. Secret Double Octopus sends a SAML authorization token to Okta.
   d. The user is redirected to the Okta portal and is logged in.

Creating a SAML 2.0 Service in the Octopus Management Console

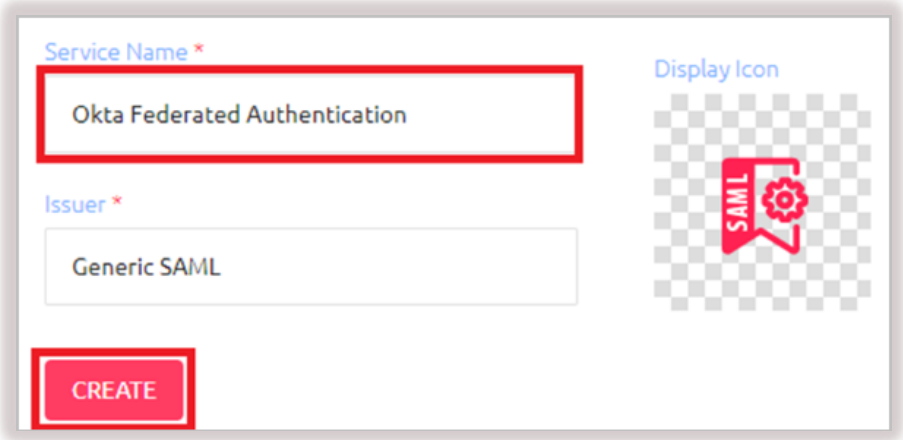
The procedure below explains how to add the SAML 2.0 service and copy some of the service settings. You will use these settings later to complete configuration in the Okta Management Platform.

To add the SAML 2.0 service:

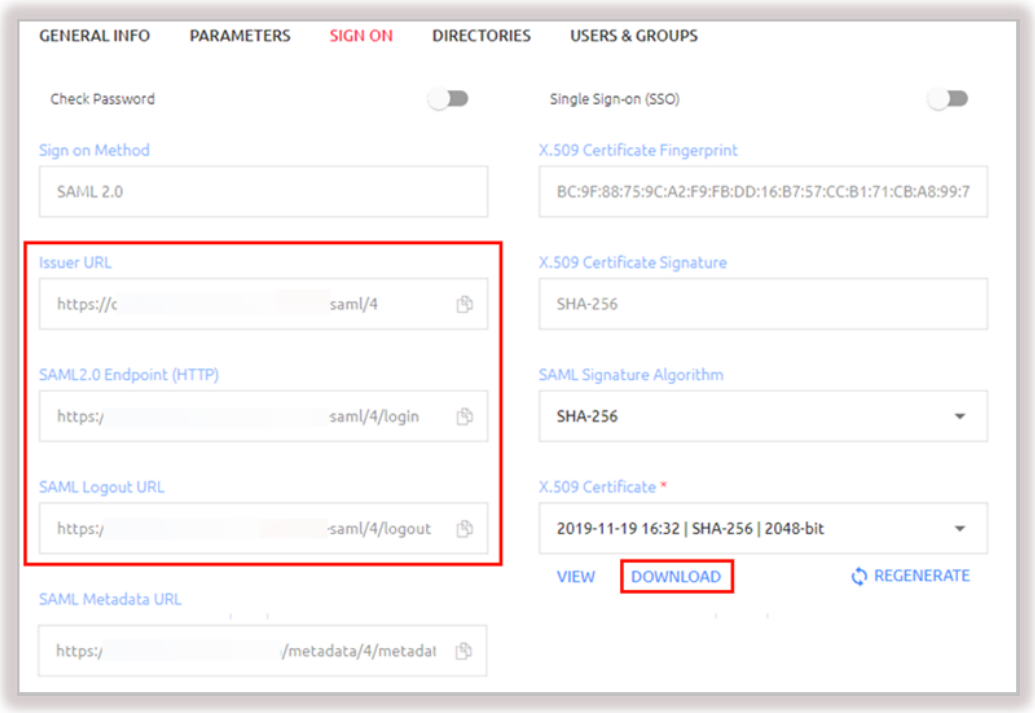
1. From the Octopus Management Console, open the **Services** menu and click **Add Service**. Scroll to **Generic SAML** and click **Add**.



2. In the dialog that opens, enter a meaningful Service Name (such as the one shown below). Then, click **Create**.



3. Open the **Sign On** tab, and copy the **Issuer URL**, **SAML 2.0 Endpoint (HTTP)** and **SAML Logout URL** in separate lines in a Notepad or text editor file.



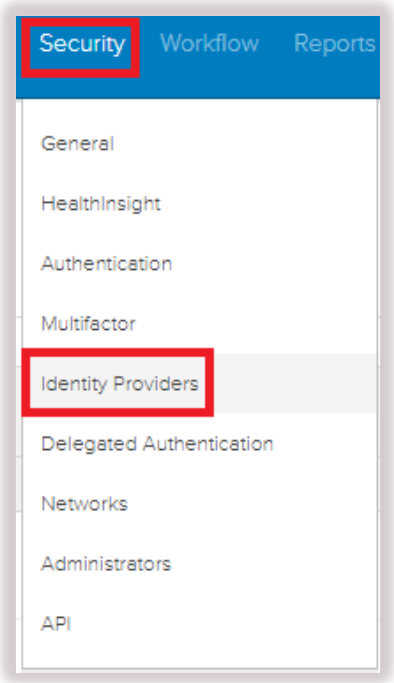
Then, download the X.509 Certificate file to your machine.

Creating a SAML IDP in the Okta Management Platform

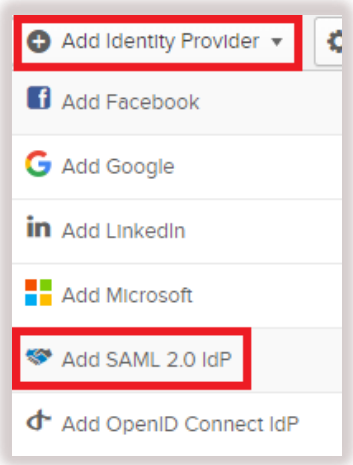
Follow the procedure below to configure a third-party Identity Provider (IdP).

To create a SAML IdP:

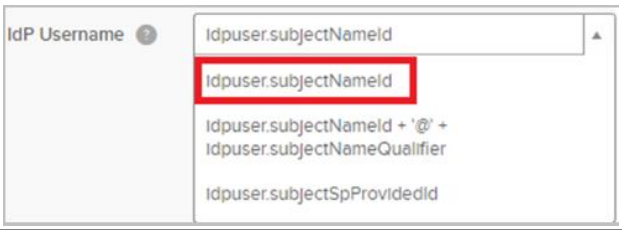
1. Log into your Okta portal as an administrator and navigate to **Security > Identity Providers**.



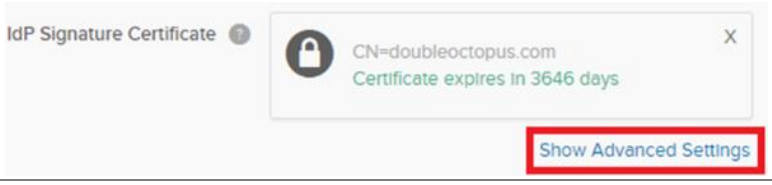
2. Select **Add Identity Provider > Add SAML 2.0 IdP**.



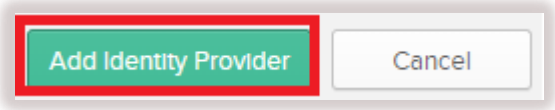
3. In the **General Settings** section, configure the following settings:

Setting	Value / Notes
Name	Enter a meaning name, e.g., Octopus Authenticator
IdP Username	Select **idpuser.subjectNameId** 
Match against	Select **Email**
If no match is found	Select **Redirect to Okta sign-in page**

4. In the **SAML Protocol Settings** section, configure the following settings:

Setting	Value / Notes
IdP Issuer URI	Paste the **Issuer URL** from the Octopus SAML 2.0 service settings
IdP Single Sign-On URL	Paste the **SAML2.0 Endpoint (HTTP)** from the Octopus SAML 2.0 service settings
IdP Signature Certificate	Browse to the x.509 Certificate that you exported from the SAML service and upload it. Then, click **Show Advanced Settings**. 
Request Binding	Select **HTTP POST**
Response Signature Verification	Select **Assertion**
Destination	Paste the **SAML2.0 Endpoint (HTTP)** from the Octopus SAML 2.0 service settings
Okta Assertion Consumer Service URL	Select the **Trust-specific** radio button

5. Click **Add Identity Provider**.



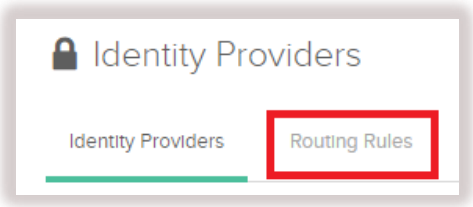
Creating an Identity Provider Routing Rule

The procedure below presents the steps required to create a routing rule within the Okta platform to send authentication requests to the Secret Double Octopus platform.

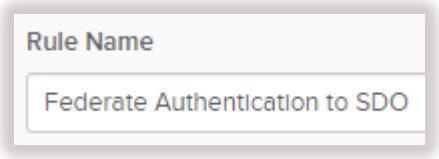
The rule created in this example instructs Okta to send any username that has a specific domain to the configured Identity Provider. The actual trigger that determines which users are routed to the Identity Provider may vary according to your business needs.

To create an Identity Provider routing rule:

1. In the Okta portal, navigate to **Security > Identity Providers**.
2. Select **Routing Rules**.

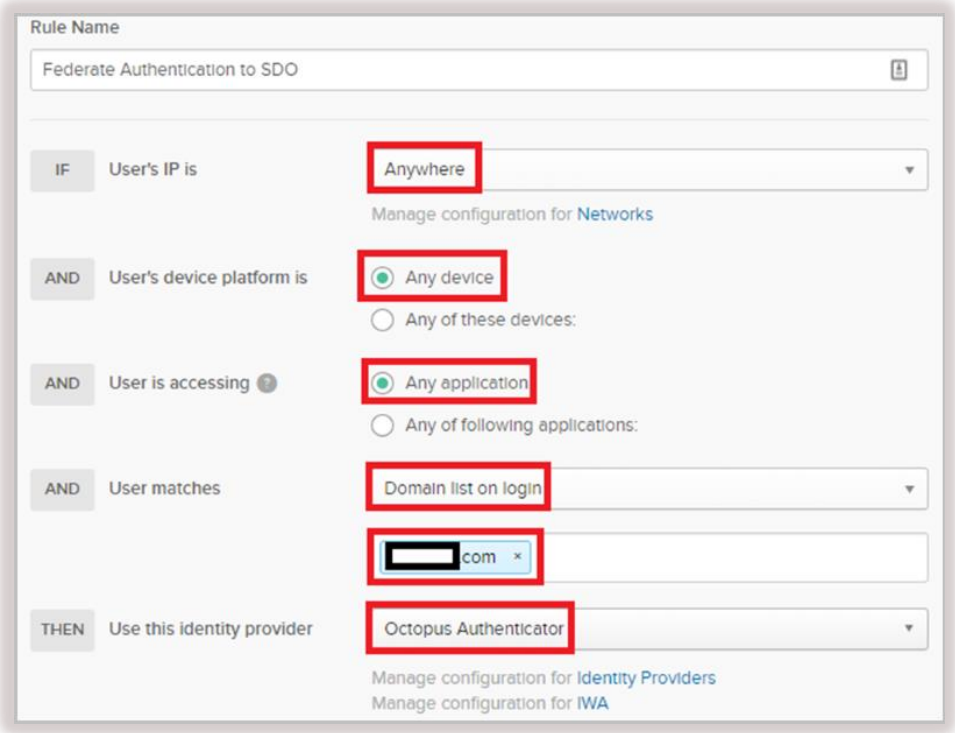


   Then, click **Add Routing Rule**.
3. In the **Rule Name** field, enter a descriptive name, e.g., **Federate Authentication to SDO**.



4. Configure the rule settings as follows:

Setting	Value / Notes
IF User's IP is	Select **Anywhere**
AND User's device platform is	Select **Any device**
AND User is accessing	Select **Any application**
AND User matches	Select **Domain list on login**. Then, in the field below, enter your domain name.
THEN Use this identity provider	Select the Identity Provider you created earlier.



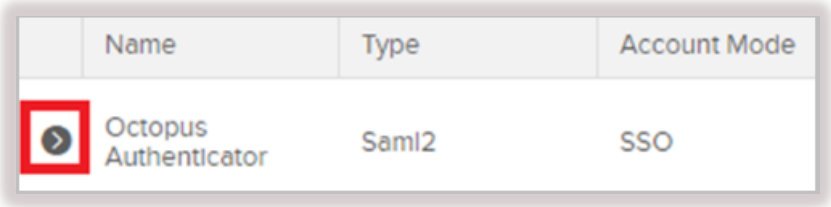
5. Click **Create Rule**.

Configuring SAML 2.0 Service Parameters

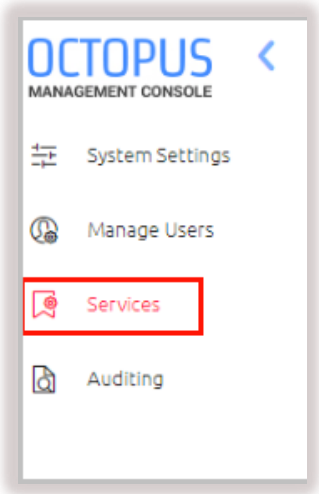
The procedure below outlines the final steps for configuring the SAML integration between Okta and Secret Double Octopus. In this final phase, you will copy information from the Okta Management Platform and complete the settings for the SAML 2.0 service in the Octopus Management Console.

To configure SAML 2.0 service parameters:

1. In the Okta portal, navigate to **Security > Identity Providers**.
2. Display the details of the IdP you created earlier by clicking the Expand icon.



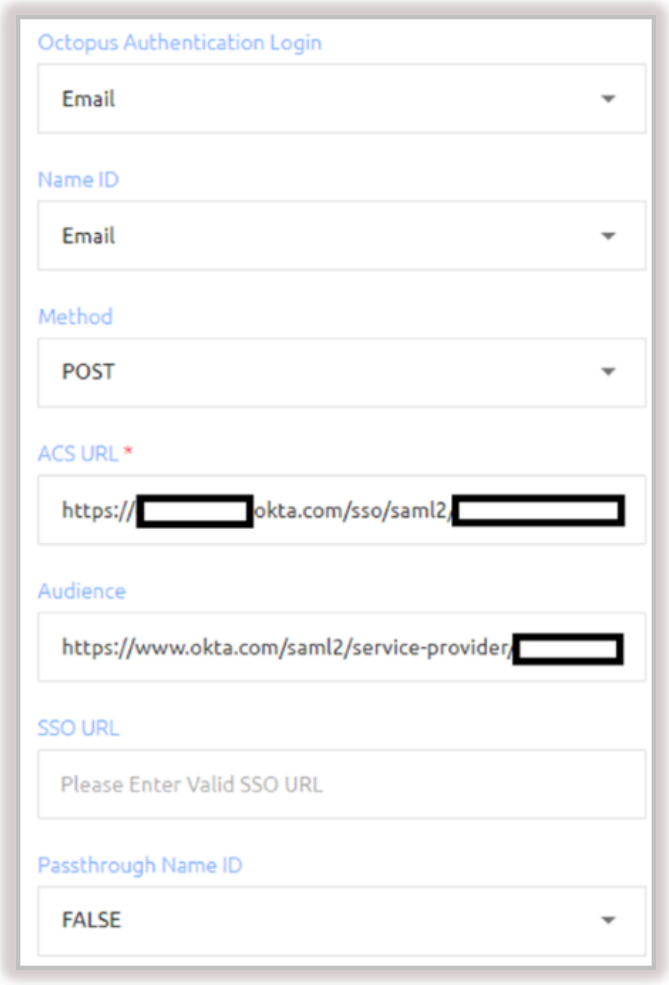
   Copy the **Assertion Consumer Service URL** and the **Audience URI** values to a text file.
3. Log into the Secret Double Octopus Management Console and select the **Services** menu.



4. In the tile of the SAML 2.0 service that you created earlier, click  to display the service settings.

5. Open the **Parameters** tab and configure the following settings:

Setting	Value / Notes
Octopus Authentication Login	Select **Email**
Name ID	Select **Email**
Method	Select **POST**
ASC URL	Paste the Okta Assertion Consumer URL here
Audience	Paste the Okta Audience URI here
Passthrough Name ID	Select **FALSE**



6. At the bottom of the page, click **Save**.
7. Publish your changes.