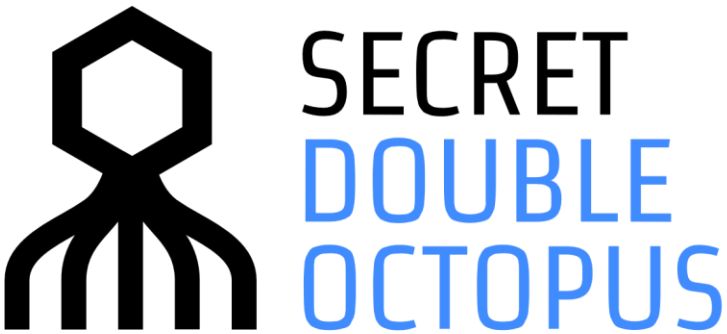
APRIL 19, 2020



How to Configure Octopus Authentication for the Idaptive Service

CONTENTS

Introduction

This document describes the configurations required for SAML 2.0 integration between the Octopus Authenticator and the Idaptive service. This integration utilizes Idaptive's partner management functionality.

The integration process involves the following sequential phases:

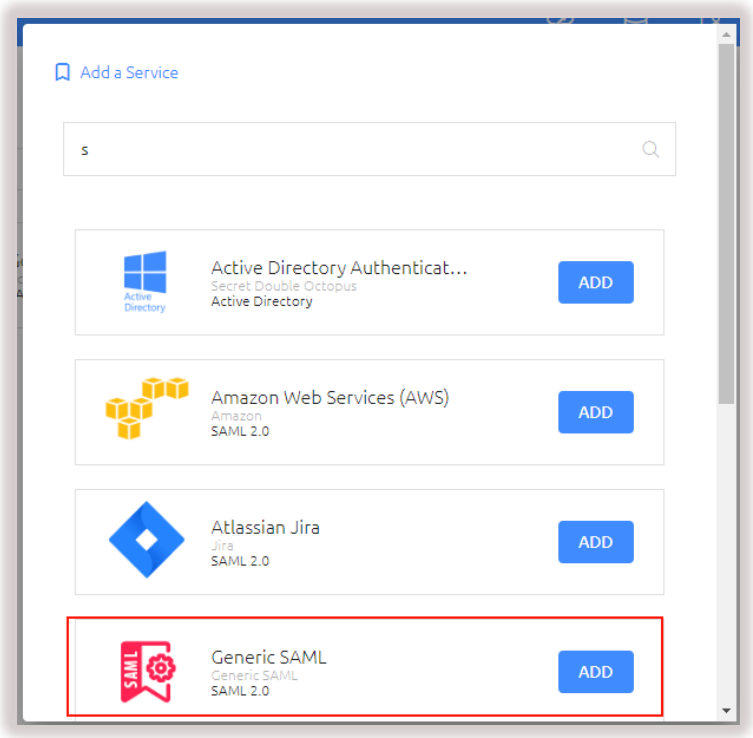
- Creating the Idaptive SAML Service
- Configuring the Idaptive Identity Provider Setup
- Completing Service Integration

Creating the Idaptive SAML Service

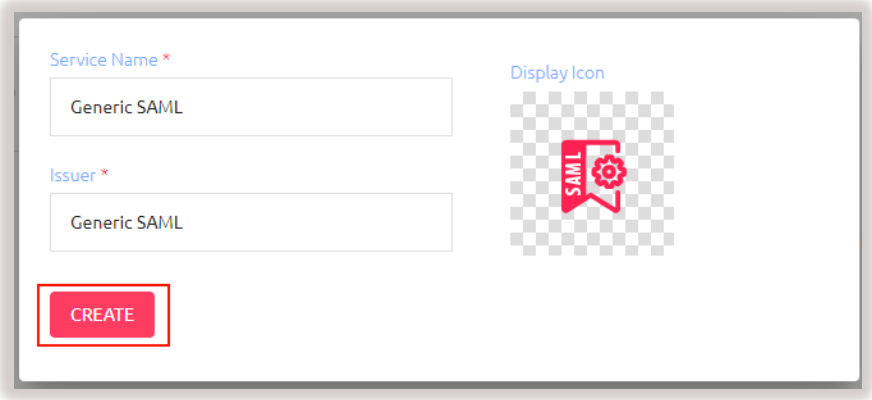
The following procedure explains how to create the required SAML service in the Octopus Management Console. The service settings will be used later in the Idaptive Identity Provider setup.

To add and configure the Idaptive SAML service:

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

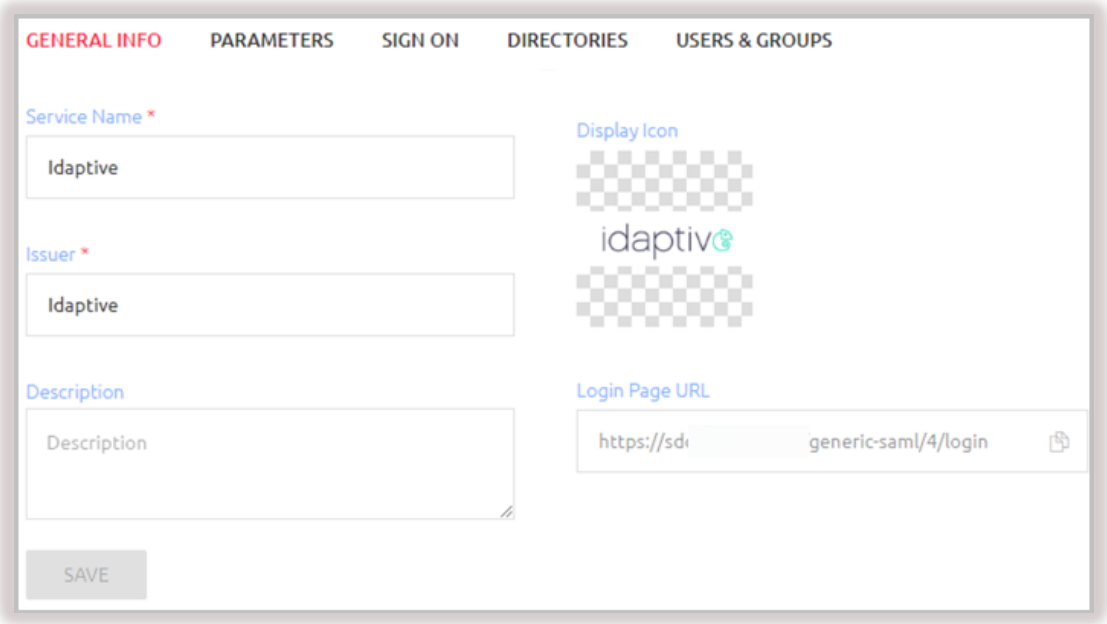


Then, in the dialog that opens, click **Create**.



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

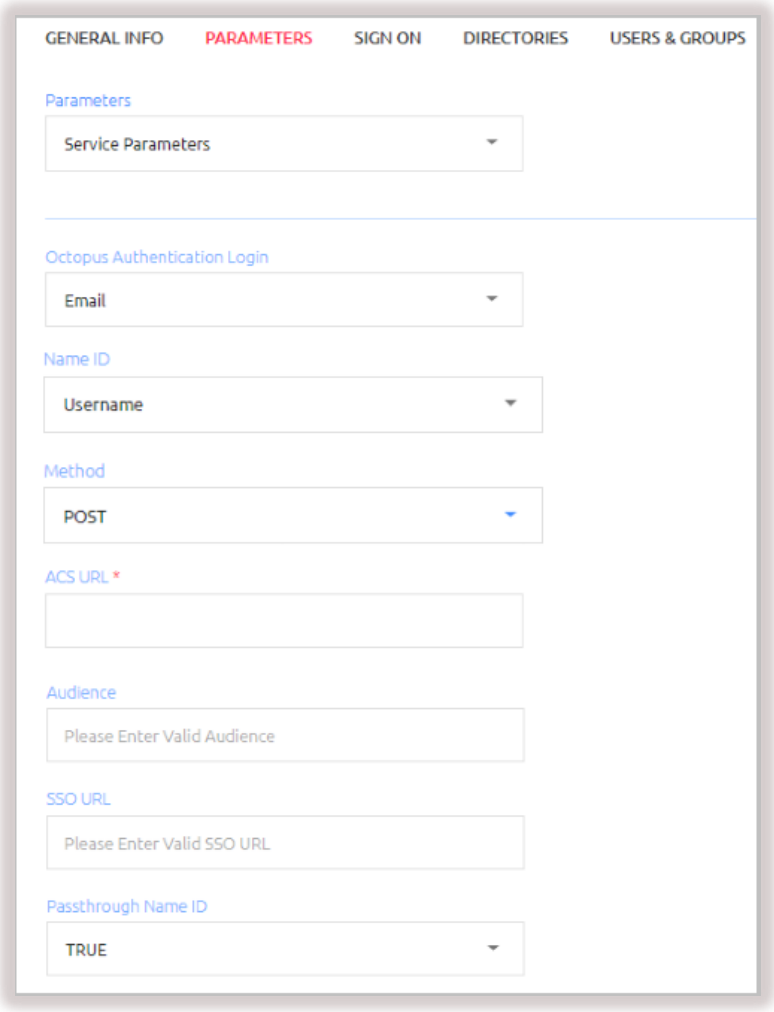
Setting	Description
Service Name	Idaptive
Issuer	Idaptive
Description	Enter a brief note about the service
Display icon	This icon will be displayed on the Login page for the service. To change the default icon, click and upload the image of your choice.
Login Page URL	<https://<Enterprise Base URL>/generic-saml/<No.>/login>



Then, click **Save**.

3. Open the **Parameters** tab and review the following settings. Do not configure any additional parameters.

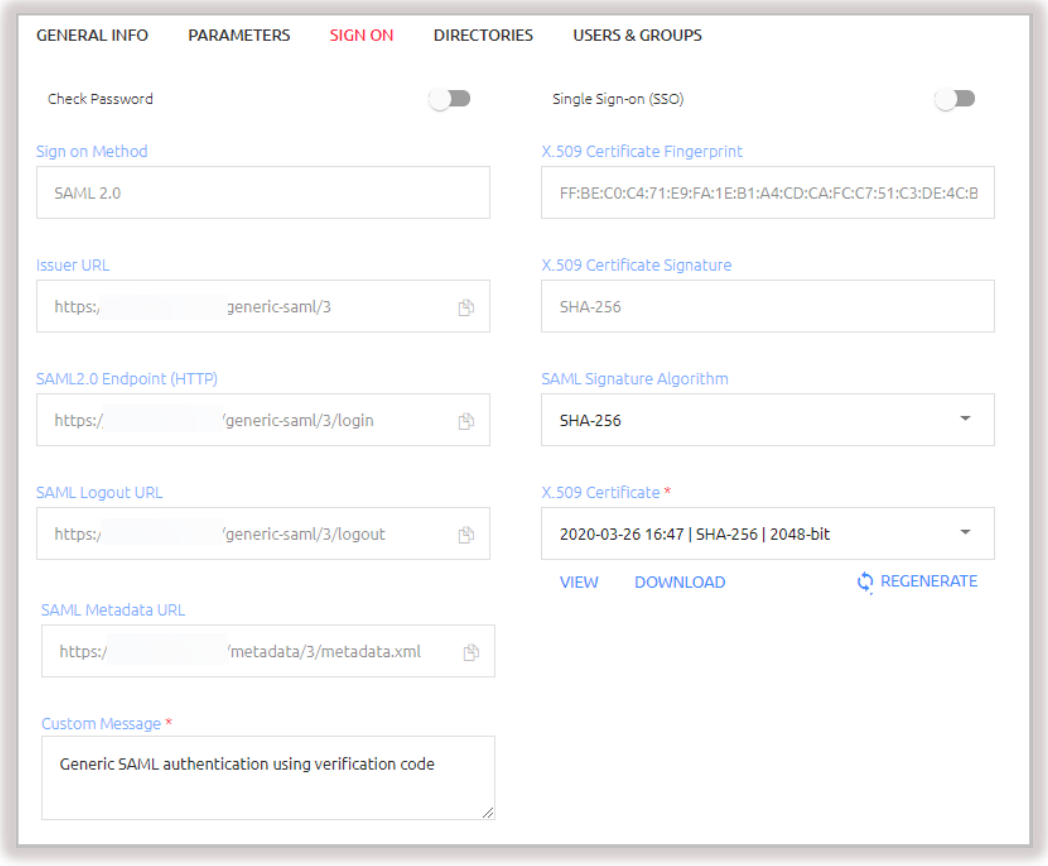
Setting	Value / Notes
Octopus Authentication Login	Select the login method for the Octopus Authenticator Server.
Name ID	Select the login method for the Idaptive service.
Method	Select **POST**.
ACS URL	The Service Provider Authentication Response URL for Idaptive's Identify Provider. You will add this parameter later, after you configure the IdP setup.



4. At the bottom of the **Parameters** tab, click **Save**.

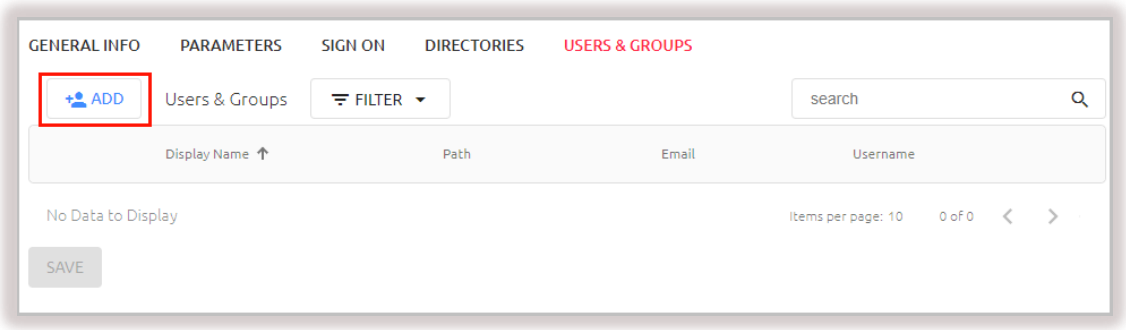
5. Open the **Sign On** tab and configure the following settings. We recommend not to change default values.

Setting	Value
Check Password	Disabled (default setting)
Single Sign-on (SSO)	Disabled (default setting)
Sign on Method	SAML 2.0
Issuer URL	https://<Enterprise base URL>/ generic-saml/<No>
SAML 2.0 Endpoint (HTTP)	https://<Enterprise base URL>/generic-saml/login
SAML Signature Algorithm	SHA-256 (default)
X.509 Certificate	X.509 certificate for the Octopus Authenticator Idaptive service
Custom Message	The message displayed to the user upon successful login



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

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



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

9. 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.

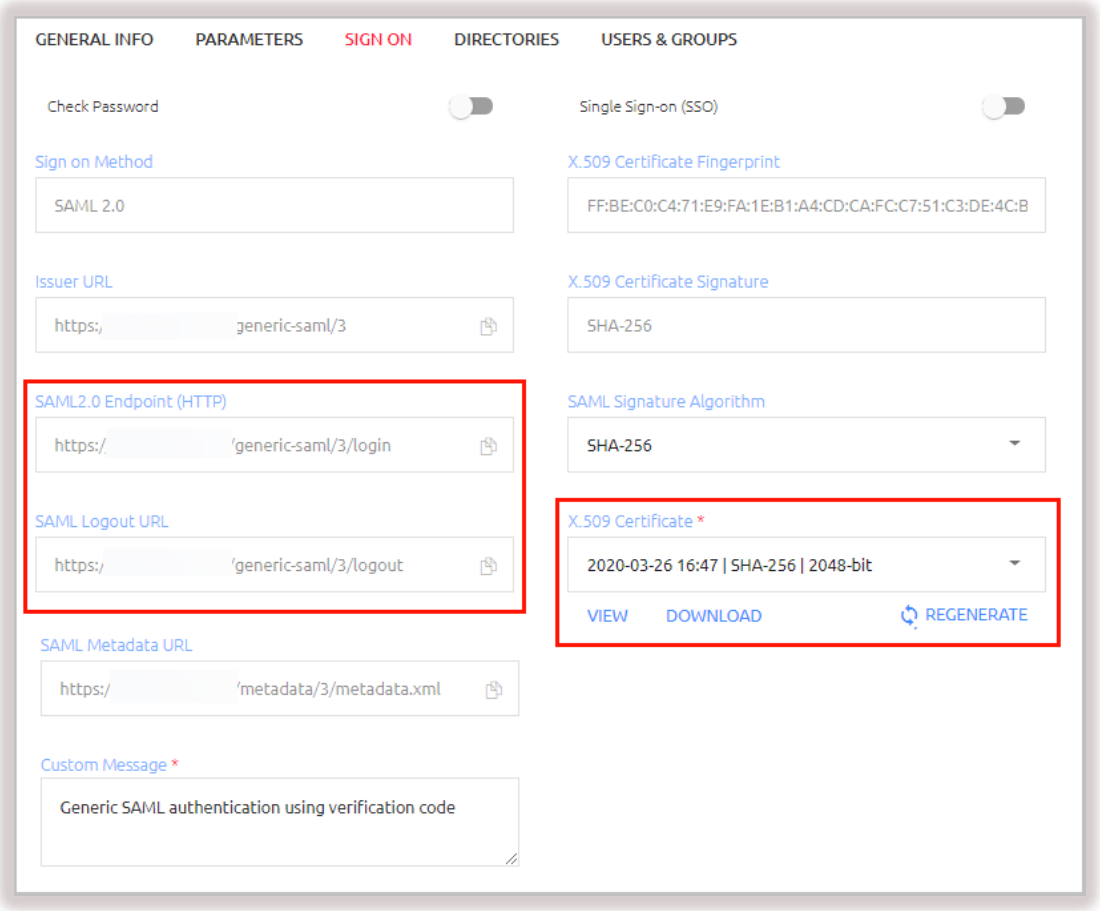
   The groups and users you selected are listed in the **Users & Groups** tab.
10. Click **Save** and then publish your changes.

Configuring the Idaptive Identity Provider Setup

The following procedure explains how to configure Partner Management settings in your Idaptive Admin account to support integration with the Octopus Authenticator.

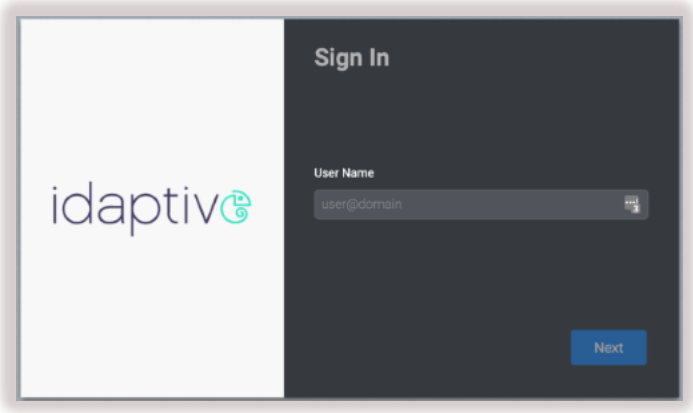
Before you begin, make sure that you have access to the following elements. They can be copied or downloaded from the **Sign On** tab of the Idaptive SAML service that you created in the Octopus Management Console.

- **SAML2.0 Endpoint (HTTP):** Click the Copy icon to copy the URL.
- **SAML Logout URL:** Click the Copy icon to copy the URL.
- **X.509 Certificate:** Click **Download** to download the **cert.pem** file.

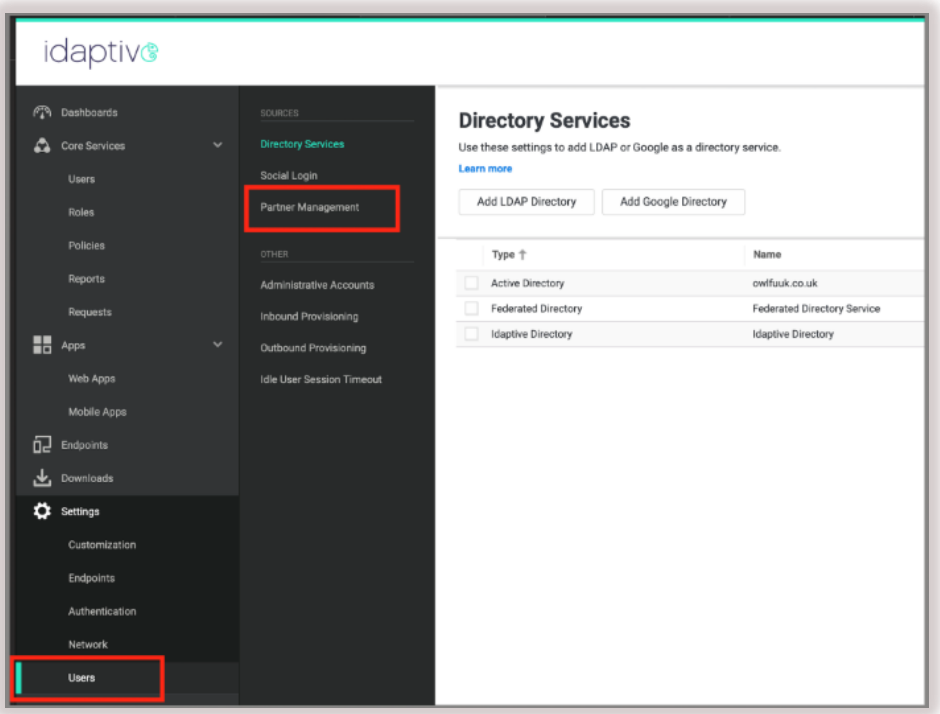


To configure the Idaptive IdP setup:

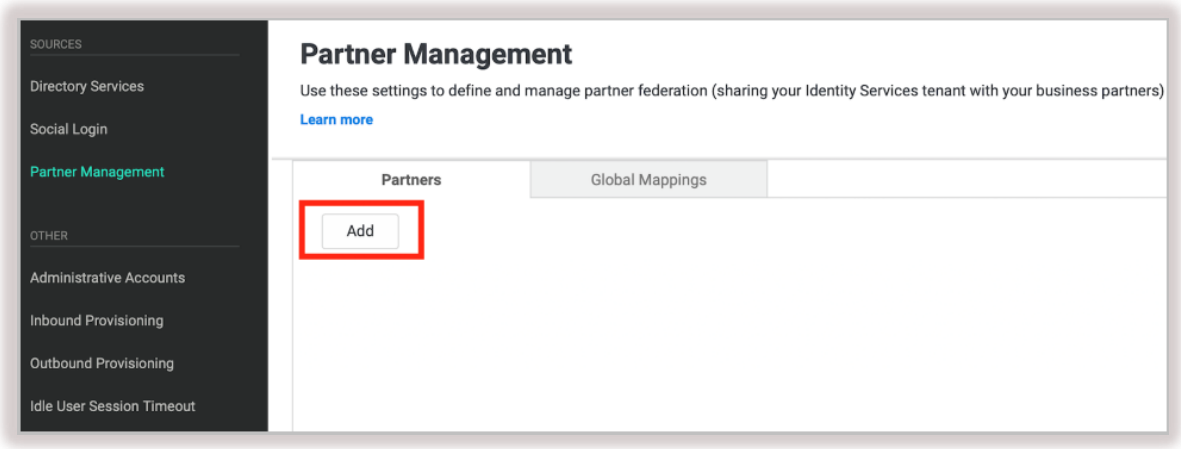
1. Log into your Idaptive Admin account.



2. From the **Admin** menu, navigate to **Settings > Users > Partner Management**.

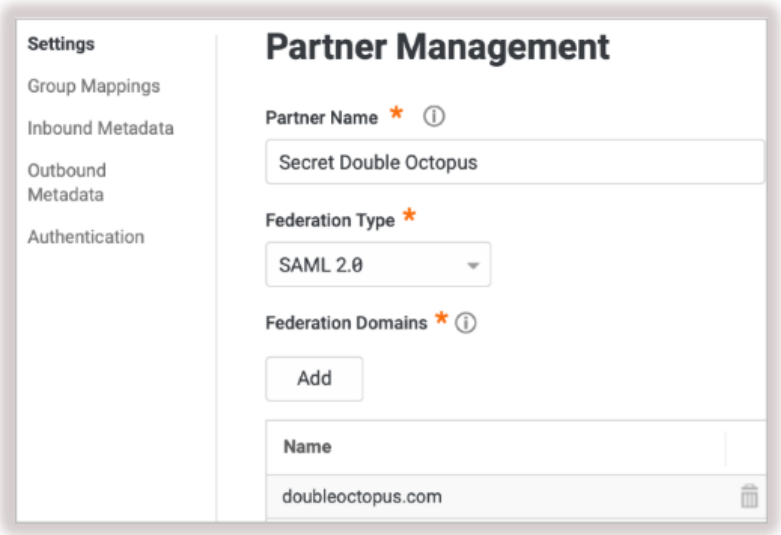


3. On the **Partner Management** page, click **Add**.

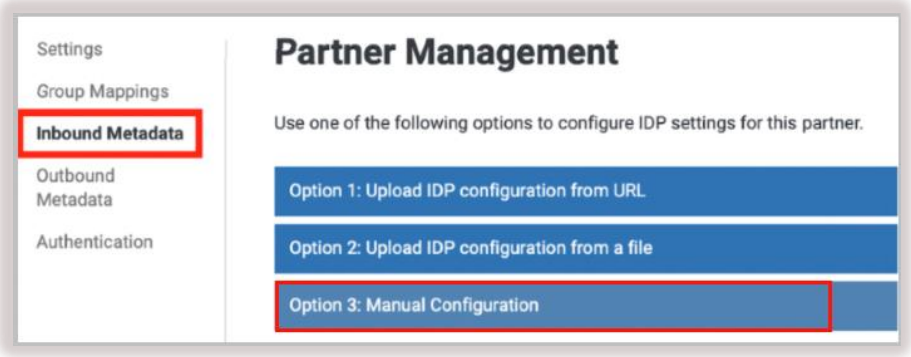


4. Configure the following settings on the **Settings** tab:

Setting	Value / Notes
Partner Name	Secret Double Octopus
Federation Type	Select **SAML 2.0**
Federation Domains	Company domain name, e.g., *doubleoctopus.com*, *acme. com*

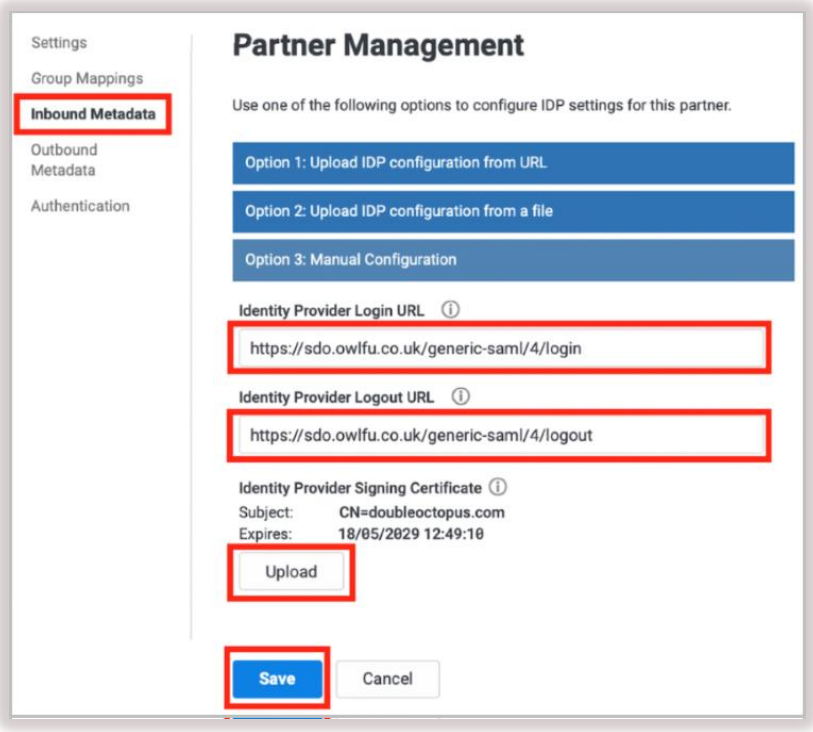


5. Click **Inbound Metadata** and select **Option 3: Manual Configuration**.



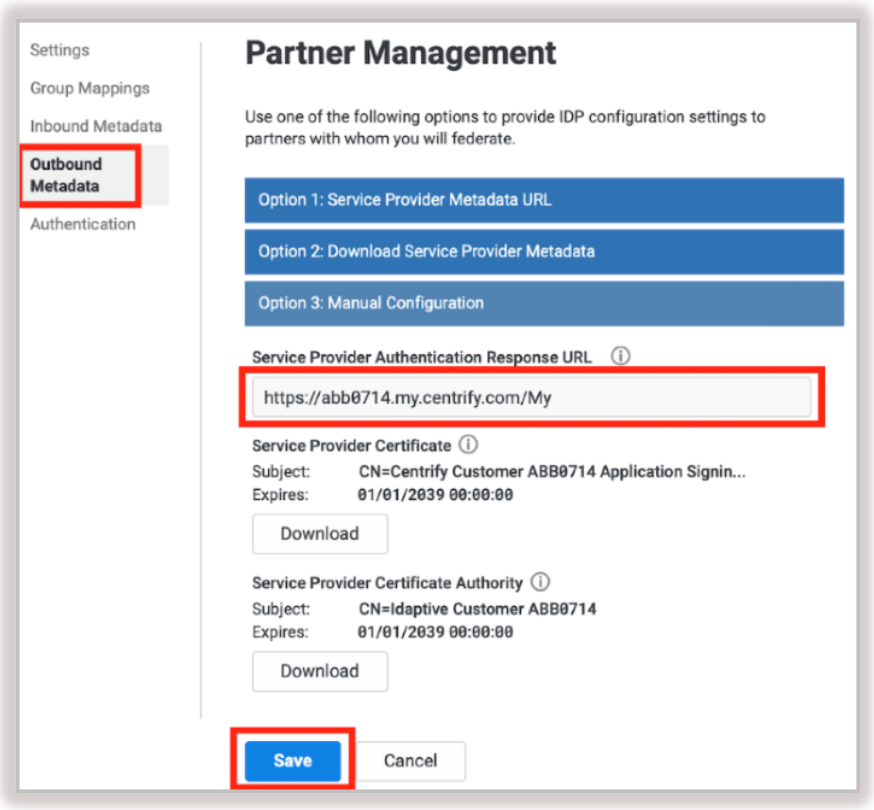
6. Configure the following settings:

Setting	Value / Notes
Identity Provider Login URL	Paste the **SAML 2.0 Endpoint** URL (from the Idaptive SAML service in the Octopus Management Console) in the field.
Identity Provider Logout URL	Paste the **SAML Logout URL** in the field.
Identity Provider Signing Certificate	Upload the X.509 certificate file that you downloaded from the Idaptive SAML service in the Octopus Management Console.



7. Click **Save**.

8. Click **Outbound Metadata**, and verify that the **Service Provider Authentication Response URL** has been generated.



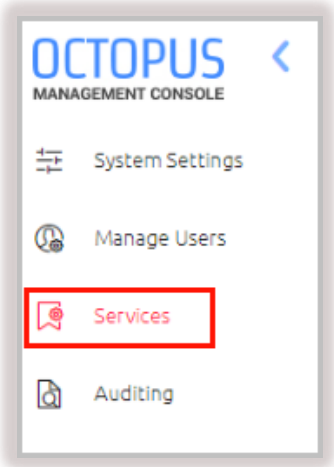
   Make note of this value, as you will need it for the last phase of service integration (Completing Service Integration).
9. Click **Save**.

Completing Service Integration

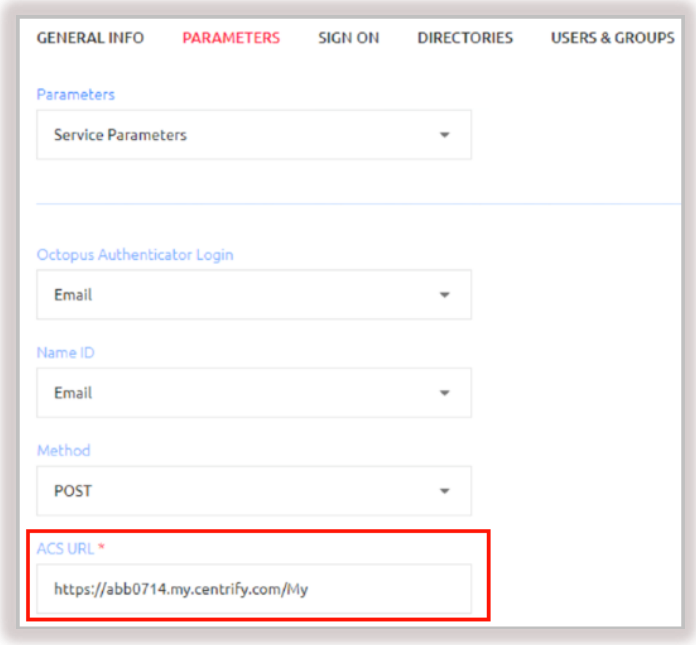
To complete the integration process, you need to configure the Octopus Authenticator Idaptive service with the correct Authentication Response URL from your Idaptive Admin account.

To complete service integration:

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



2. In the tile of the AWS SAML service, click ✎ to display the service settings.
3. Open the **Parameters** tab. Then, copy the Service Provider Authentication Response URL from your Idaptive Admin account, and paste it in the **ACS URL** field.



4. At the bottom of the **Parameters** tab, click **Save** and then publish your changes.