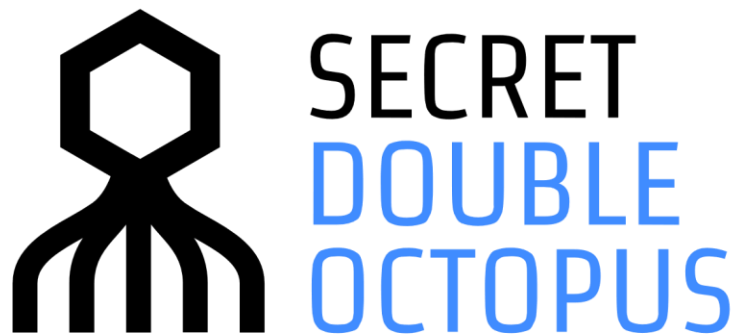


MAY 26, 2020



How to Configure Octopus Authentication for Box Web Service

CONTENTS

Introduction	3
Creating the Box SAML Service	4
Configuring the Box 3 rd Party IdP Setup.....	10
Completing SSO Activation	12

Introduction

This document describes the configurations required for SAML 2.0 integration between the Octopus Authenticator and Box Web Service.

The integration process involves the following sequential phases:

- Creating the Box SAML Service
- Configuring the Box 3rd Party IdP Setup
- Completing SSO Activation

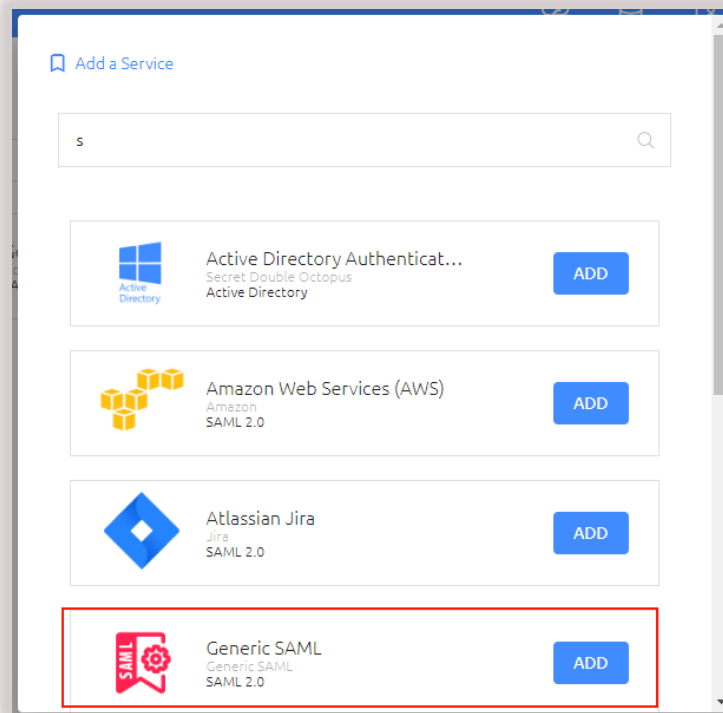
Note: Setting up this integration requires collaboration with the Box Support team. For details, refer to Configuring the Box 3rd Party IdP Setup on page 10.

Creating the Box SAML Service

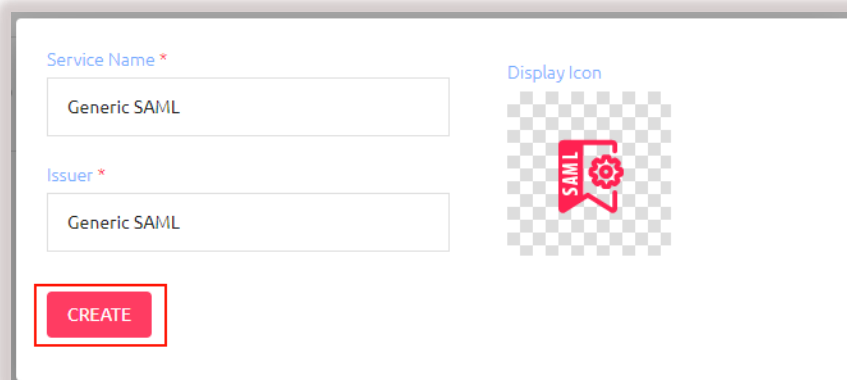
The following procedure explains how to create the required SAML service in the Octopus Management Console.

To add and configure the Box 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**.



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

Setting	Description
Service Name	Box
Issuer	Box
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>

The screenshot shows the configuration page for the 'box' service. The 'GENERAL INFO' tab is selected. The 'Service Name' and 'Issuer' fields are both set to 'box'. The 'Description' field is empty. The 'Display Icon' field shows a blue 'box' logo. The 'Login Page URL' field is set to 'https://oct.doubleoctopus.com/generic-saml/117/log'. A 'SAVE' button is located at the bottom left of the form.

Then, click **Save**.

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

Setting	Value / Notes
Octopus Authentication Login	The login method for the Octopus Authenticator Server.
Name ID	The Box login method. Select Email .
Method	Select POST .
ACS URL	https://sso.services.box.net/sp/ACS.saml2
Audience	box.net
SSO URL	https://<your box subdomain>.account.box.com/

4. At the bottom of the **Parameters** tab, click **Add Parameter** and create a new **Email** parameter. Then, click **Save**.

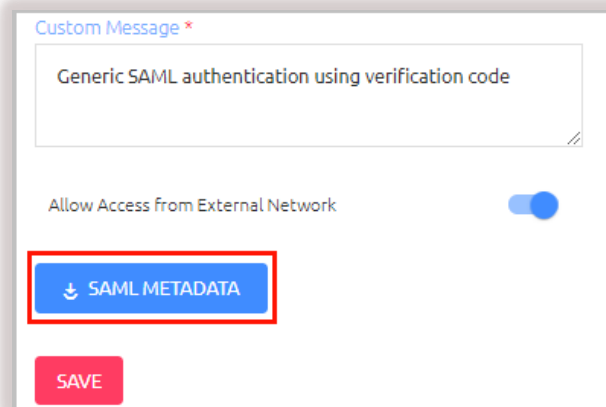
- Open the **Sign On** tab and configure the following settings. We recommend not to change default values.

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 Box Web Service
Custom Message	The message displayed to the user upon successful login

The screenshot displays the 'SIGN ON' configuration page with the following settings:

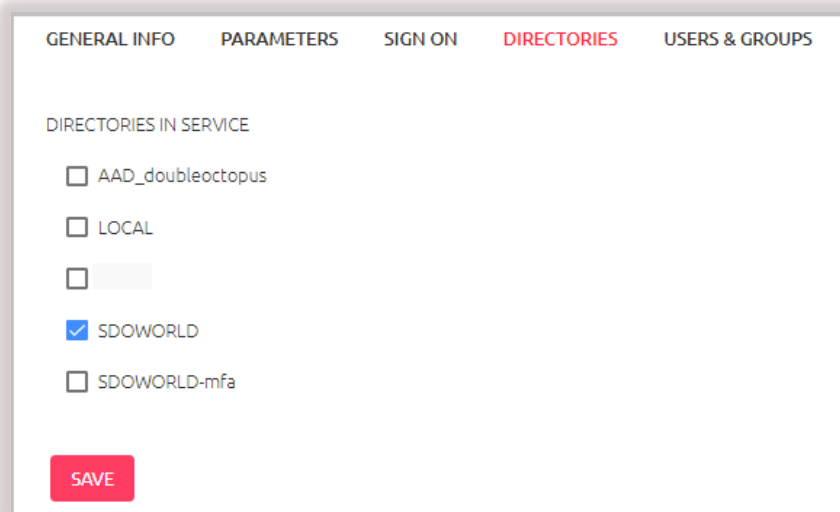
- Check Password:** Disabled (toggle)
- Single Sign-on (SSO):** Disabled (toggle)
- Sign on Method:** SAML 2.0
- Issuer URL:** https://oct.doubleoctopus.com/generic-saml/117
- SAML 2.0 Endpoint (HTTP):** https://oct.doubleoctopus.com/generic-saml/117/log
- SAML Logout URL:** https://oct.doubleoctopus.com/generic-saml/117/log
- SAML Metadata URL:** https://oct.doubleoctopus.com/metadata/117/metac
- Custom Message *:** Generic SAML authentication using verification code
- X.509 Certificate Fingerprint:** 5E:4C:33:34:0E:C7:60:D8:F0:60:41:4A:17:96:3C:15:C7:7C:E9
- X.509 Certificate Signature:** SHA-256
- SAML Signature Algorithm:** SHA-256
- X.509 Certificate *:** 2020-04-12 14:41 | SHA-256 | 2048-bit

- At the bottom of the **Sign On** tab, click **SAML METADATA**.

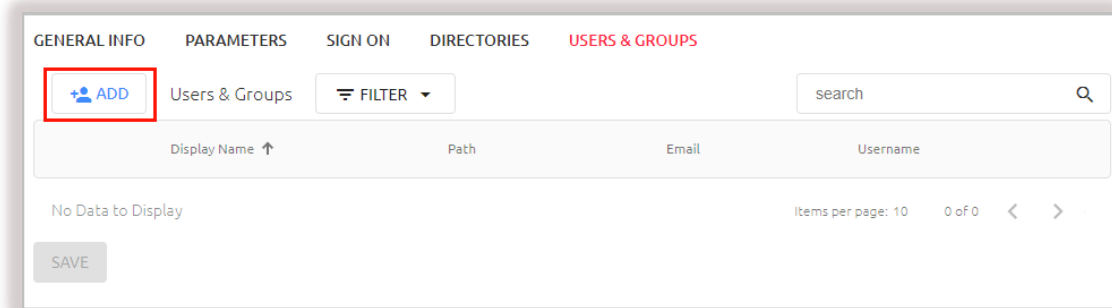


This displays all data configured for the service in XML format. Save and store the XML file. You will use it later when configuring the Box 3rd party IdP.

- Click **Save**.
- Open the **Directories** tab and select the checkbox of the directory to be integrated with the service. Then, click **Save**.



9. Open the **Users & Groups** tab and click **Add**.



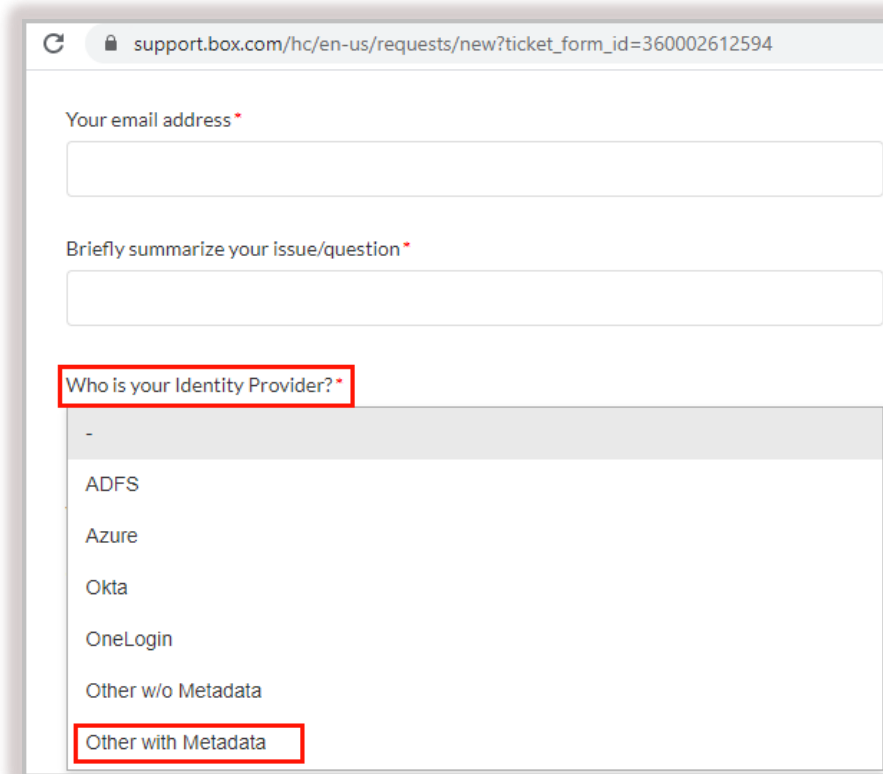
- A popup opens, with a list of directories displayed on the left.
10. Expand the relevant directory and select the checkboxes of the groups and users that you want to add to the service. Then, click **Save** to close the popup.
- The groups and users you selected are listed in the **Users & Groups** tab.
11. Click **Save** and then publish your changes.

Configuring the Box 3rd Party IdP Setup

Setting up SSO with a 3rd party IdP needs to be done through the Box Support team. Follow the steps below to complete your request.

To send a Box support ticket requesting SSO setup:

1. Go to https://support.box.com/hc/en-us/requests/new?ticket_form_id=360002612594
2. For **Identity Provider**, select **Other with Metadata**.



The screenshot shows a web browser window with the URL `support.box.com/hc/en-us/requests/new?ticket_form_id=360002612594`. The form contains the following fields:

- Your email address ***: A text input field.
- Briefly summarize your issue/question ***: A text area.
- Who is your Identity Provider? ***: A dropdown menu with the following options:
 -
 - ADFS
 - Azure
 - Okta
 - OneLogin
 - Other w/o Metadata
 - Other with Metadata** (highlighted with a red box)

3. Complete the following fields with the values listed in the table below:

Field	Value / Attribute
Box Subdomain	Your Box subdomain
User's email	email
User's first name	firstName
User's last name	lastName

Box.Subdomain *

Ex. acme.box.com

What is the attribute for the user's email? *

Ex. "SAML_SUBJECT" "emailaddress"

What is the attribute for groups?

If using groups, include the attribute here

What is the attribute for the user's first name?

Ex. "firstName", "givenname"

What is the attribute for the user's last name?

Ex. "lastName", "surname"

4. Under **Attachments**, upload the Metadata XML file that you downloaded from the SAML service in the Octopus Management Console.

Attachments *

Add file or drop files here

Submit

5. Click **Submit**.

When you receive a response from Box Support, follow the instructions given. Afterwards, make sure that you can login using Octopus Authenticator.

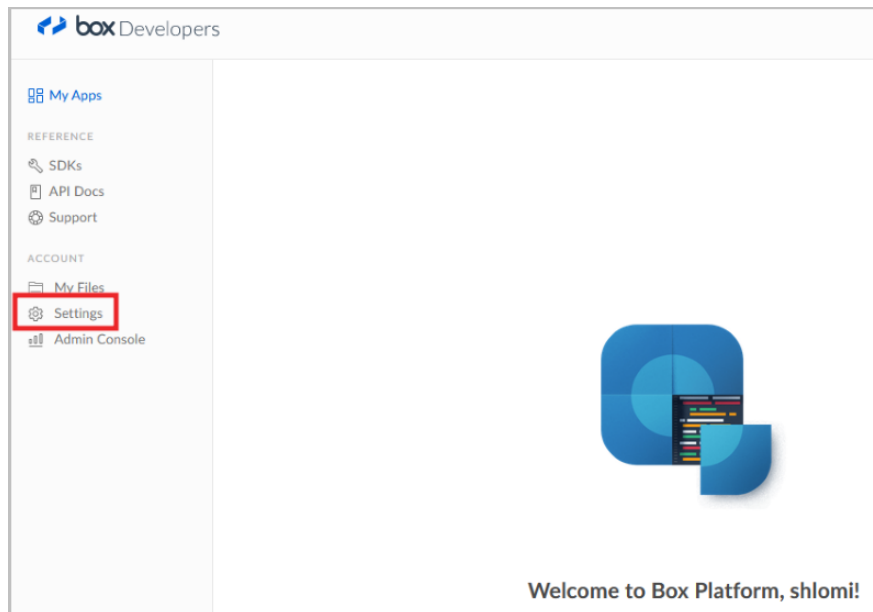
Once you have verified that you can sign in and out of Box successfully using SSO, you are ready to complete the SSO activation, as described in the next section.

Completing SSO Activation

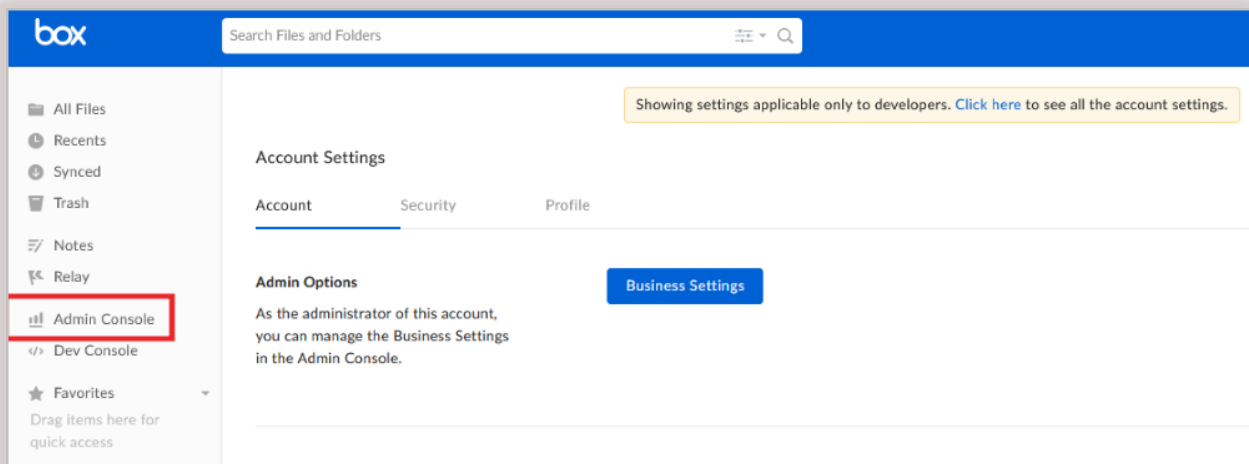
The procedure below describes how you can completely secure your account by making SSO required for all users. Once you make this change in your Box Admin account, users will no longer be able to log in using their Box credentials.

To complete SSO activation:

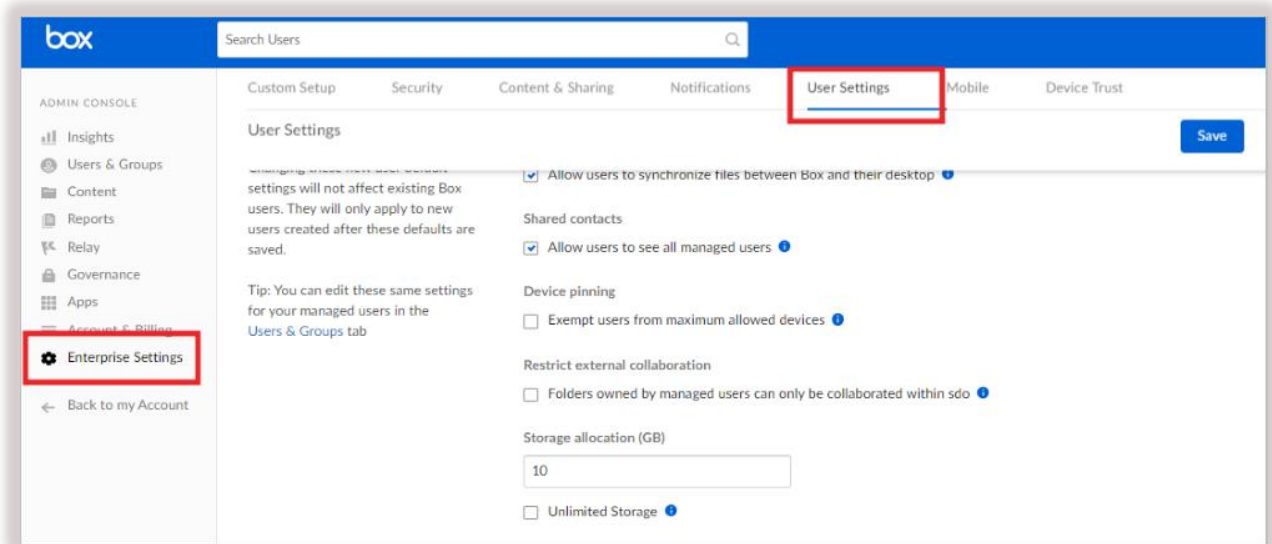
1. Log into your Box Admin account. Under **ACCOUNT**, select **Settings**.



2. On the **Account Settings** page, select **Admin Console**.



3. Navigate to **Enterprise Settings > User Settings**.



4. Scroll to the **Configure Single Sign On (SSO) for All Users** section and enable the **SSO Required** toggle button.

