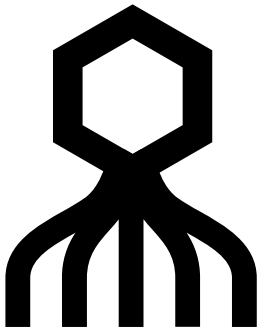
MAY 6, 2021



SECRET DOUBLE OCTOPUS

How to Configure Octopus Authentication for Citrix Workspace

VERSION 4.8.4

CONTENTS

Introduction

This document describes the configurations required for SAML 2.0 integration between the Octopus Authenticator and Citrix Workspace.

Integration Environment

The environment used for the integration described in this document is based on the following software versions:

- Octopus Authentication Server version 4.8.4
- Citrix Workspace via Citrix cloud

Prerequisites

Before beginning the integration process, make sure that you have access to a **unique enterprise certificate**. The certificate can usually be downloaded from the Enterprise Root Certificate Authority server of your organization.

Integration Workflow

The integration process involves the following sequential phases:

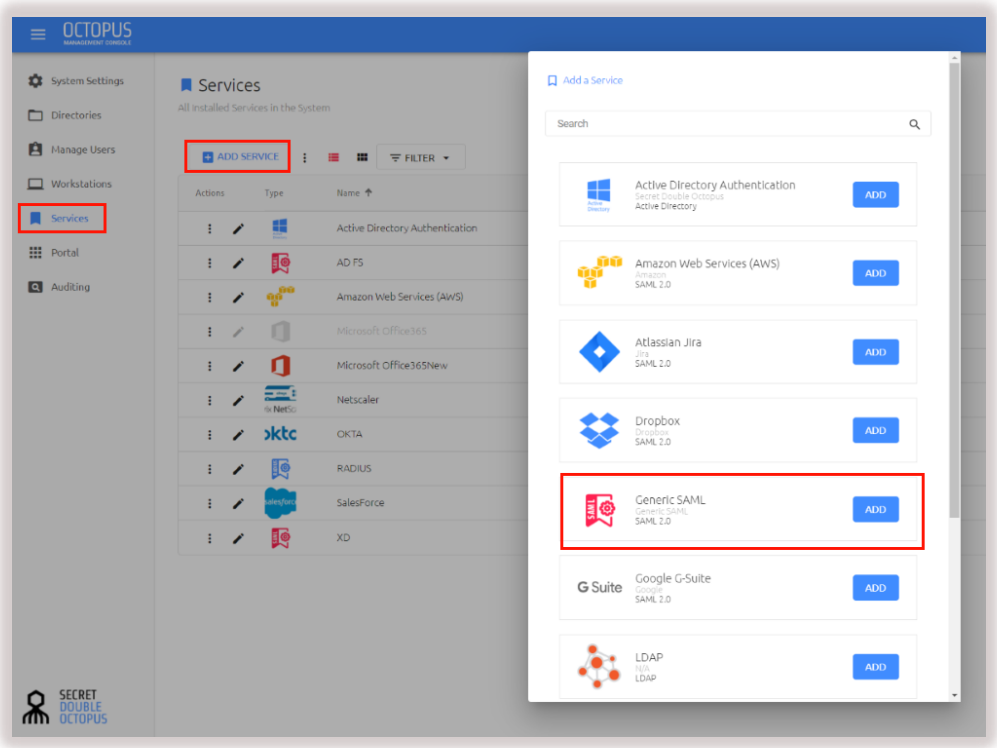
- Creating the Citrix SAML Service: Add and configure the required SAML service in the Octopus Management Console
- Configuring Citrix Workspace: Configure SAML authentication settings in your Citrix Workspace environment
- Running the Solution: Test the authentication flow

Creating the Citrix SAML Service

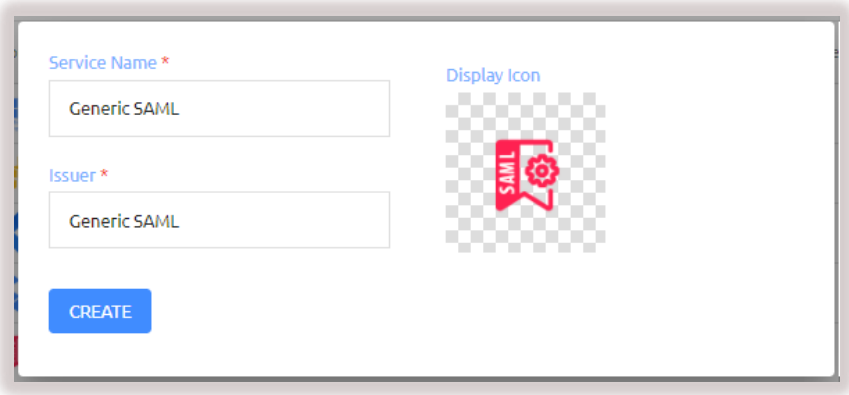
The following procedure explains how to create the required SAML service in the Octopus Management Console. The service settings will be used later in the Citrix Workspace configuration.

To add and configure the Citrix SAML service:

1. From the Octopus Management Console, open the **Services** menu. At the upper left corner of the page, click **Add Service**.
2. In the **Generic SAML** tile, click **Add**.

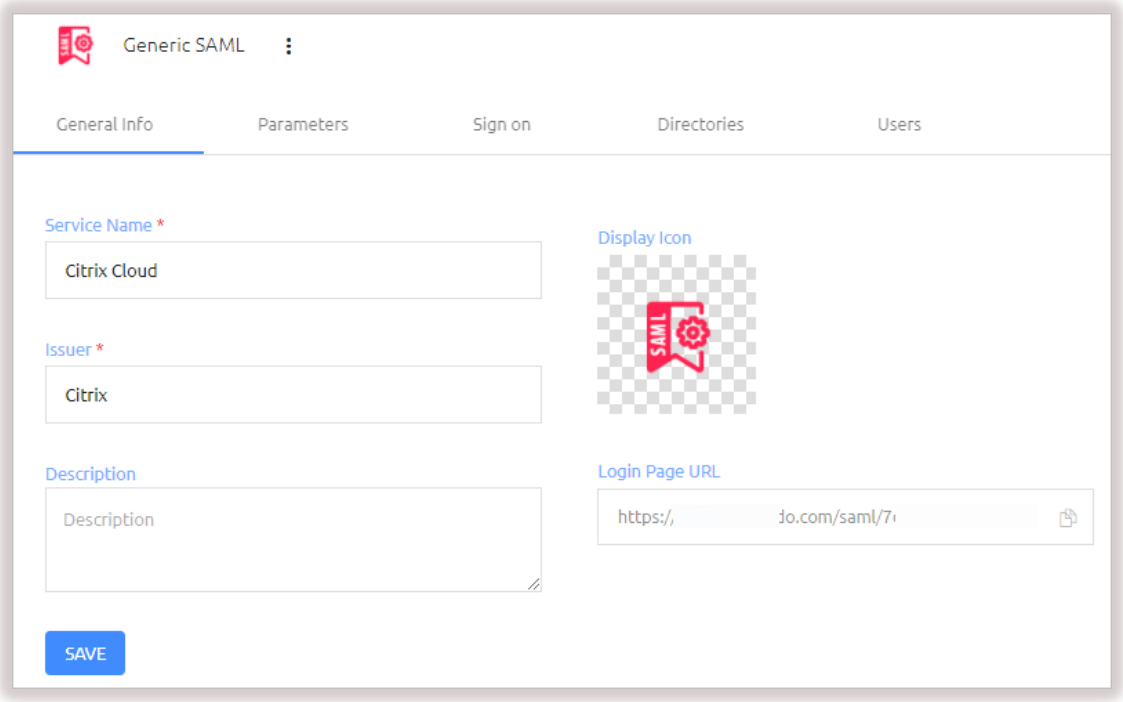


Then, in the dialog that opens, click **Create**.



3. Configure the following settings in the **General Info** tab:

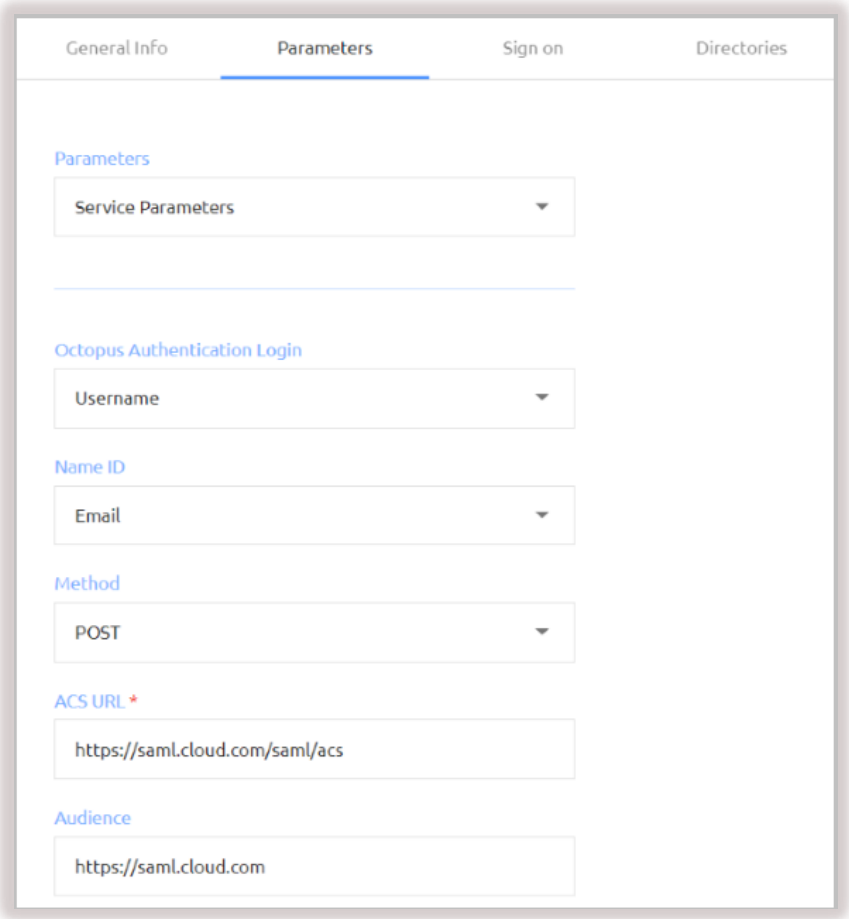
Setting	Description
Service Name	Enter a display name to identify the Service Provider (e.g., Citrix Cloud).
Issuer	Enter the issuer of the service (e.g., Citrix).
Description	Enter a brief note about the service.
Display icon	This icon will be displayed on the Login page for the service. To change the default icon, click and upload the image of your choice. (Supported image size is 488x488 pixels.)
Login Page URL	<https://<Enterprise Base URL>/generic-saml/<No.>/login> The **Enterprise Base URL** can be modified in **System Settings > General Settings**.



Then, click **Save**.

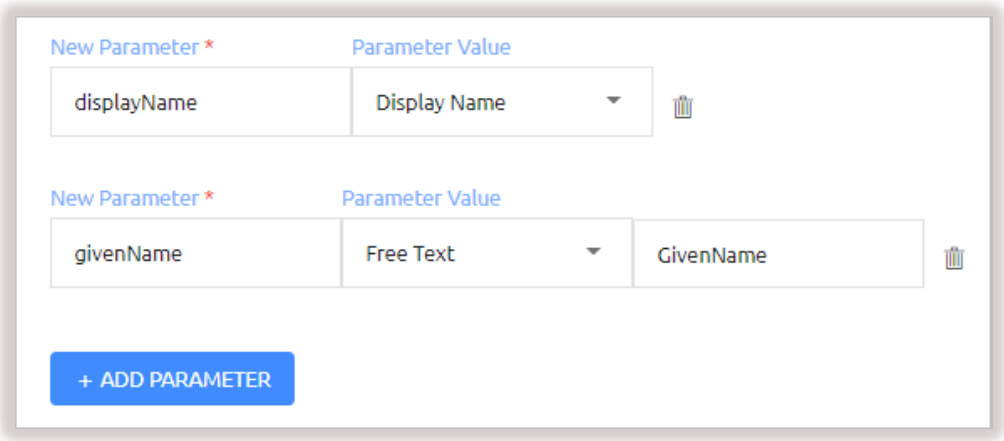
4. Open the **Parameters** tab, and configure the following settings:

Setting	Value / Notes
Octopus Authenticator Login	The identifier required for the Octopus Authentication Server.
Name ID	The parameter required for Citrix StoreFront login.
Method	POST
ASC URL	https://saml.cloud.com/saml/acs
Audience	https://saml.cloud.com



5. At the bottom of the **Parameters** tab, click **Add Parameter** and create the parameters listed in the table below.

   If the required value does not appear in the **Parameter Value** dropdown list, select **Free Text** and then enter the value in the field that appears to the right (as shown in the following example).

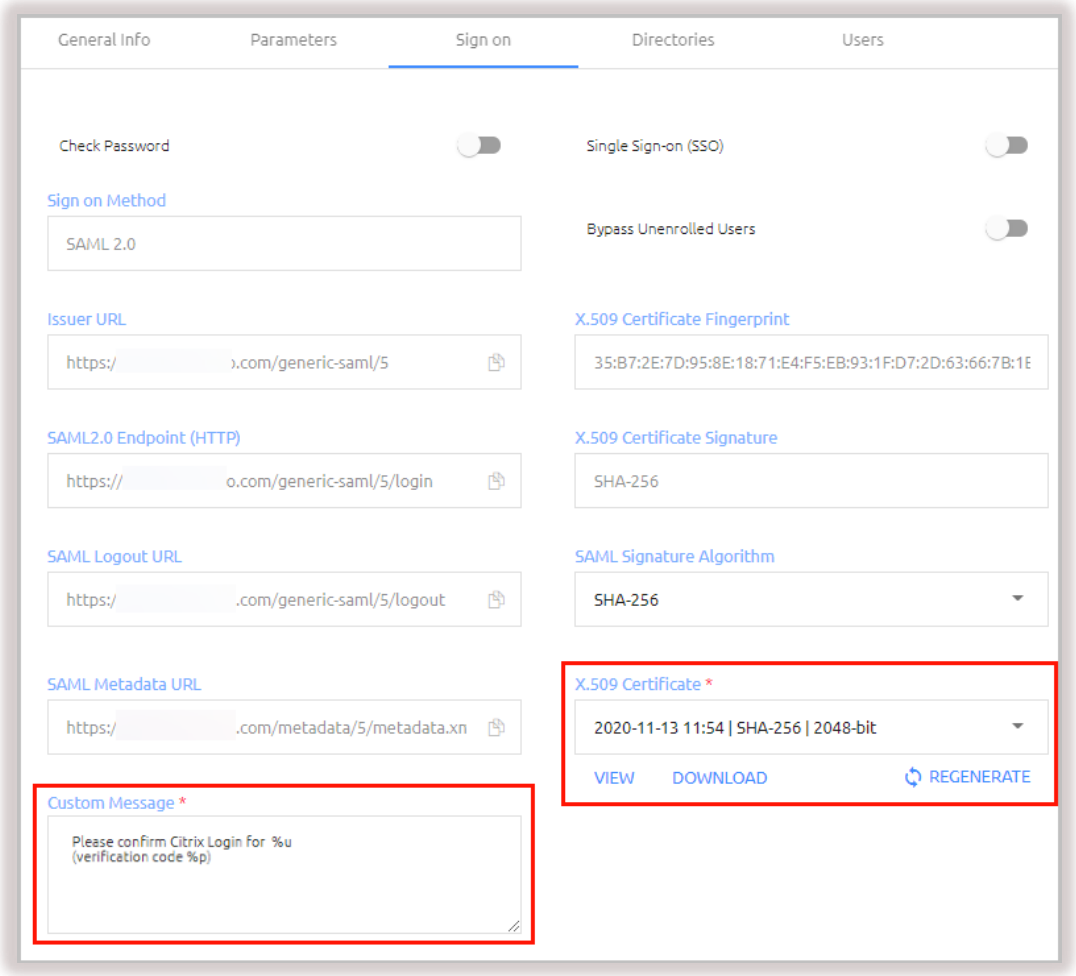


Parameter name	Parameter Value
displayName	Display Name
givenName	GivenName
familyName	Sn
cip_sid	ObjectSid
cip_upn	UserPrincipalName
cip_email	Email
cip_oid	ObjectGUID

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

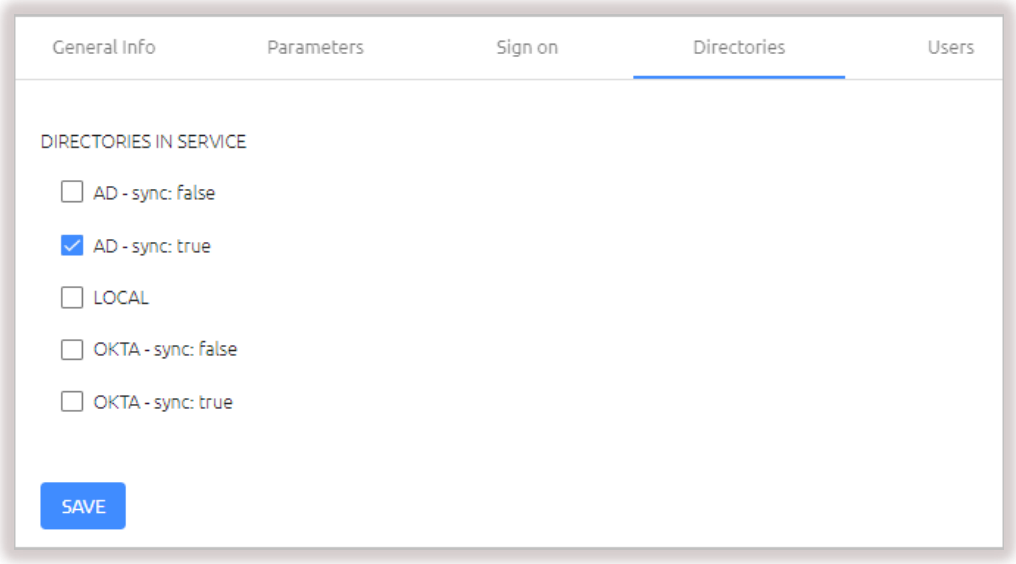
7. Open the **Sign on** tab, and update the default message in the **Custom Message** field. (This is the message displayed to the user upon successful login.)

   Then, under **X.509 Certificate**, click **Download** to download the certificate.

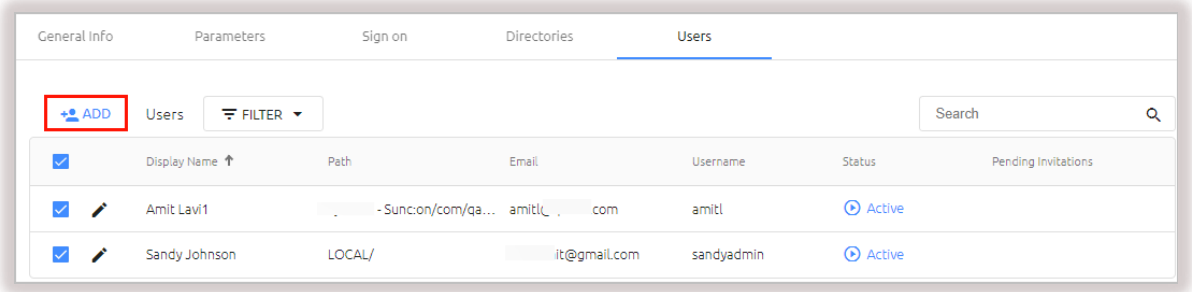


8. At the bottom of the **Sign on** tab, click **Save**.

9. Open the **Directories** tab and select the checkboxes of the directories you want to integrate with the service. Then, click **Save**.



10. Open the **Users** tab and click **Add**.



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

11. Expand the directories list and select the checkboxes of the groups and users that you want to add to the service. Then, click **Save** to close the popup.

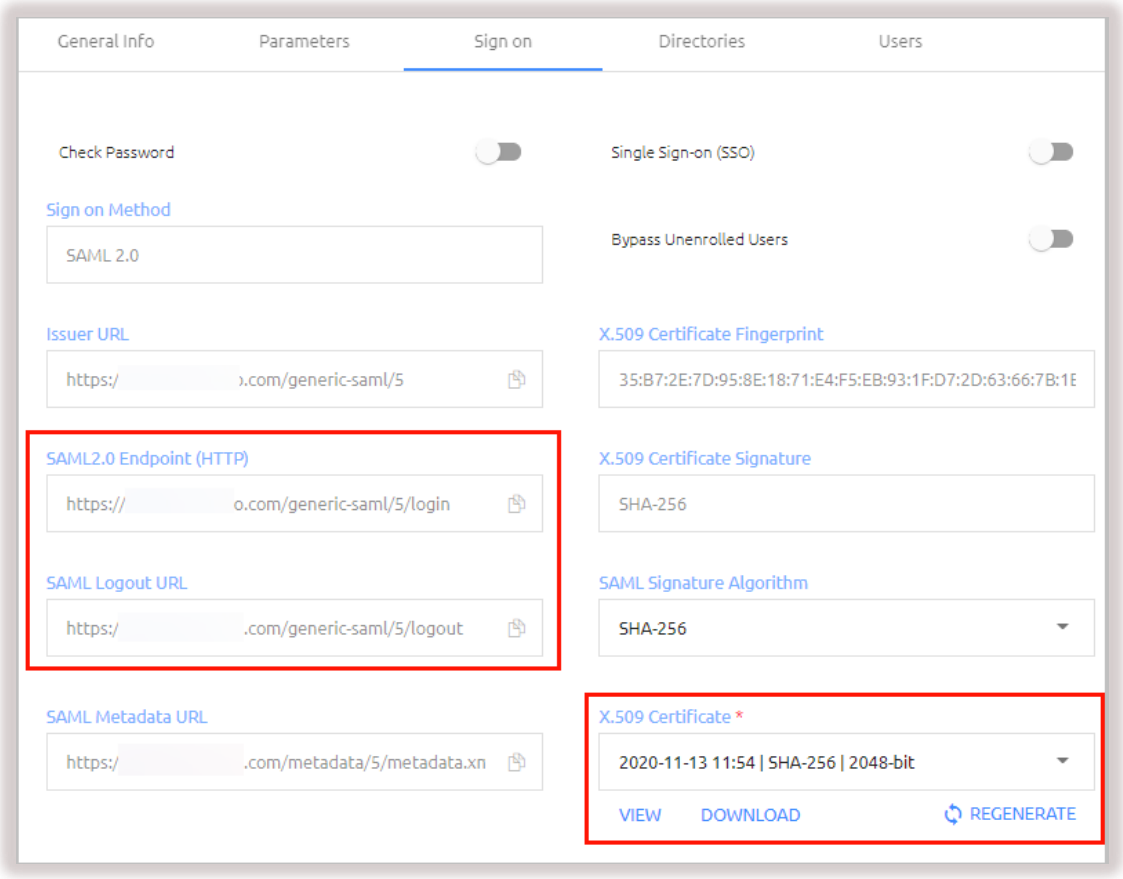
    The groups and users you selected are listed in the **Users** tab.

12. At the bottom of the **Users** tab, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

Configuring Citrix Workspace

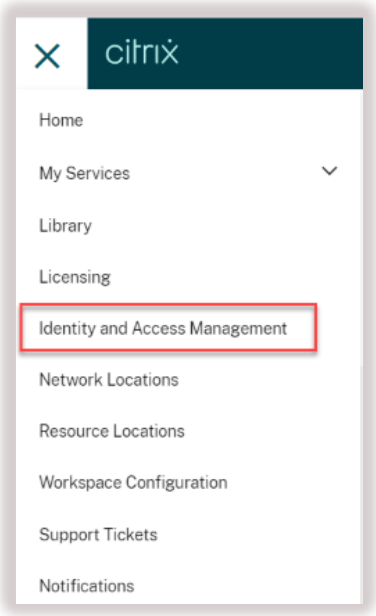
The procedure below explains how to set up SAML authentication in Citrix Workspace with Secret Double Octopus integration. Before you start, make sure you have access to the **SAML2.0 Endpoint (HTTP)** URL and the **SAML Logout URL** of the Octopus SAML service. You can copy the values from the **Sign on** tab by clicking the Copy icons.

In addition, verify that you have downloaded the X.509 certificate.

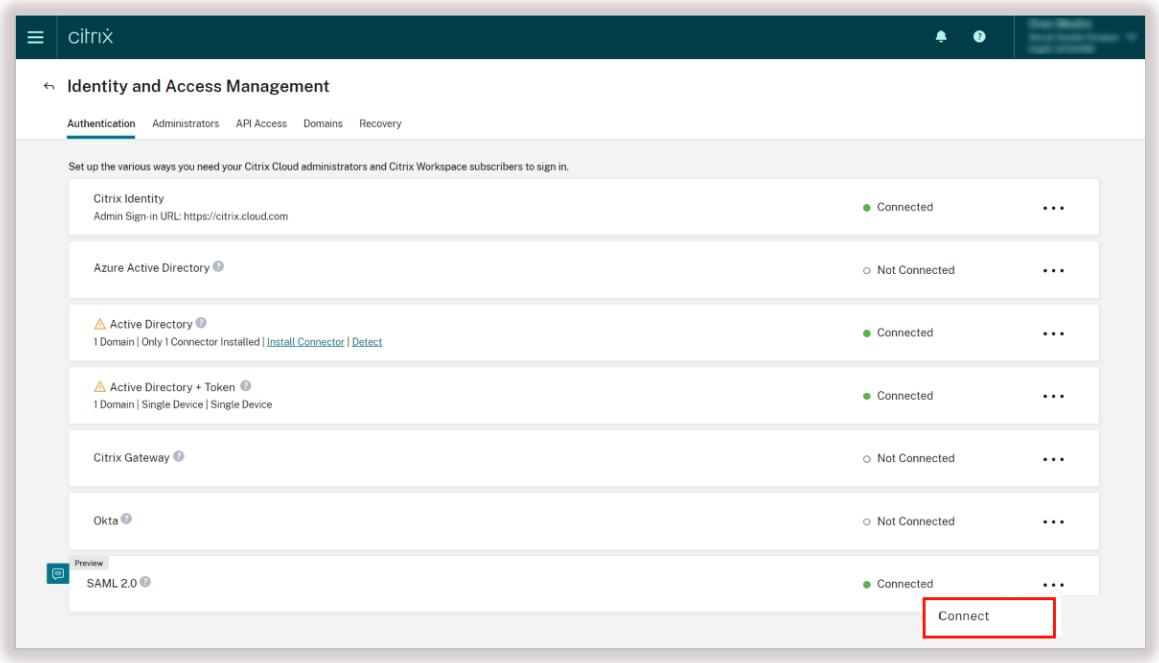


To configure SAML authentication in Citrix Workspace:

1. From the navigation menu of Citrix Workspace, select **Identity and Access Management**.



2. On the page that opens, in the **SAML 2.0** row, click **Connect**.

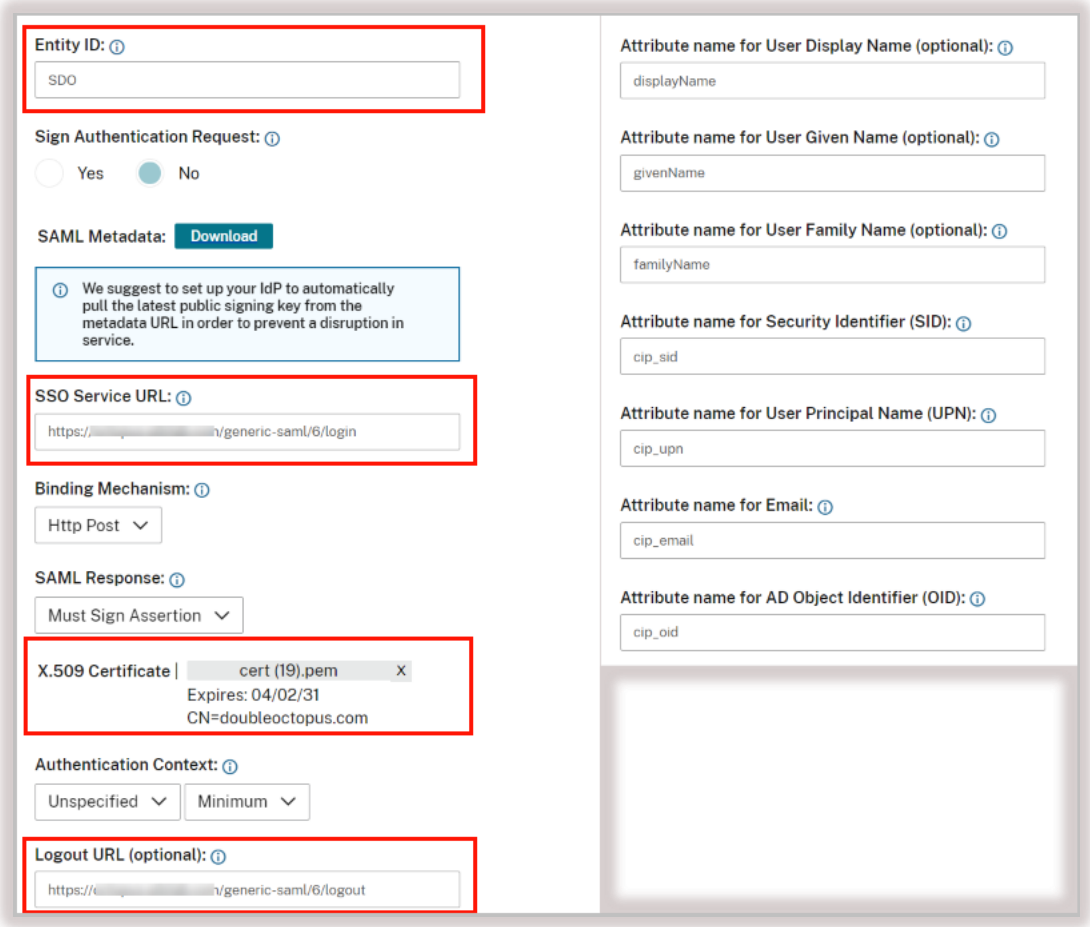


The **SAML Configuration** dialog opens.

3. Configure the following settings:

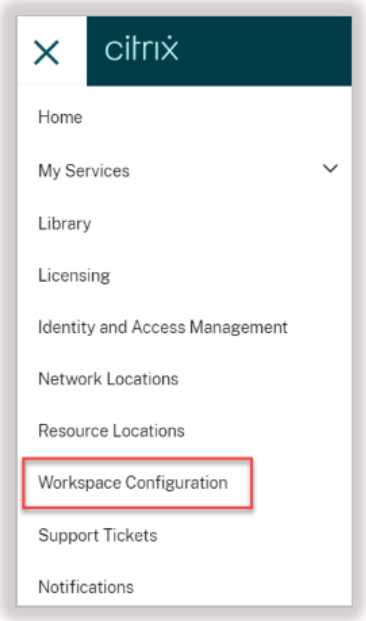
Setting	Value / Notes
Entity ID	Enter a name for the SAML service you created (e.g., SDO).
SSO Service URL	Paste the **SAML2.0 Endpoint (HTTP)** URL of the Octopus service.
Logout URL	Paste the **SAML Logout URL** of the Octopus service.

Then, under **X.509 Certificate**, import the service certificate.

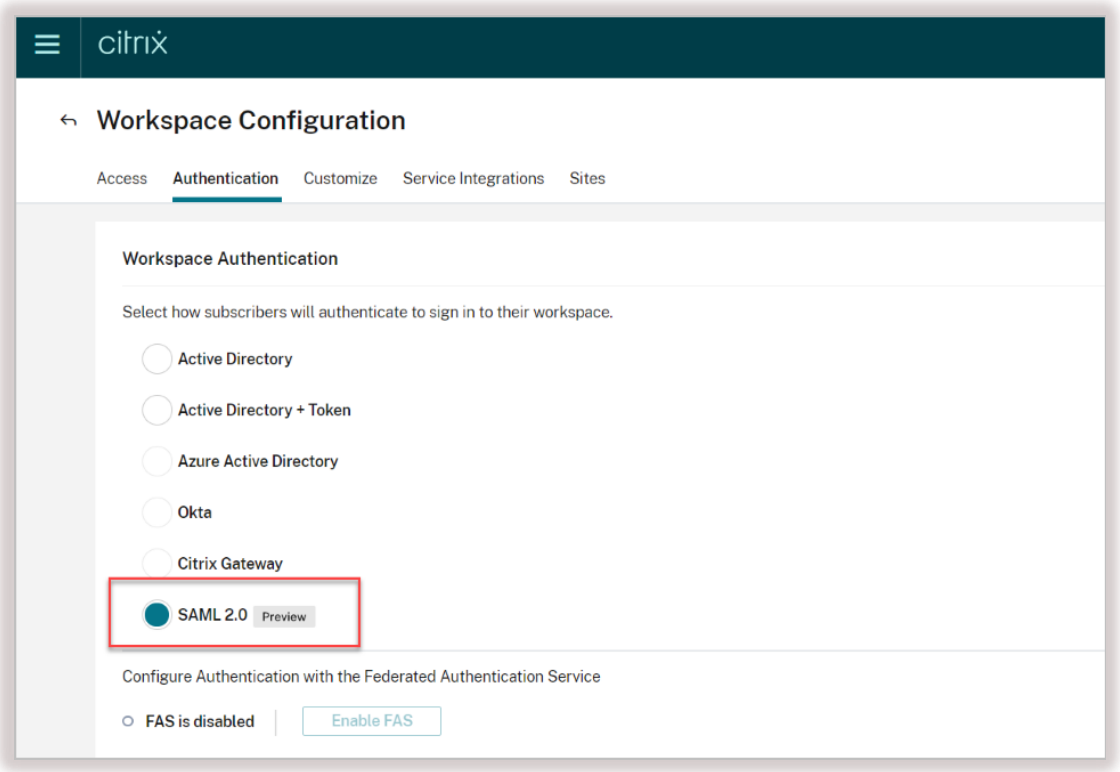


4. To save your changes, click **OK**.

5. From the navigation menu of Citrix Workspace, select **Workspace Configuration**.



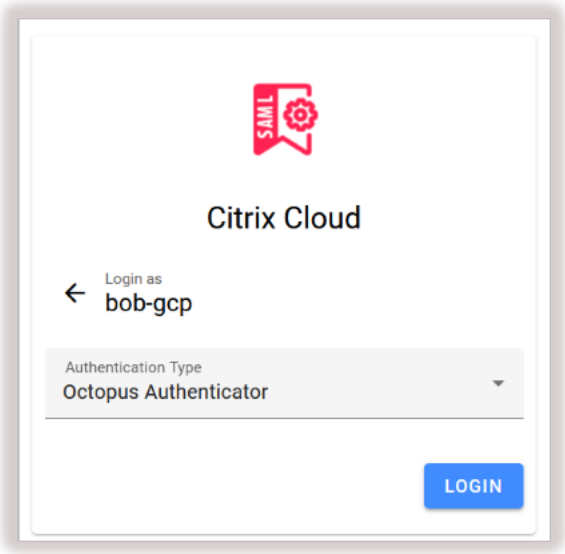
6. On the page that opens, open the **Authentication** tab and select the **SAML 2.0** radio button.



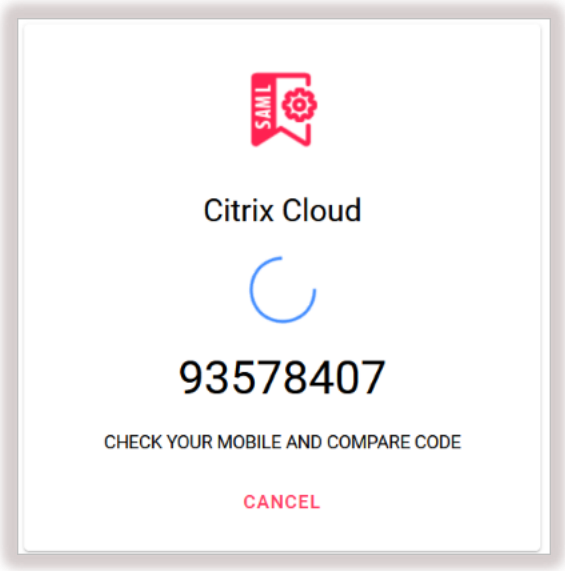
Running the Solution

This section describes the user experience of logging into Citrix Workspace via the Octopus Authenticator. The authentication process is as follows:

1. From a browser, the user opens the FQDN of the Citrix Cloudspace. The user is then redirected to the Secret Double Octopus authentication page.
2. The user enters a username and clicks **Login**.

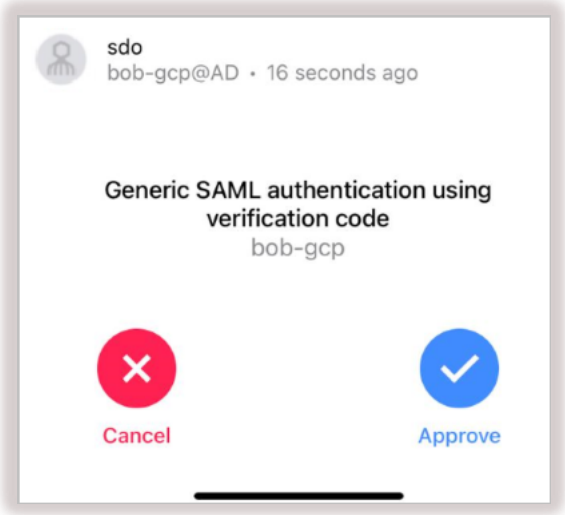


A verification code is generated and displayed on the webpage.

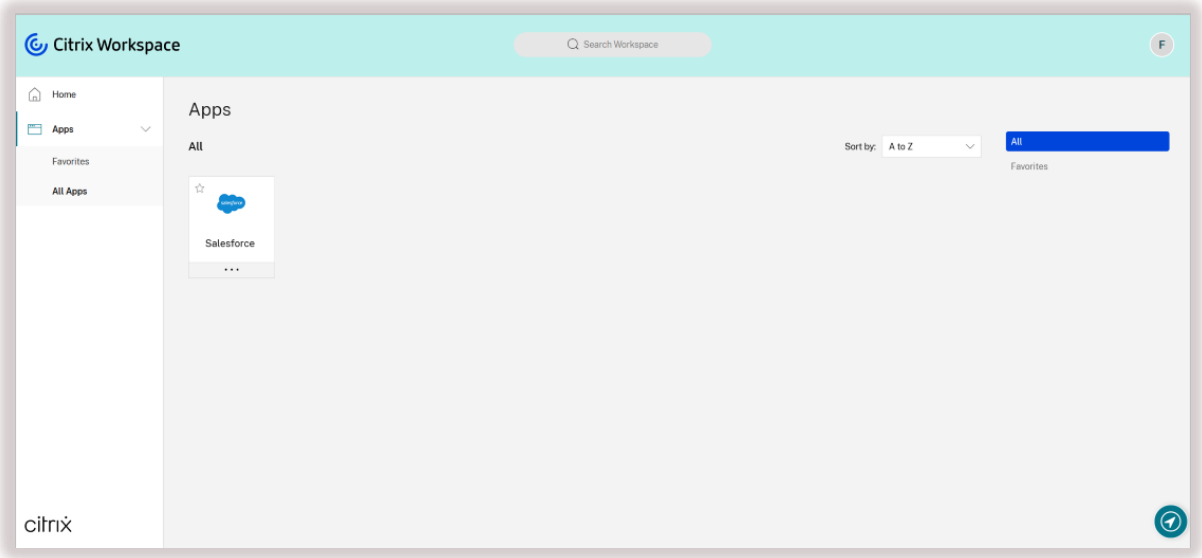


A notification with this number then appears on the user's Octopus Mobile App, asking for authentication approval.

3. The user taps **Approve**.



After successful authentication, the user is logged into Citrix Workspace.



Contacting Support

For any questions, issues or additional assistance, please do not hesitate to reach out to the Secret Double Octopus support team by:

- Visiting our Support Website
- Contacting your Sales Engineer
- Sending an email to support@doubleoctopus.com