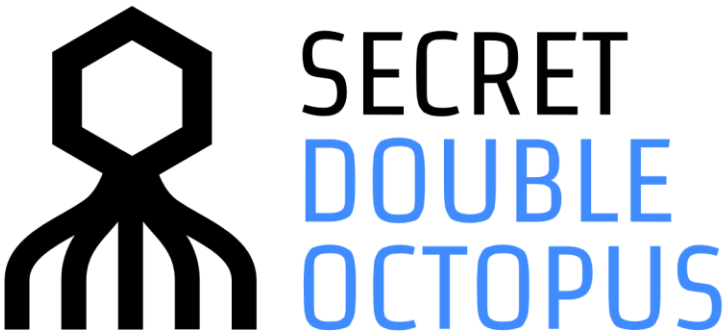
MARCH 29, 2020



How to Configure Octopus Authentication for Citrix NetScaler Gateway

CONTENTS

Introduction

This document describes the configurations required for SAML 2.0 integration between the Octopus Authenticator and Citrix NetScaler. The documentation is based on the following software versions:

- Octopus Authentication Server version 4.4.1
- Citrix NetScaler Gateway version 12.0

Prerequisites

Communication between the 3rd party Identity Provider and the Service Provider in the SAML protocol is signed with a certificate. Since the certificate should be unique to the organization, it needs to be downloaded from the service that you will create in the Octopus Management Console. Step-by-step instructions for doing so are provided in this document.

Important: When authentication for Citrix NetScaler is forwarded to Citrix XenApp/XenDesktop, the Citrix StoreFront must be set to **Pass-through from NetScaler Gateway** and the Citrix Federated Authentication Service (FAS) needs to be installed.

Integration Workflow

The integration process involves the following sequential phases:

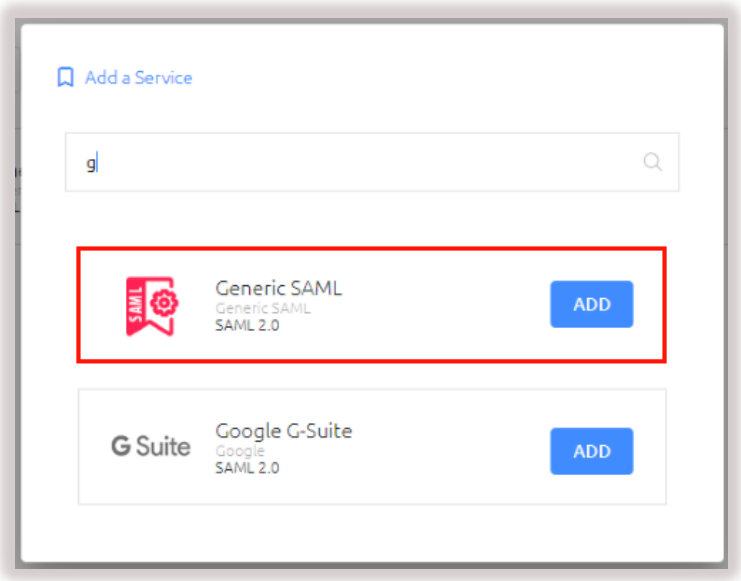
- Creating the Citrix SAML Service
- Configuring the Citrix NetScaler Gateway
- Completing Service Integration
- Running the Solution

Creating the Citrix SAML Service

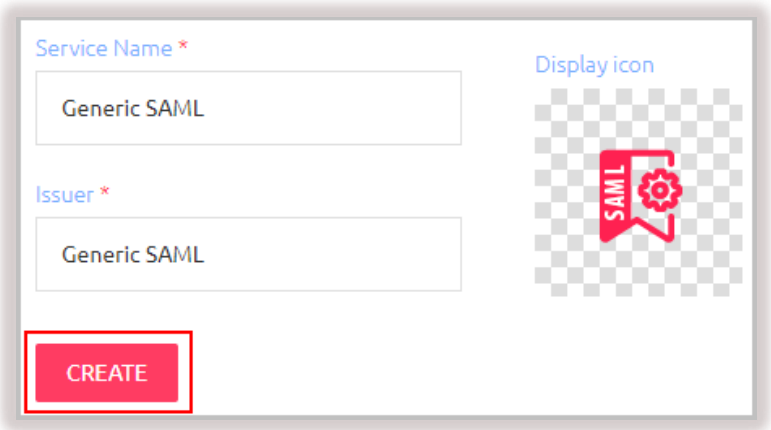
The following procedure explains how to create the required SAML service in the Octopus Management Console. The service settings will be used later in the Citrix NetScaler Gateway configuration.

To add and configure the Citrix SAML service:

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

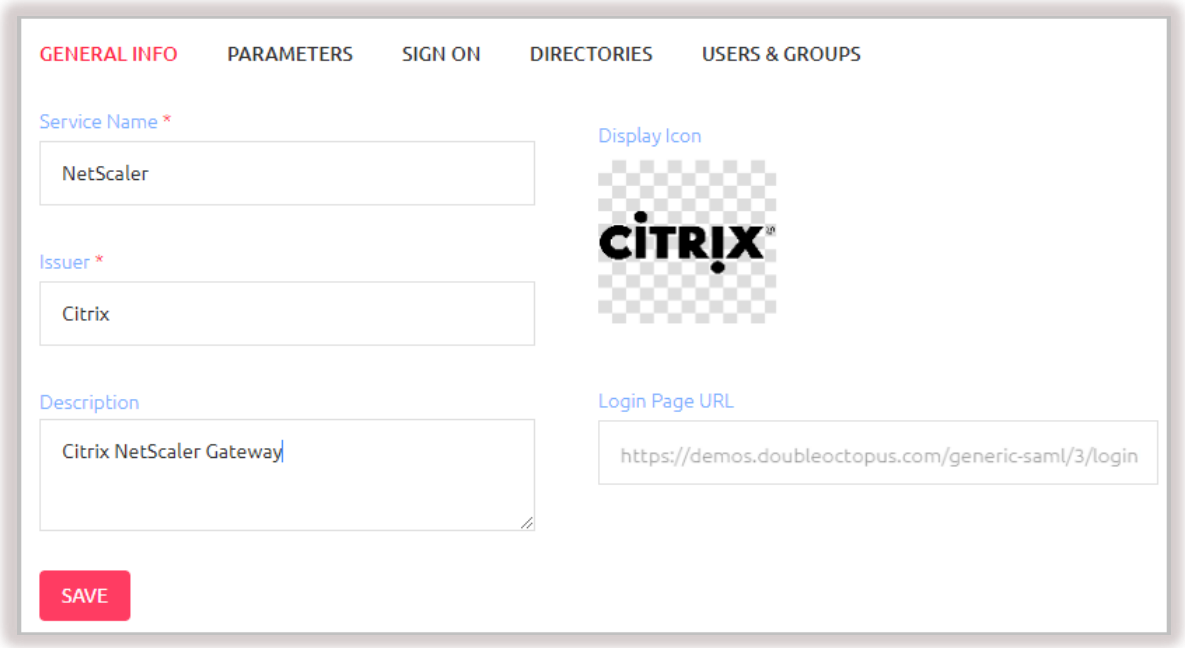


Then, in the dialog that opens, click **Create**.



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

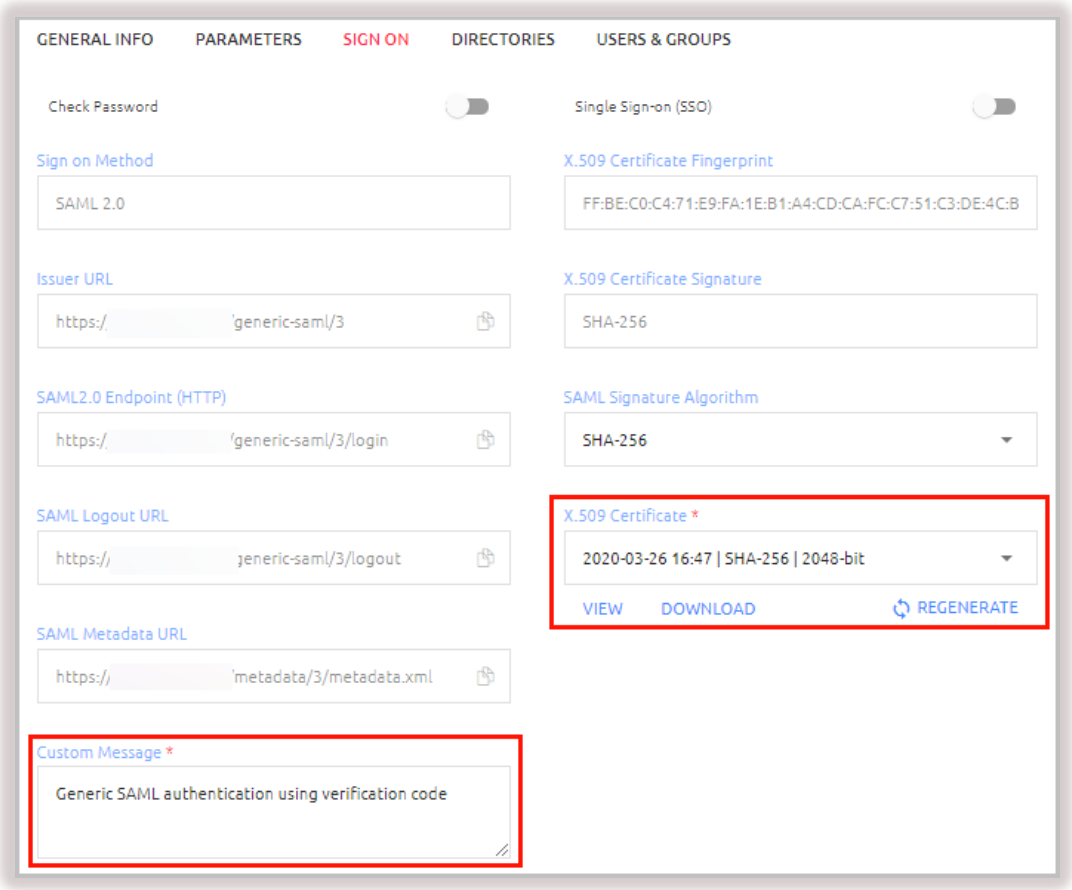
Setting	Description
Service Name	Enter a display name to identify the Service Provider (e.g., NetScaler).
Issuer	Enter the issuer of the service (e.g., Citrix).
Description	Enter a brief note about the service.
Display icon	Click and upload an icon that will be displayed on the Login page for the service.



Then, click **Save**.

3. 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.



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

Note: You will configure service parameters and add users to the service at a later stage of the integration (Completing Service Integration).

Configuring the Citrix NetScaler Gateway

For successful integration, the Octopus Authentication Server has to be set as an Identity Provider in Citrix NetScaler. In order to do this, the following processes need to be carried out:

- Updating the Octopus Authentication SAML Certificate
- Adding the 3rd Party SAML Authentication Server
- Creating the SAML Authentication Policy
- Assigning the Policy to the NetScaler Virtual Server

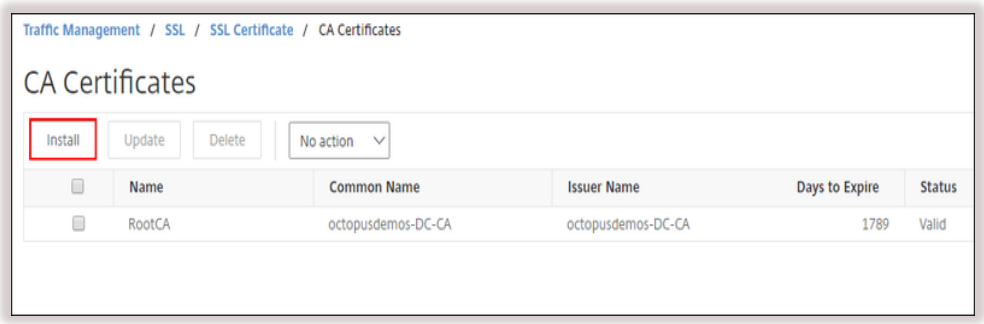
Updating the Octopus Authentication SAML Certificate

Follow the procedure below to install the SAML service certificate in Citrix NetScaler.

To update the Octopus Authentication SAML certificate:

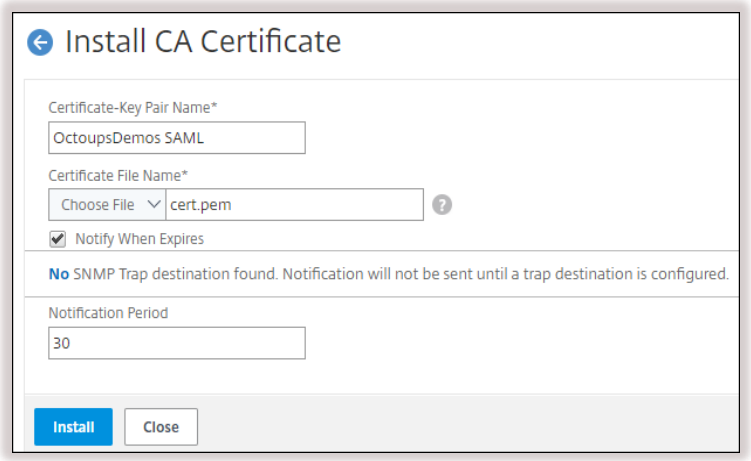
1. In the Citrix NetScaler Admin Console, select the **Configuration** tab.

   Then, navigate to **Traffic Management > SSL > Certificates > CA Certificates**, and click **Install**.



   The **Install CA Certificate** window opens.

2. In the **Certificate-Key Pair Name** field, enter a name for the certificate.



3. Under **Certificate File Name**, select **local** from the dropdown list. Then, navigate to and select the certificate that you downloaded when configuring the Octopus Authenticator SAML Service (Creating the Citrix SAML Service).
4. Click **Install**.

Adding the 3rd Party SAML Authentication Server

The following procedure explains how to add the 3rd party Authentication Server to Citrix NetScaler.

To add the 3rd party Authentication Server:

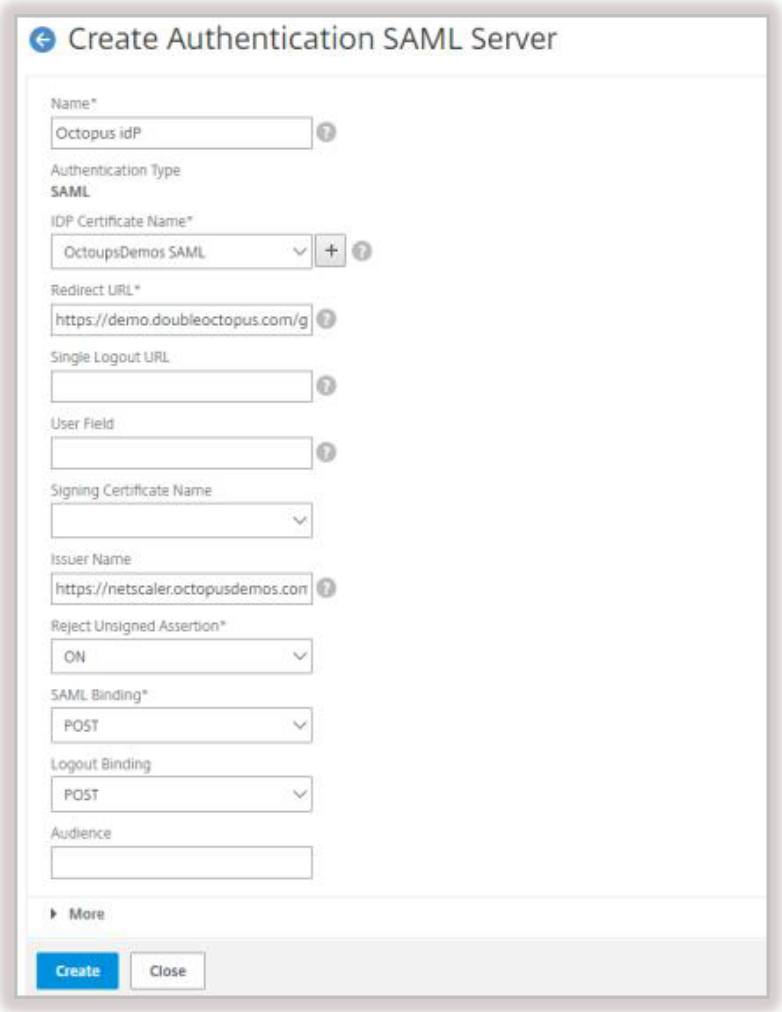
1. From the **Configuration** tab of the Citrix NetScaler Admin Console, navigate to **NetScaler Gateway > Policies > Authentication > SAML**.

   Select the **Servers** tab, and click **Add**.

   The **Create Authentication SAML Server** window opens.

2. Configure the following settings:

Setting	Value / Notes
Name	Enter a name for the server (e.g., Octopus IDP).
IDP Certificate Name	Select the IDP certificate that you installed (Updating the Octopus Authentication SAML Certificate).
Redirect URL	The identity provider login URL. Copy the value from the SAML 2.0 Endpoint (HTTP) field **in** the **Sign On** tab of the Citrix service that you created in the Octopus Management Console.
Issuer Name	The NetScaler virtual server URL (e.g., *https://netscaler.octopusdemos.com*)**.**



3. Click **Create**.

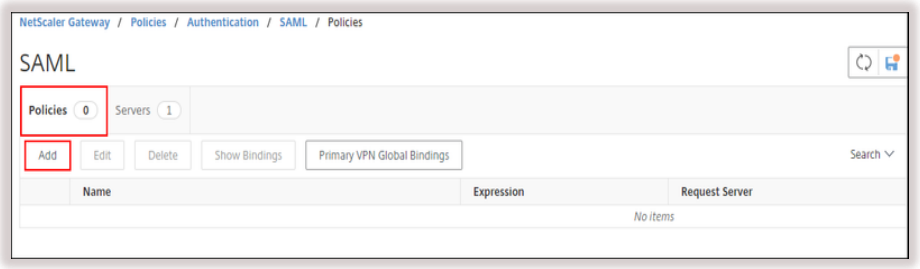
Creating the SAML Authentication Policy

Follow these steps to add and configure the authentication policy.

To create the SAML authentication policy:

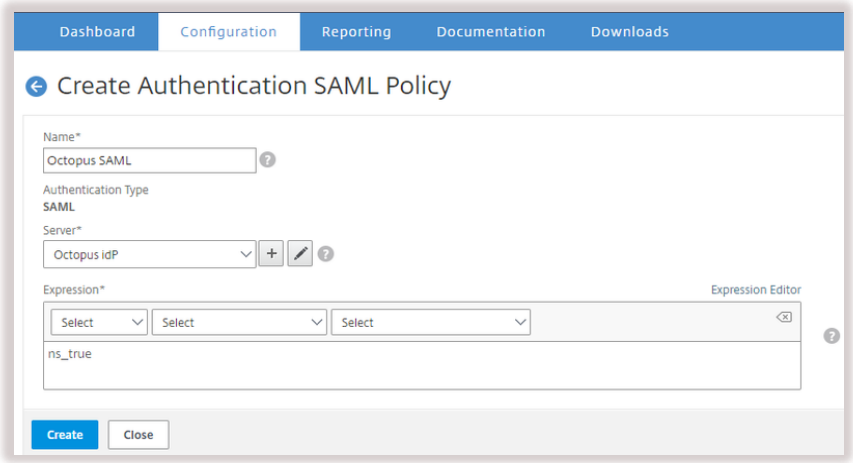
1. From the **Configuration** tab of the Citrix NetScaler Admin Console, navigate to **NetScaler Gateway > Policies > Authentication > SAML**.

   Select the **Policies** tab, and click **Add**.



   The **Create Authentication SAML Policy** window opens.
2. Configure the following settings:

Setting	Value / Notes
Name	Enter a name for the policy (e.g., Octopus SAML).
Server	Select the SAML server that you added **(**Adding the 3rd Party SAML Authentication Server).
Expression	Enter the required logical expression (e.g., *ns_true*).



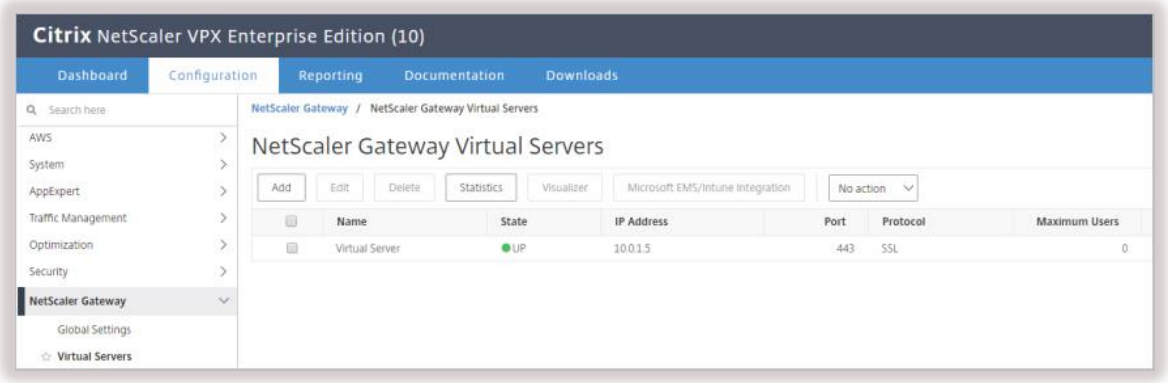
3. Click **Create**, and then click **OK** in the confirmation popup.

Assigning the Policy to the NetScaler Virtual Server

The procedure below explains how to bind the SAML authentication policy to the selected virtual server.

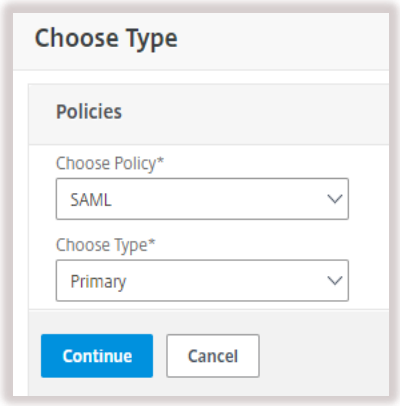
To assign the policy:

1. From the **Configuration** tab of the Citrix NetScaler Admin Console, navigate to **NetScaler Gateway > Virtual Servers**. Then, select the virtual server to be assigned to the SAML policy.

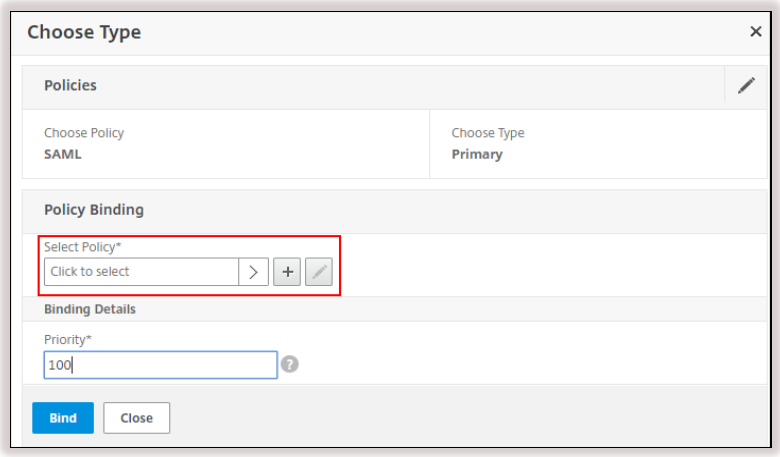


   The **VPN Virtual Server** window opens.
2. In the **Basic Authentication** portion of the **VPN Virtual Server** window, click the **+** icon to open the **Choose Type** dialog.
3. From the **Choose Policy** dropdown, select **SAML**, and from the **Choose Type** dropdown, select **Primary**.

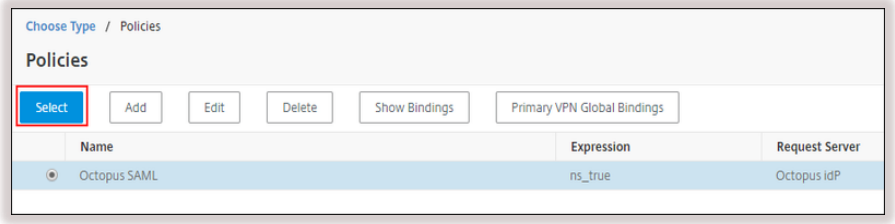
   Then, click **Continue**.



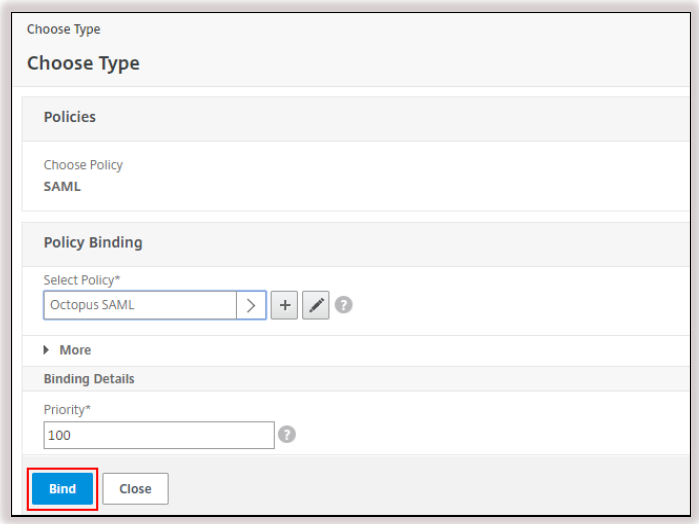
4. Click in the **Select Policy** field and choose the SAML authentication policy that you created.



Then, click **Select**.



5. At the bottom of the **Choose Type** dialog, click **Bind**.



6. Click **Done**.

   Then, in the upper right corner of the NetScaler Admin Console, click  to save the running configuration.

Completing Service Integration

To complete the integration, the Octopus Authentication SAML service needs to be configured to receive authentication requests from Citrix NetScaler and authenticate the relevant users. The following sections present:

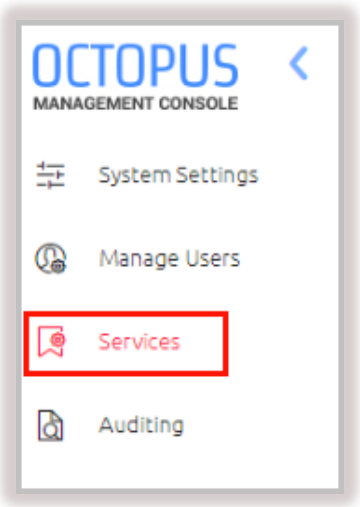
- Configuring the Citrix Service Parameters
- Assigning Users to the Service

Configuring the Citrix Service Parameters

Follow the procedure below to edit the parameters of the Citrix SAML service you created in the Octopus Management Console.

To configure the service parameters:

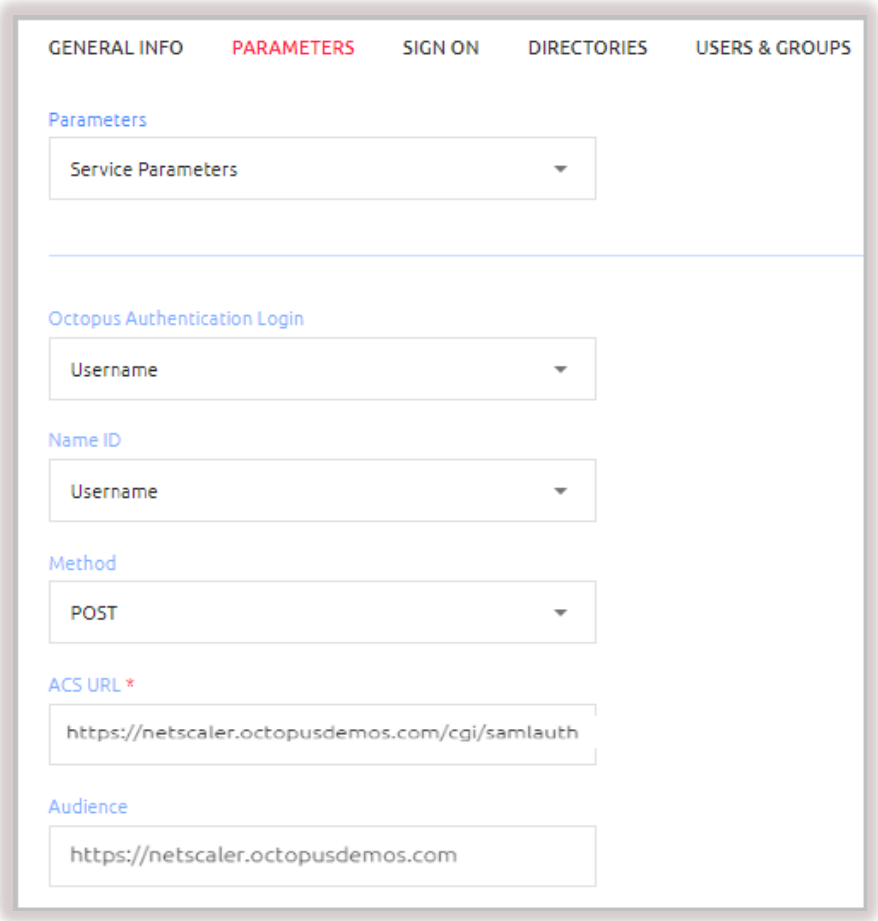
1. Log into the Octopus Management Console and open the **Services** menu.



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

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

Setting	Value / Notes
Octopus Authentication Login	Login method for the Octopus Authentication Server
Name ID	Login parameter for Citrix NetScaler
Method	POST
ACS URL	*https://<NetScaler Virtual Server FQDN>/cgi/samlauth*
Audience	Enter the issuer value



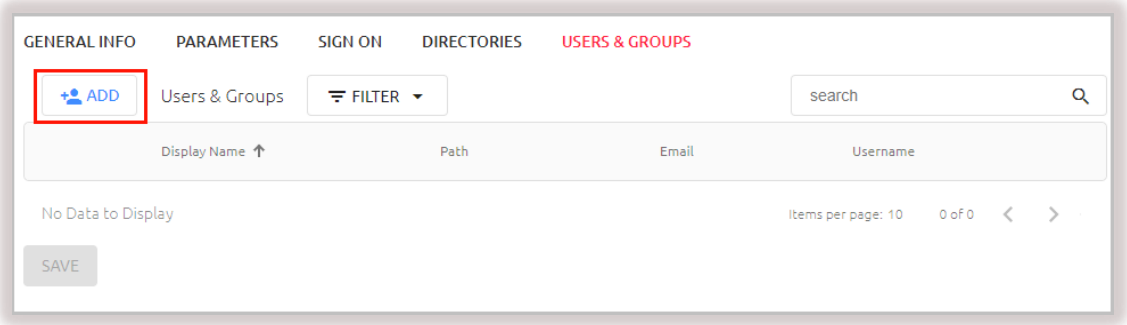
4. At the bottom of the **Parameters** tab, click **Save**.

Assigning Users to the Service

Follow the steps below to specify the users who are authorized to authenticate through the service.

To assign users to the service:

1. From the settings of the Citrix SAML service, open the **Directories** tab. Then, select the checkbox of the directory to be integrated with the service. (Local or LDAP
2. Open the **Users & Groups** tab and click **Add**.



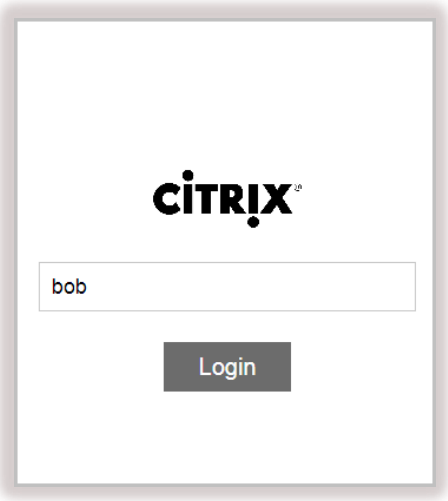
   A popup opens, with a list of directories displayed on the left.
3. Expand the relevant directory and select the checkboxes of the groups and users that you want to add to the service. Then, click **Done** to close the popup.

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

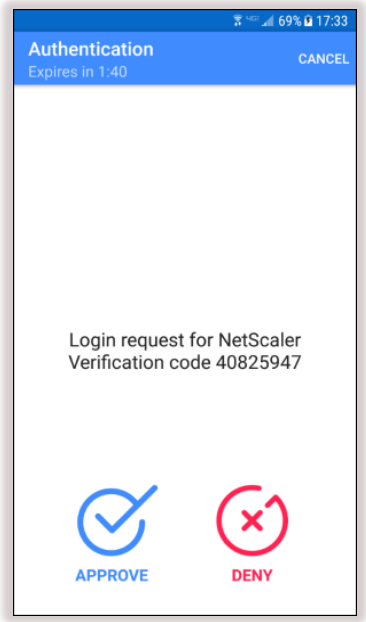
Running the Solution

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

1. From a browser, the user opens the Citrix Netscaler Gateway login page. The user is then redirected to the Double Octopus Authentication page.
2. The user enters a username and clicks **Login**.



A challenge number 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 onto Citrix NetScaler Gateway. When Citrix StoreFront is configured, the user is redirected to the Citrix StoreFront page.