

Integrations

SAML Authentication

V6.0.3

CONTENTS

1	SAML Authentication	1
2	Installing SAML Authentication	2
3	Uninstalling SAML Authentication	3
4	Configuring SAML Authentication	4
4.1	Configuring SAML Authentication in Microsoft Azure Portal	4
4.2	Configuring SAML Authentication in Logpoint	9
4.3	Configuring Default Settings	12
4.4	Downloading Logpoint Metadata	13
4.5	Mapping Roles	14
5	Login with SAML Authentication	17
6	Manage SAML Authentication Users	21

SAML AUTHENTICATION

SAML Authentication enables you to log into Logpoint using the SAML Identity Providers (IdPs). You can also implement *Azure Active Directory* multi factor authentication using SAML. Go to [Configuring SAML Authentication in Microsoft Azure Portal](#) for details.

You can use it to configure any SAML IdPs that are SAML v2 compliant, including:

1. Microsoft's Active Directory Federation Services (ADFS)
2. OneLogin
3. IdentityServer4
4. Shibboleth
5. Ping Identity
6. CyberArk
7. Ilex

INSTALLING SAML AUTHENTICATION

Prerequisite

Logpoint v7.0.0 or later

To install SAML Authentication:

1. Download the .pak file from the [Help Center](#).
2. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

After installing SAML Authentication, you can find it under *Settings >> System Settings >> Plugins*.

UNINSTALLING SAML AUTHENTICATION

1. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
2. Click the **Uninstall** (🗑️) icon in **Actions**.
3. Click **Yes**.

CONFIGURING SAML AUTHENTICATION

To implement *Azure Active Directory* using *SAML*, you must first configure *SAML* in Microsoft Azure Portal and then configure SAML Authentication in Logpoint.

4.1 Configuring SAML Authentication in Microsoft Azure Portal

To implement *Azure Active Directory* using *SAML*, first you need to:

1. *Add Azure AD SAML Toolkit*
2. *Creating User Account*
3. *Assign the User Account to an Enterprise Application*
4. *Enable SAML*

in the Microsoft Azure Portal and then *configure SAML Authentication in Logpoint* .

4.1.1 Adding Azure AD SAML Toolkit

1. Go to the [Microsoft Azure Portal](#) and log in with your credentials.
2. Go to **Azure Active Directory** from the navigation bar and click **Enterprise applications**.
3. Click **All applications** and **+ New application**.
4. Search and click **Azure AD SAML Toolkit**.
5. Click **Create**.

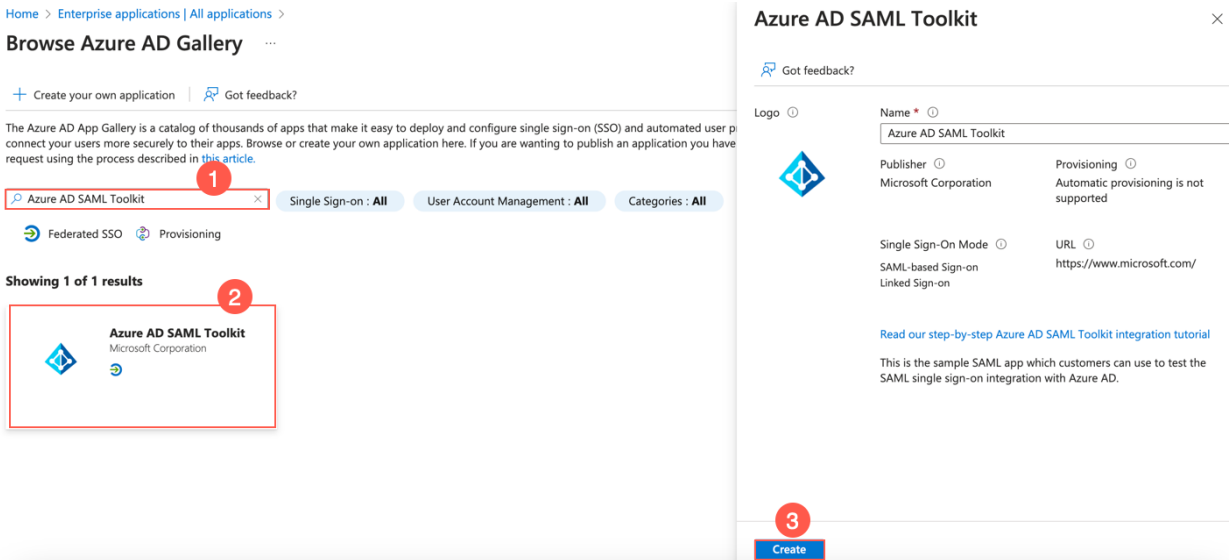


Fig. 1: Adding Azure AD SAML Toolkit

4.1.2 Creating User Account

1. Go to **Azure Active Directory** from the navigation bar of Microsoft Azure Portal and click **Users**.
2. Click the **+ New user** drop-down and click **Create a new user**.
3. Enter the users information and click **Review + create**.
4. Click **Create**.

[Home](#) > [Users](#) >

Create new user ...

Create a new internal user in your organization

Basics Properties Assignments **Review + create**

Basics

User principal name	SAML@logpointsiemoutlook.onmicrosoft.com 
Display name	SAML
Mail nickname	SAML
Password	 
Account enabled	Yes

Properties

User type	Member
-----------	--------

Assignments

Administrative units

Groups

Roles

Create

< Previous

Next >

Fig. 2: Creating a New User

4.1.3 Assigning the User Account to an Enterprise Application

1. Go to **Azure Active Directory** from the navigation bar of Microsoft Azure Portal and click **Enterprise applications**.
2. Click the previously added **Azure AD SAML Toolkit**.

3. Go to **Users and groups** from the navigation bar and click **+ Add user/group**.

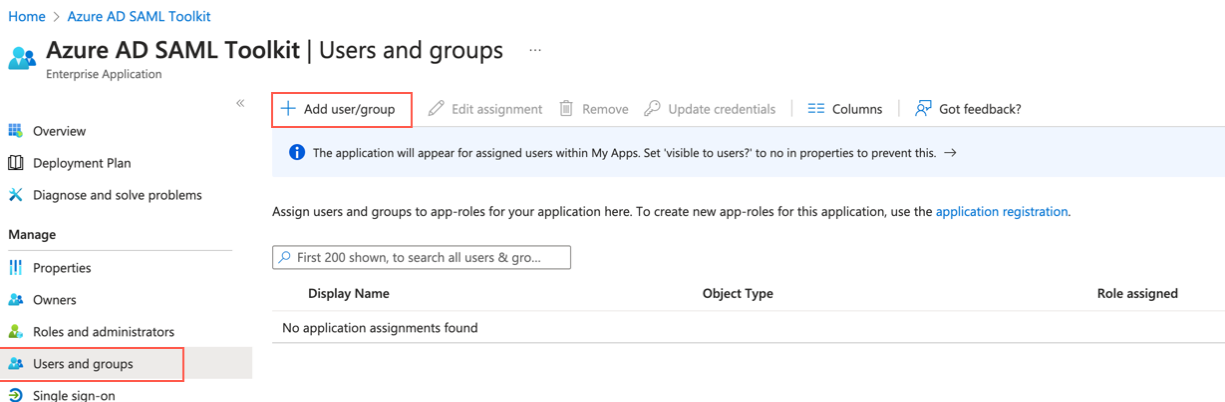


Fig. 3: Adding User/Group

4. Click **None selected** under **Users and groups**.
5. Search for the user or group to assign to the application and select it.
6. Click **Select** and then **Assign**.

4.1.4 Enabling SAML

1. Go to **Azure Active Directory** from the navigation bar of Microsoft Azure Portal and click **Enterprise applications**.
2. Click the previously added **Azure AD SAML Toolkit**.
3. Go to **Single sign-on** from the navigation bar and click **SAML**.

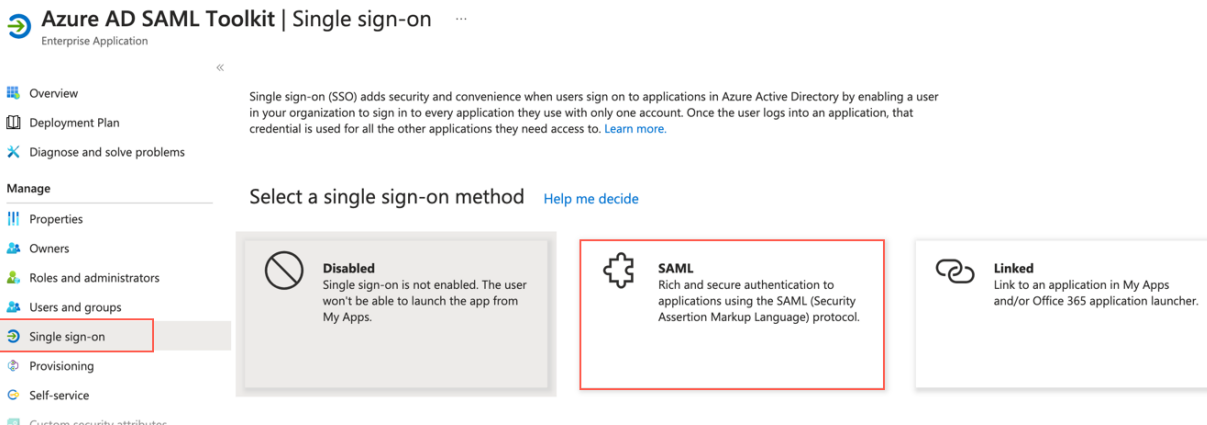


Fig. 4: Enabling SAML

4. Click the edit icon of **Basic SAML Configuration**.
5. Click **Add reply URL** and enter `https://samltoolkit.azurewebsites.net/SAML/Consume`.
6. In **Sign on URL**, enter `https://samltoolkit.azurewebsites.net/`.
7. Click **Save**.

Basic SAML Configuration

 Save
  Got feedback?

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://samltoolkit.azurewebsites.net/SAML/Consume 		☒ ⓘ 

[Add reply URL](#)

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*



Patterns: https://samltoolkit.azurewebsites.net/

Fig. 5: Adding URL

8. Note down the value of **Identifier (Entity ID)** of **Basic SAML Configuration**. You must enter it as **Issuer (EntityID)** while *configuring* SAML Authentication in Logpoint.
9. Search and **Download** the Certificate (Base64) of **SAML Signing Certificate**. You must enter it as **X.509 Certificate** while *configuring* SAML Authentication in Logpoint.
10. Note down the **Login URL** and **Azure AD Identifier** of Set up Azure AD SAML Toolkit. You must enter **Login URL** as **SSO EndPoint URL** and **Azure AD Identifier** as **EntityID** while configuring SAML Authentication in Logpoint.

4.2 Configuring SAML Authentication in Logpoint

The time zones of the IdP server and Logpoint must be identical.

1. Go to *Settings >> System Settings* from the navigation bar and click **Plugins**.
2. Find **SAML Authentication** and click **Manage**.

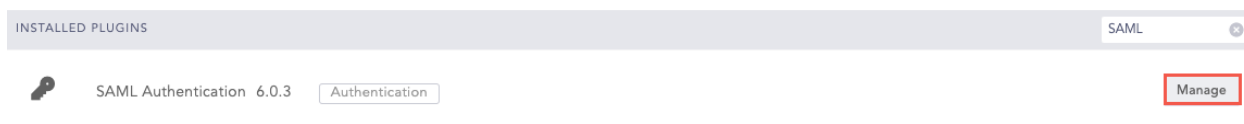


Fig. 6: Manage SAML Authentication

3. Click **ADD SERVER**.

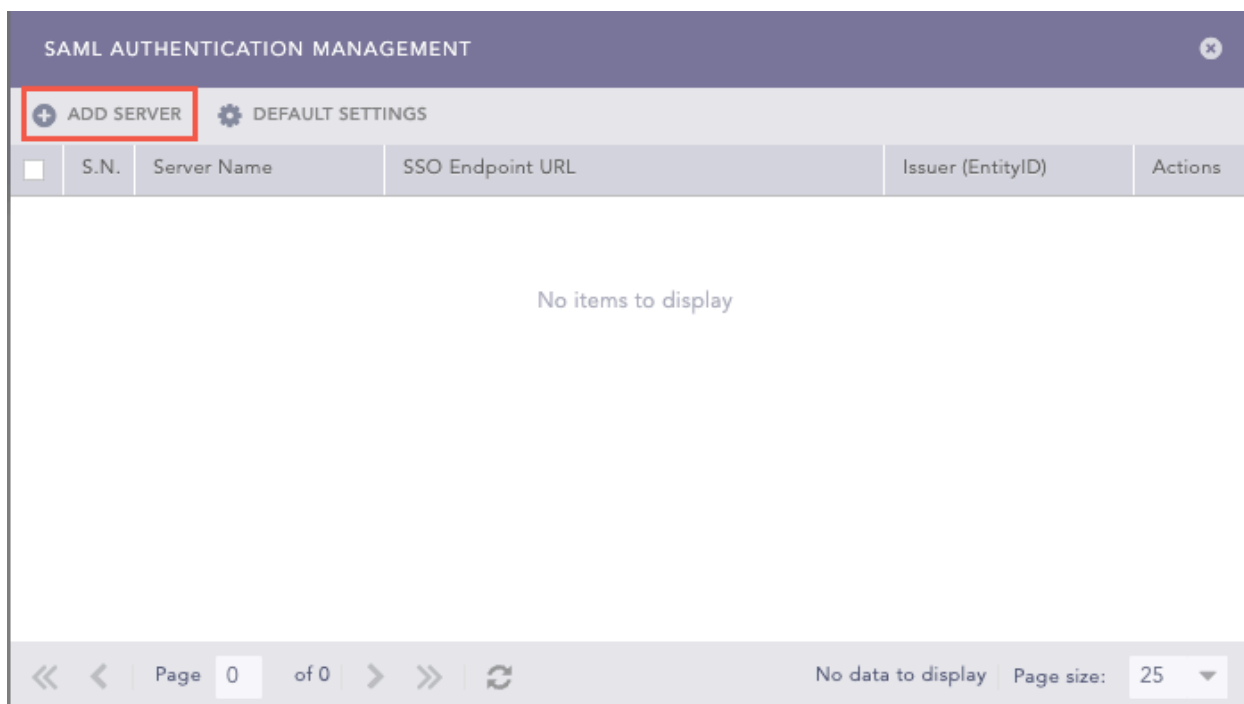


Fig. 7: Add SAML Server

4. Enter a unique **Server Name**.
5. In **Issuer (EntityID)**, enter the Logpoint's IP address. You must add these Issuer (EntityID) and ACS (Consumer) URL in your IdP server. For Shibboleth, you must download the [Logpoint metadata file](#) and upload it in its server.
SAML Authentication generates the **ACS (Consumer) URL** automatically.

6. Enter the **EntityID**. You can find it in your IdP metadata file as **entity ID**.
7. Enter the **SSO EndPoint URL**. You can find it in your IdP metadata file as **Location** in **SingleSignOnService**. The **SingleSignOnService** must be **HTTP-POST**.
8. Enter the **X.509 Certificate**. You can find it in your IdP metadata file as the signing certificate. For Shibboleth, you can find it as the FrontChannel signing certificate.
9. In **Response Username Field**, enter the field to extract the username from the SAML response.
10. In **Response Role Field**, enter the field to extract the role from the SAML response.
11. Click **Save**.

SAML SERVER INFORMATION

SERVICE PROVIDER (LOGPOINT)

Server Name

SAML

Issuer (EntityID)

mysaml-sso

ACS (Consumer) URL

https://10.45.13.7/pluggables/Authentication/SAMLAAuthentication/login

IDENTITY PROVIDER

EntityID

example.idp

SSO Endpoint URL

https://mysaml.plugins.com

X.509 CERTIFICATE

Certificate

Save

Cancel

Fig. 8: Adding an IdP Server

12. Click **Yes** to make SAML authentication as the default authentication. Otherwise, click **No**.

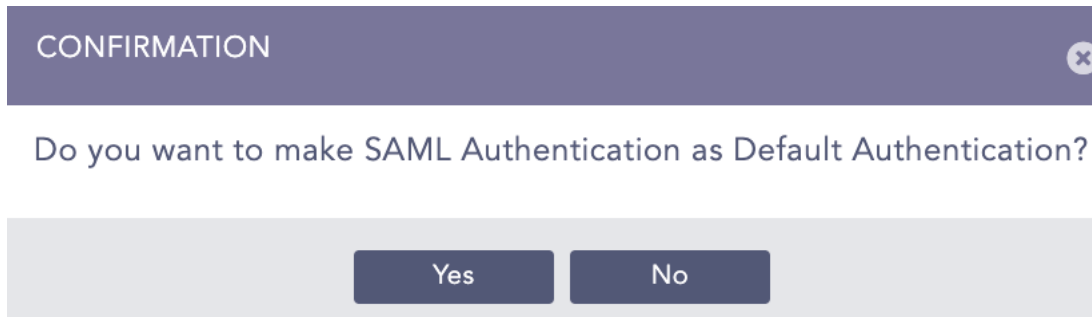


Fig. 9: Select Authentication

Once you add an IdP server, **Role Mapping** is added and **Add Server** is removed in SAML Authentication management.

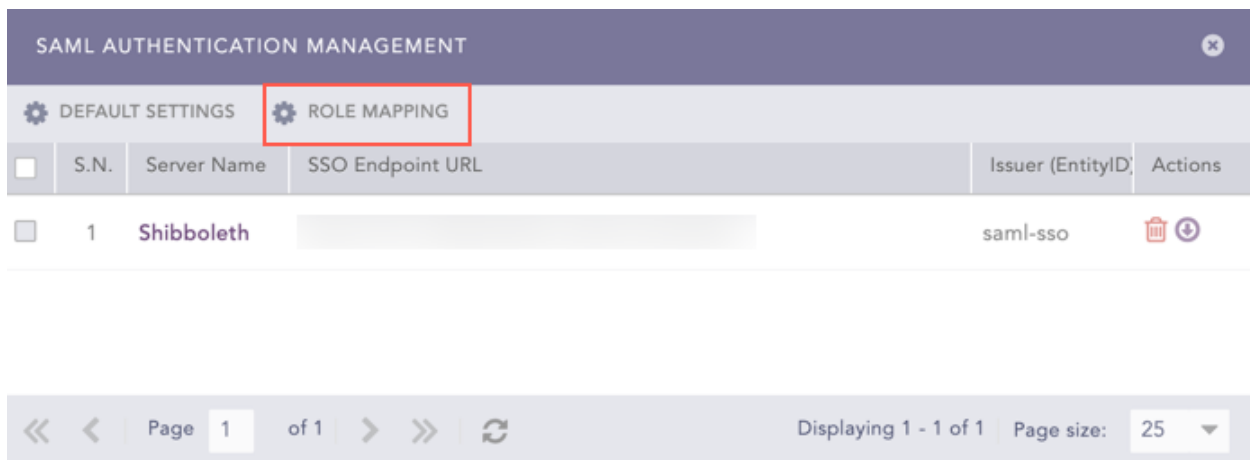


Fig. 10: SAML Authentication Management

4.3 Configuring Default Settings

1. Go to *Settings >> System Settings* from the navigation bar and click **Plugins**.
2. Find **SAML Authentication** and click **Manage**.
3. Click **Default Settings**.

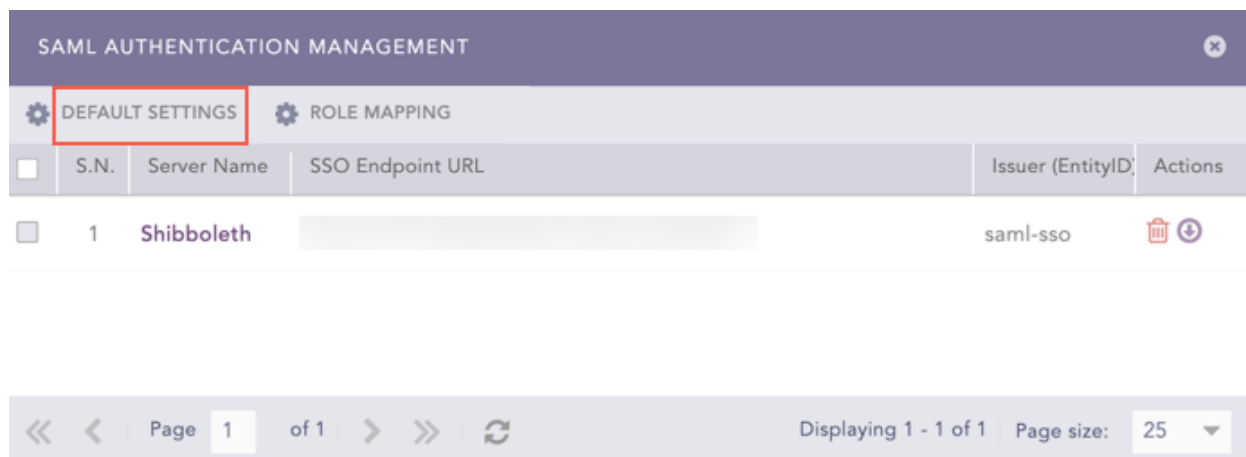


Fig. 11: SAML Authentication Management

4. Select a Logpoint user group as the **Default Role**. SAML Authentication assigns the user group to the SAML Authentication users whose role attribute are not returned by the IdP server.
5. Click **Save**.

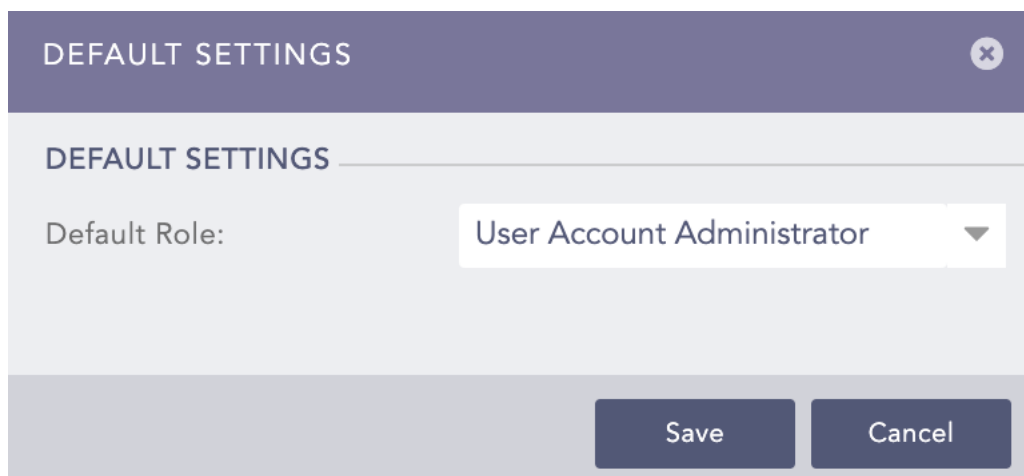


Fig. 12: Default Settings

4.4 Downloading Logpoint Metadata

1. Go to *Settings >> System Settings* from the navigation bar and click **Plugins**.
2. Find **SAML Authentication** and click **Manage**.
3. Click the **Download** icon from **Actions**.

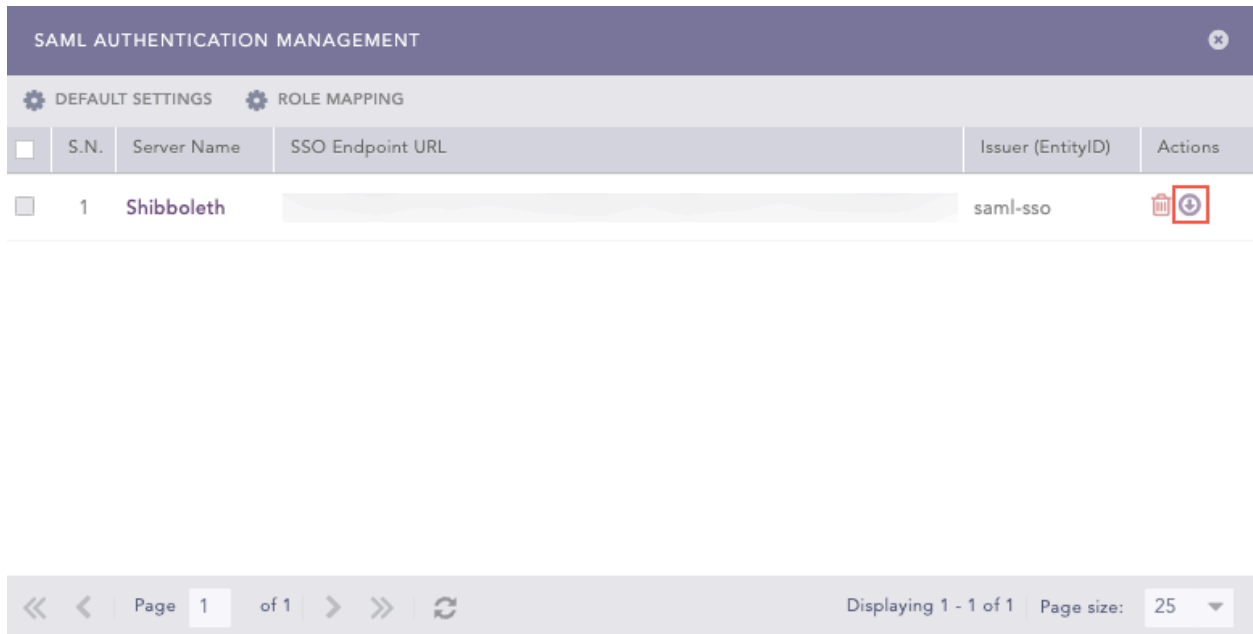


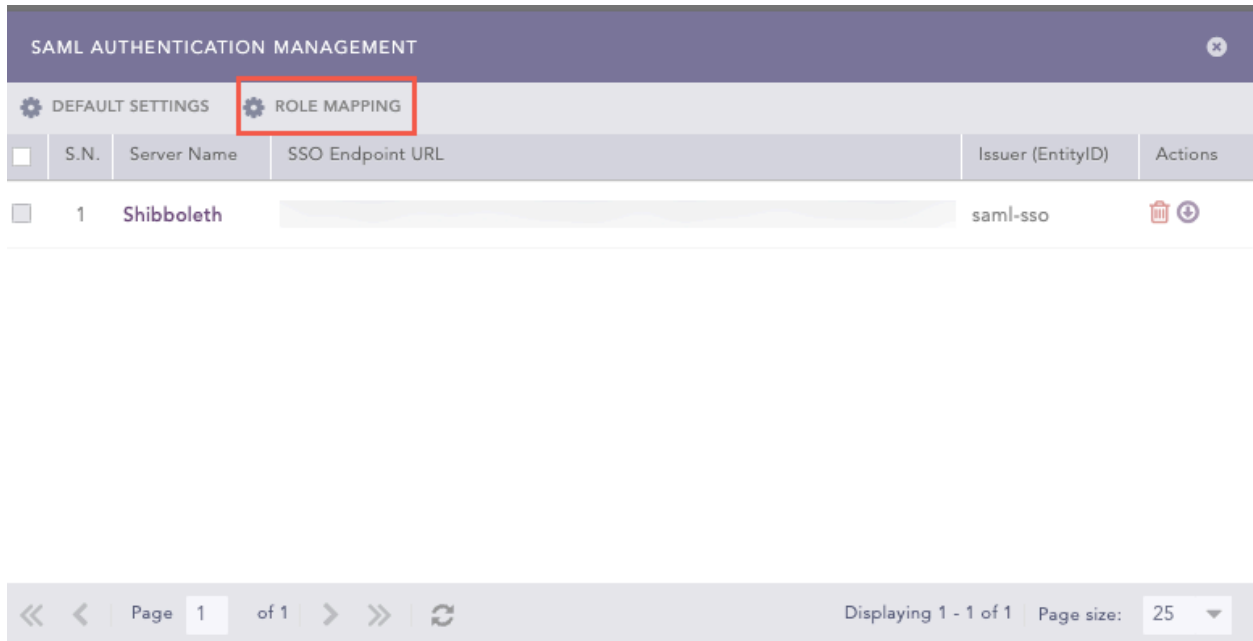
Fig. 13: Downloading Logpoint Metadata

4.5 Mapping Roles

You can map a SAML role to a Logpoint user group to grant access permission in Logpoint. A SAML role can be mapped to a single Logpoint user group only. This is mandatory.

To map a SAML role to a Logpoint user group:

1. Go to *Settings >> System Settings* from the navigation bar and click **Plugins**.
2. Find **SAML Authentication** and click **Manage**.
3. Click **Roles Mapping**.

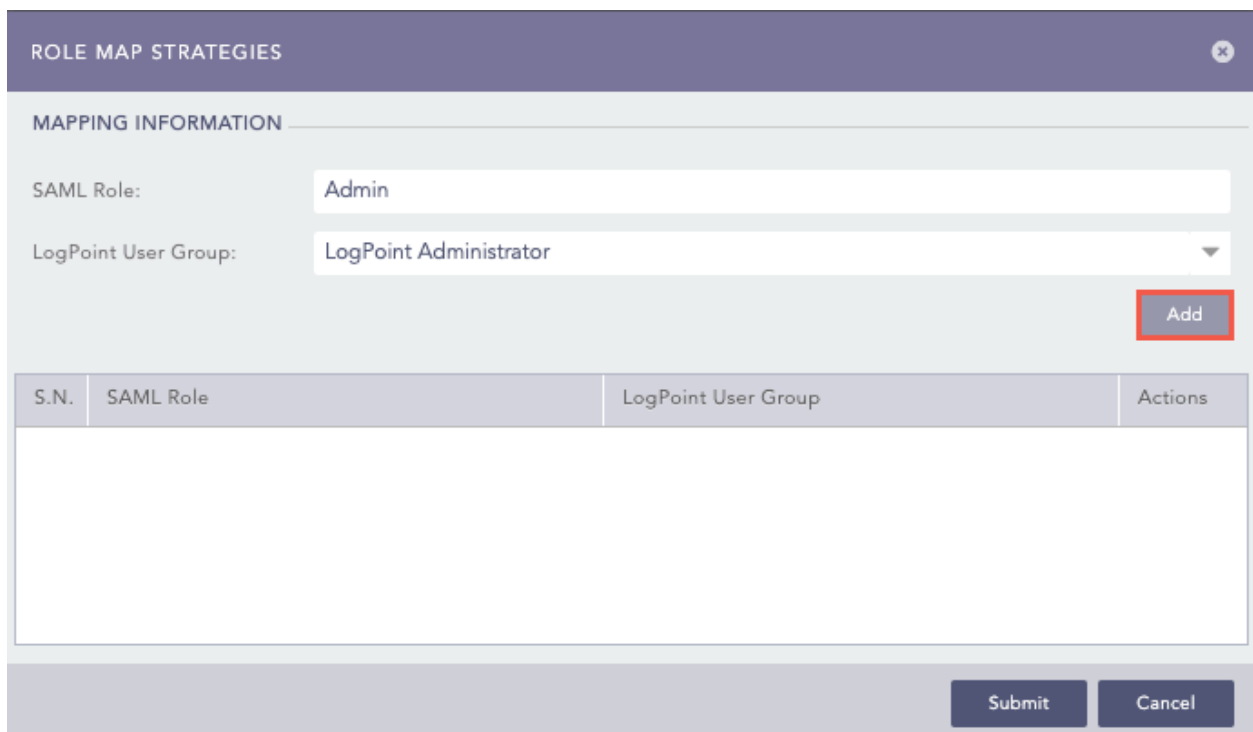


The screenshot shows the 'SAML AUTHENTICATION MANAGEMENT' interface. At the top, there are two tabs: 'DEFAULT SETTINGS' and 'ROLE MAPPING'. The 'ROLE MAPPING' tab is selected and highlighted with a red box. Below the tabs is a table with columns: S.N., Server Name, SSO Endpoint URL, Issuer (EntityID), and Actions. The table contains one entry with S.N. '1' and Server Name 'Shibboleth'. The Issuer (EntityID) is 'saml-ssso'. To the right of the entry are icons for delete and refresh. At the bottom of the interface, there is a pagination bar showing 'Page 1 of 1', 'Displaying 1 - 1 of 1', and 'Page size: 25'.

S.N.	Server Name	SSO Endpoint URL	Issuer (EntityID)	Actions
1	Shibboleth		saml-ssso	

Fig. 14: Role Mapping

4. Enter a **SAML Role**.
5. Select a **LogPoint User Group** for the provided SAML role.



The screenshot shows the 'ROLE MAP STRATEGIES' interface. It has a tab labeled 'MAPPING INFORMATION'. Below the tab, there are two input fields: 'SAML Role:' with the value 'Admin' and 'LogPoint User Group:' with the value 'LogPoint Administrator'. To the right of these fields is a red 'Add' button. Below the input fields is a table with columns: S.N., SAML Role, LogPoint User Group, and Actions. The table is currently empty. At the bottom right of the interface are 'Submit' and 'Cancel' buttons.

S.N.	SAML Role	LogPoint User Group	Actions
------	-----------	---------------------	---------

Fig. 15: SAML Role Mapping

6. Click **Add**.

You can view all the mapped SAML roles and Logpoint user groups in **Role Map Strategies**. You can either edit or delete them from **Actions**.

ROLE MAP STRATEGIES

MAPPING INFORMATION

SAML Role:

LogPoint User Group:

Add

S.N.	SAML Role	LogPoint User Group	Actions
2	Admin	LogPoint Administrator	^ v

Submit

Cancel

Fig. 16: SAML Roles

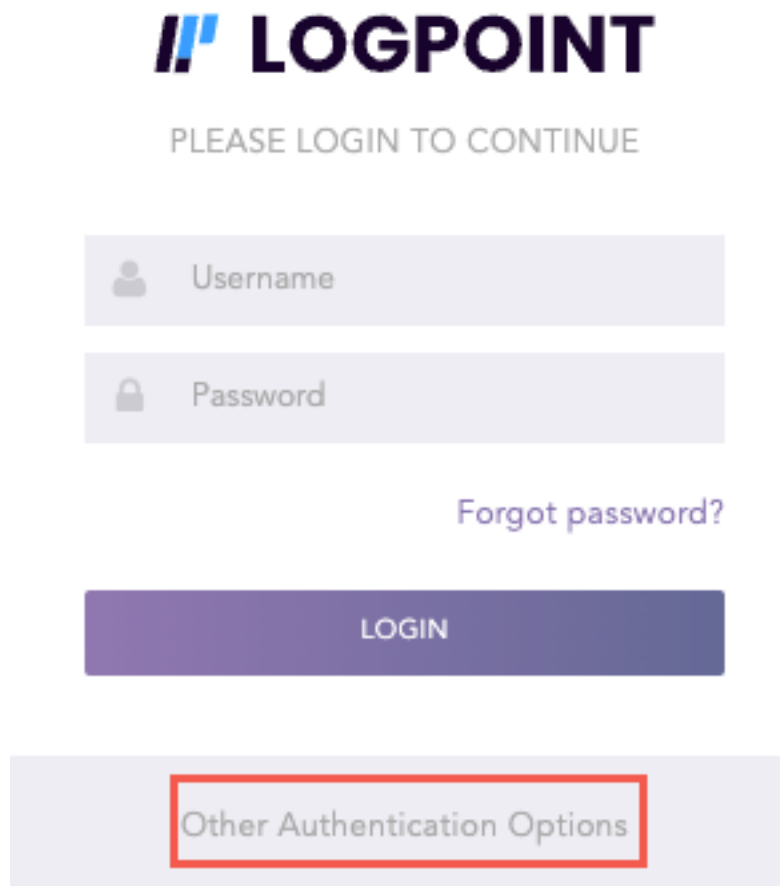
7. Click **Submit**.

LOGIN WITH SAML AUTHENTICATION

If you have selected SAML Authentication as the default authentication, Logpoint redirects you to the IdP authorization server. You can log into Logpoint using the IdP server credentials.

To log into Logpoint using SAML Authentication:

1. On the login page, click **Other Authentication Options**.



The image shows a login page for Logpoint. At the top is the Logpoint logo, which consists of two blue slanted bars followed by the word "LOGPOINT" in bold, dark blue capital letters. Below the logo is the text "PLEASE LOGIN TO CONTINUE" in a smaller, grey font. There are two input fields: the first is labeled "Username" with a grey user icon to its left, and the second is labeled "Password" with a grey lock icon to its left. Below these fields is a link that says "Forgot password?" in a purple font. A large, dark purple button with the word "LOGIN" in white capital letters is positioned below the link. At the bottom of the form is a light grey rectangular box containing the text "Other Authentication Options", which is highlighted by a red rectangular border.

Fig. 1: Other Authentication Options

2. Select **SAML Authentication**.

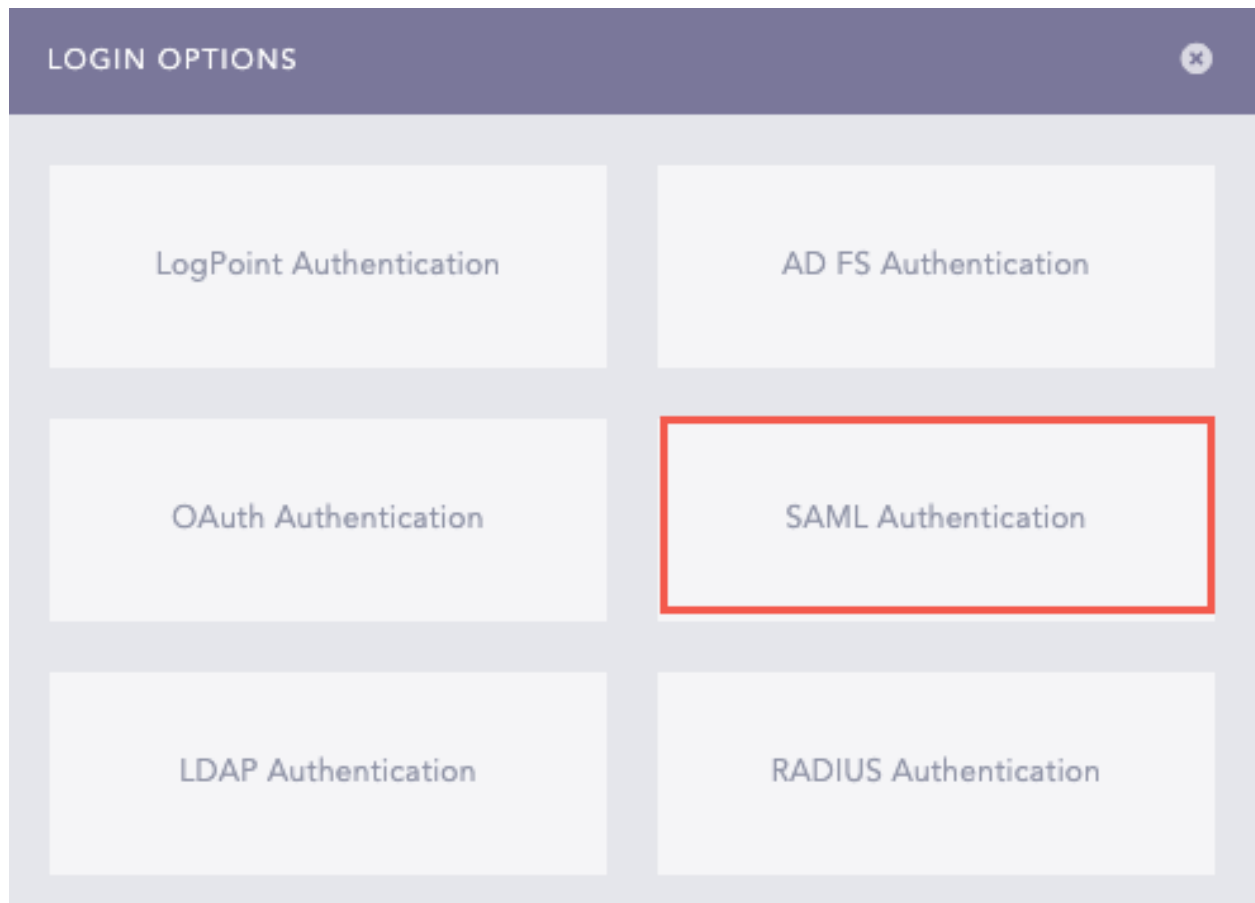


Fig. 2: Login Options

3. Click **LOGIN**.



SAML Authentication

LOGIN

Other Authentication Options

Fig. 3: SAML Authentication

4. Log in using your IdP credentials.

Once you log in, Logpoint adds "saml_" as a prefix to your username. For example, if you log in as "jackson" with SAML Authentication, Logpoint updates your username to "saml_jackson".

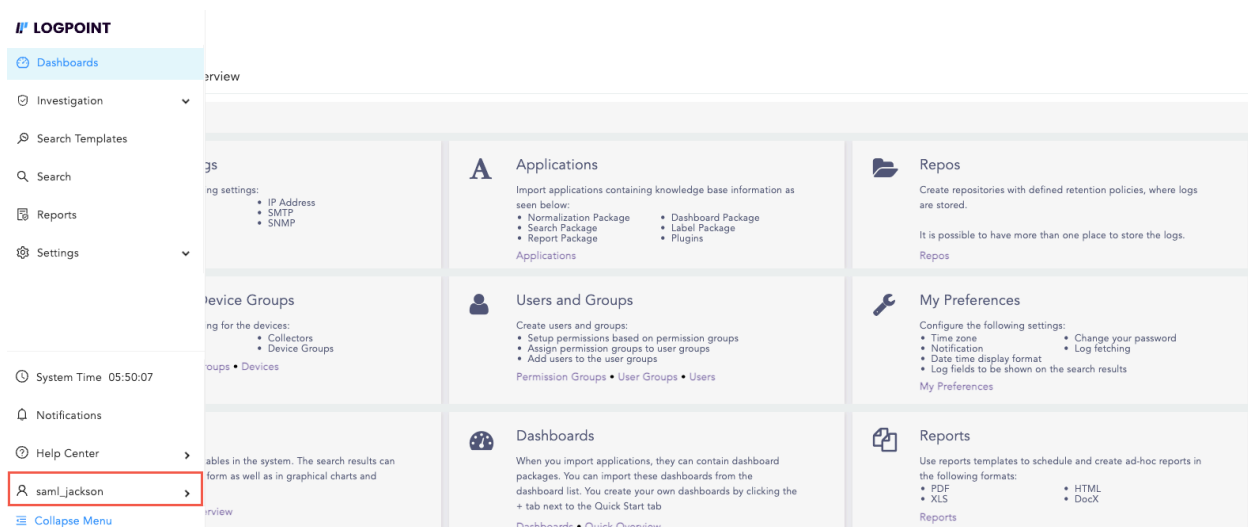


Fig. 4: User Logged in with SAML Authentication

MANAGE SAML AUTHENTICATION USERS

Logpoint users with User Account Administrator and Logpoint Administrator access can manage SAML Authentication users.

To manage the SAML Authentication users:

1. Go to *Settings >> User Accounts* from the navigation bar.
2. Click **Users**.
3. In **Plugin Users**, click **SAML Authentication**. It lists all the SAML Authentication users who have logged into Logpoint.

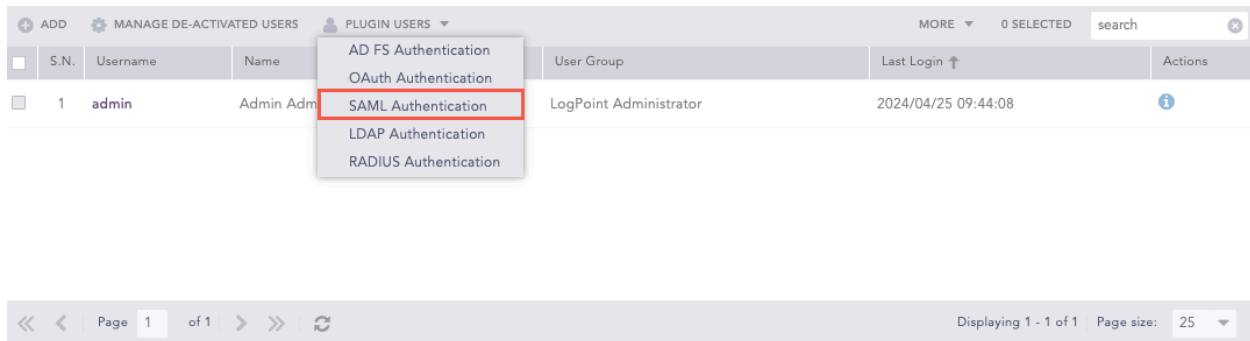
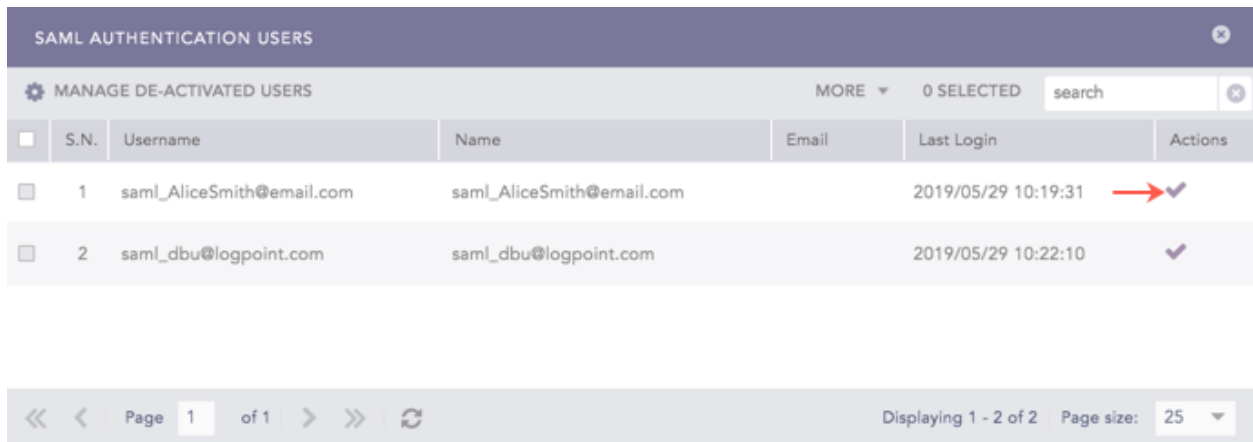


Fig. 1: Plugin Users

4. Click the **De-Activate User** icon in **Actions** to deactivate a user.

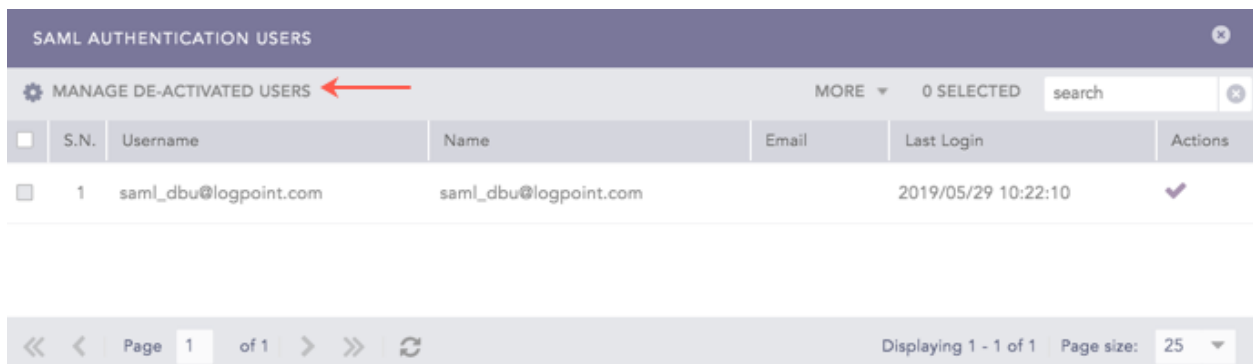


SAML AUTHENTICATION USERS						
MANAGE DE-ACTIVATED USERS						
	S.N.	Username	Name	Email	Last Login	Actions
☐	1	saml_AliceSmith@email.com	saml_AliceSmith@email.com		2019/05/29 10:19:31	
☐	2	saml_dbu@logpoint.com	saml_dbu@logpoint.com		2019/05/29 10:22:10	

Page 1 of 1 | Displaying 1 - 2 of 2 | Page size: 25

Fig. 2: De-Activate SAML Authentication Users

5. Click **Yes**.
6. Enter your credentials and click **Ok**.
7. Click **Manage De-Activated Users** to delete or activate the de-activated users.



SAML AUTHENTICATION USERS						
MANAGE DE-ACTIVATED USERS						
	S.N.	Username	Name	Email	Last Login	Actions
☐	1	saml_dbu@logpoint.com	saml_dbu@logpoint.com		2019/05/29 10:22:10	

Page 1 of 1 | Displaying 1 - 1 of 1 | Page size: 25

Fig. 3: Manage De-Activated SAML Authentication Users

8. Click the **Activate** icon or the **Delete** icon to activate or delete the de-activated user.

DEACTIVATED USERS						
MORE ▾ 0 SELECTED						
☐	S.N.	Username	Name	Email	Last Login	Actions
☐	1	saml_AliceSmith@email.com	saml_AliceSmith@email.com		2019/05/29 10:19:31	  

Navigation: << < Page 1 of 1 > >> Refresh

Displaying 1 - 1 of 1 Page size: 25 ▾

Fig. 4: Activate the De-Activated SAML Authentication User

DEACTIVATED USERS						
MORE ▾ 0 SELECTED						
☐	S.N.	Username	Name	Email	Last Login	Actions
☐	1	saml_AliceSmith@email.com	saml_AliceSmith@email.com		2019/05/29 10:19:31	  

Navigation: << < Page 1 of 1 > >> Refresh

Displaying 1 - 1 of 1 Page size: 25 ▾

Fig. 5: Delete the De-Activated SAML Authentication User