LOGPOINT

Integrations

SAML Authentication

V6.0.1

CONTENTS

CHAPTER

ONE

SAML AUTHENTICATION

SAML Authentication enables you to log in to Logpoint using the SAML Identity Providers (IdPs).

You can use it to configure any SAML IdPs that are SAML v2 compliant. This guide covers the configuration of the following IdPs:

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

Note: You can also implement *Azure Active Directory* multi factor authentication using *SAML*. Go to *Appendix* for details.

CHAPTER

TWO

INSTALLING SAML AUTHENTICATION

Prerequisite

Logpoint v7.0.0 or later

To install SAML Authentication:

1. Download the .pak file from the *Download* section in Release Notes.
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*.

CHAPTER

THREE

UNINSTALLING SAML AUTHENTICATION

You must remove SAML Authentication configuration to delete 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**.

CHAPTER

FOUR

CONFIGURING SAML AUTHENTICATION

4.1 Configuring SAML Authentication

Note: To implement *Azure Active Directory* using *SAML*, you must first configure *SAML* in Microsoft Azure Portal and then configure SAML Authentication in Logpoint. Go to *Appendix* for details.

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

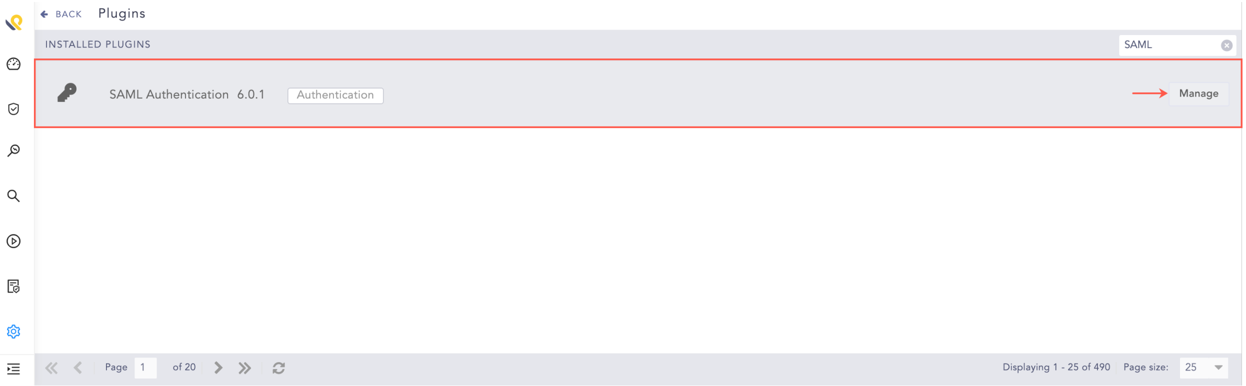


Fig. 1: Manage SAML Authentication

3. Click **ADD SERVER**.

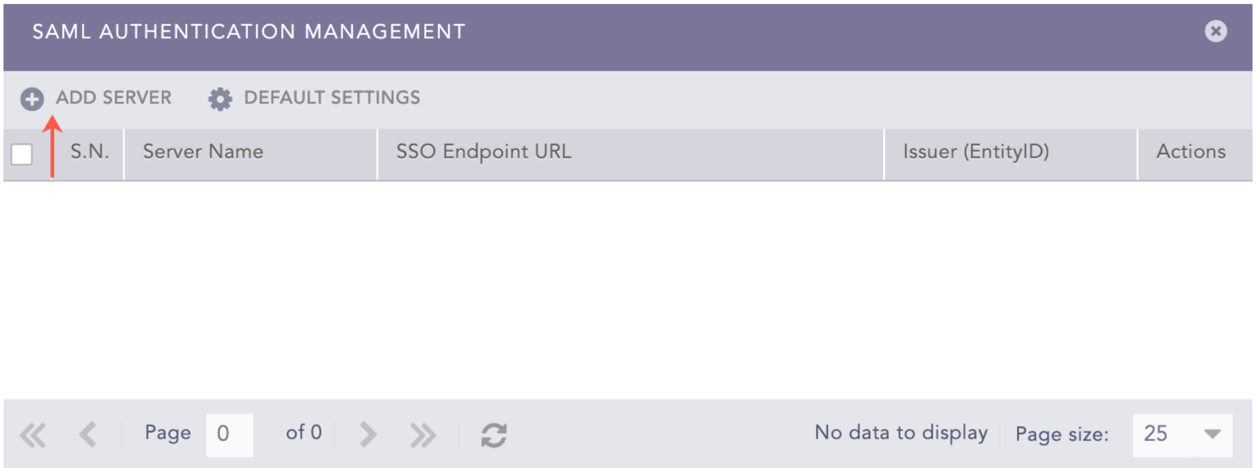


Fig. 2: Add SAML Server

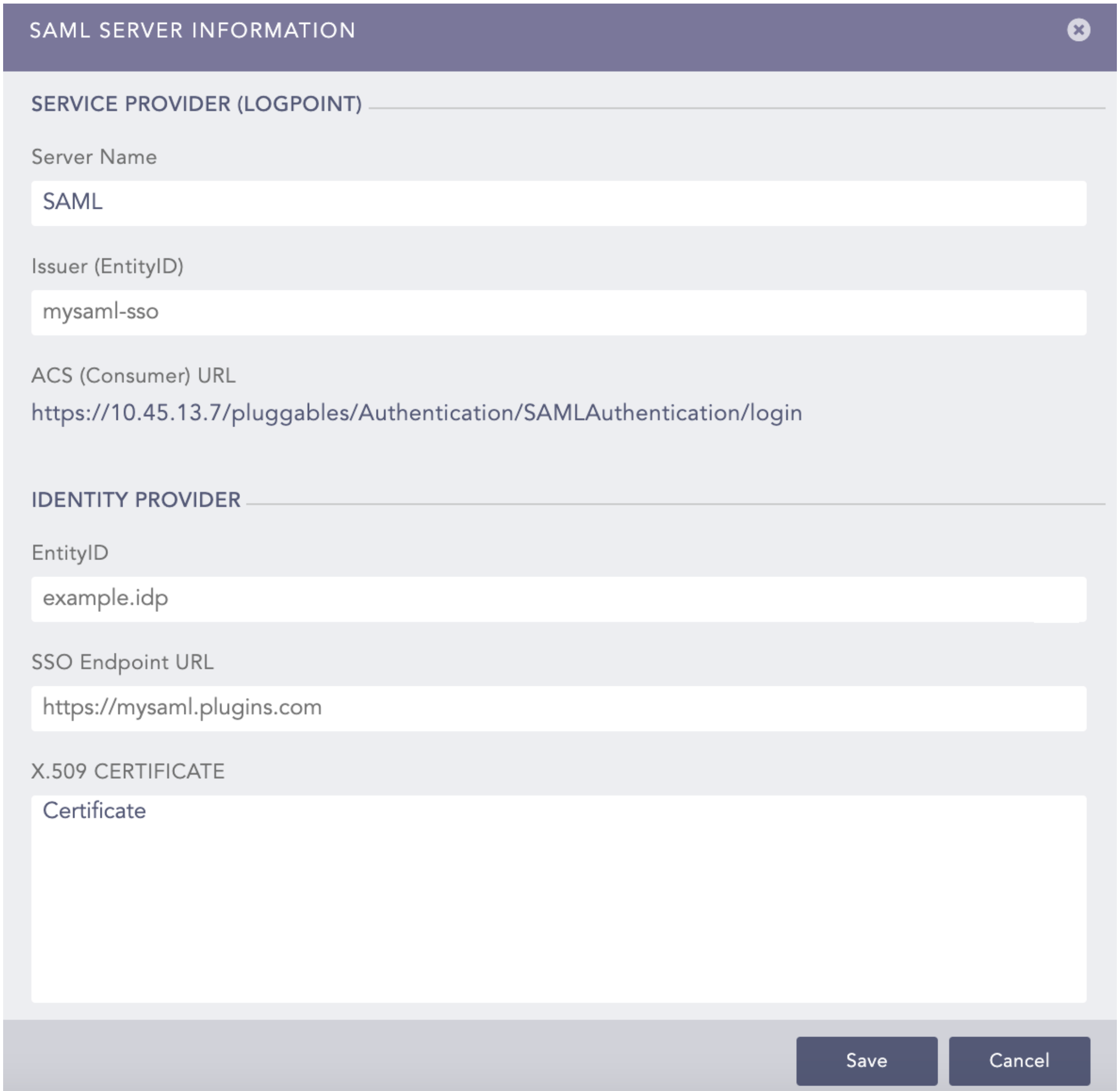
4. Enter a unique **Server Name**.
5. In **Issuer (EntityID)**, enter the Logpoint's IP address.

   SAML Authentication generates the **ACS (Consumer) URL** automatically.

Note: 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.

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**.

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



SAML SERVER INFORMATION

SERVICE PROVIDER (LOGPOINT)

Server Name: SAML

Issuer (EntityID): mysaml-sso

ACS (Consumer) URL: https://10.45.13.7/pluggables/Authentication/SAMLAuthentication/login

IDENTITY PROVIDER

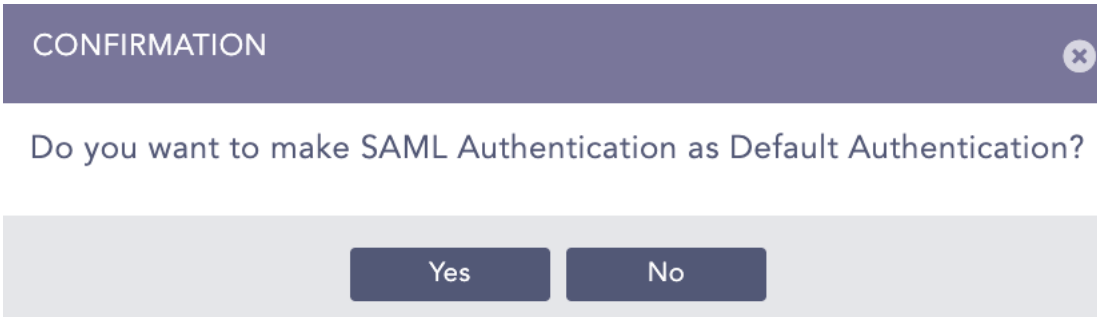
EntityID: example.idp

SSO Endpoint URL: https://mysaml.plugins.com

X.509 CERTIFICATE: Certificate

Fig. 3: Adding an IdP Server

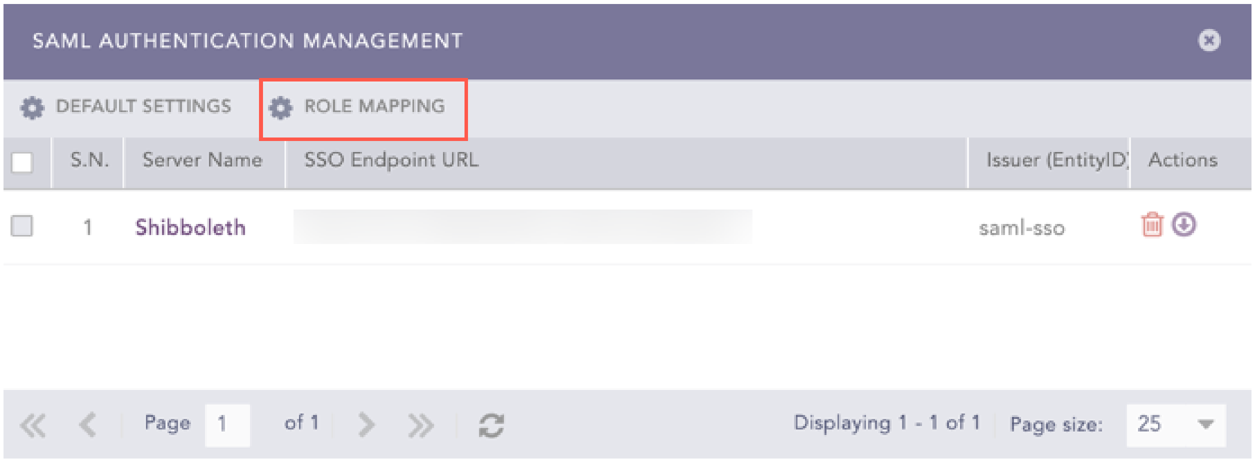
12. Click **Yes** to make SAML authentication as the default authentication. Otherwise, click **No**.



Do you want to make SAML Authentication as Default Authentication?

Fig. 4: Select Authentication

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

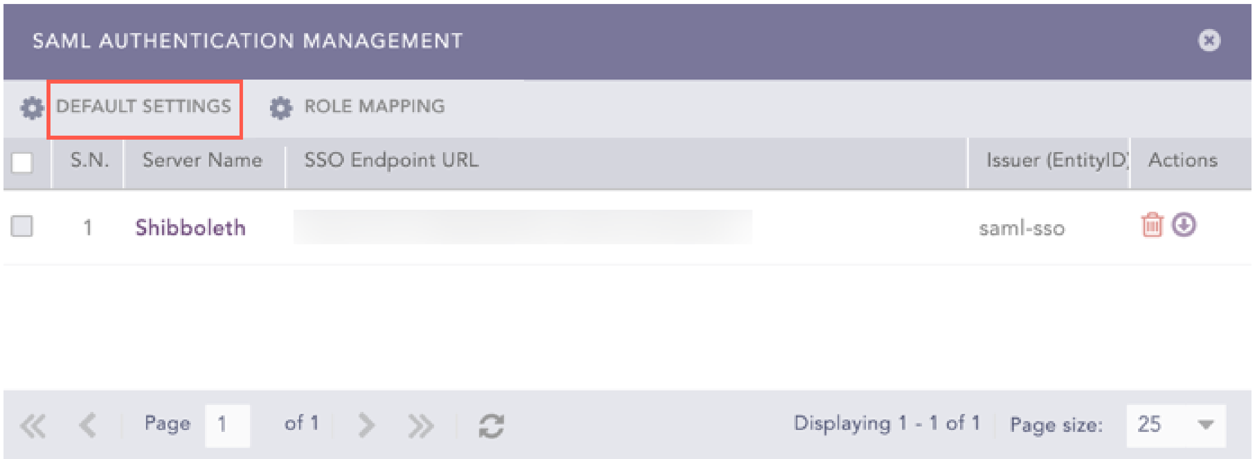


□	S.N.	Server Name	SSO Endpoint URL	Issuer (EntityID)	Actions
□	1	Shibboleth		saml-sso	

Fig. 5: SAML Authentication Management

4.2 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**.



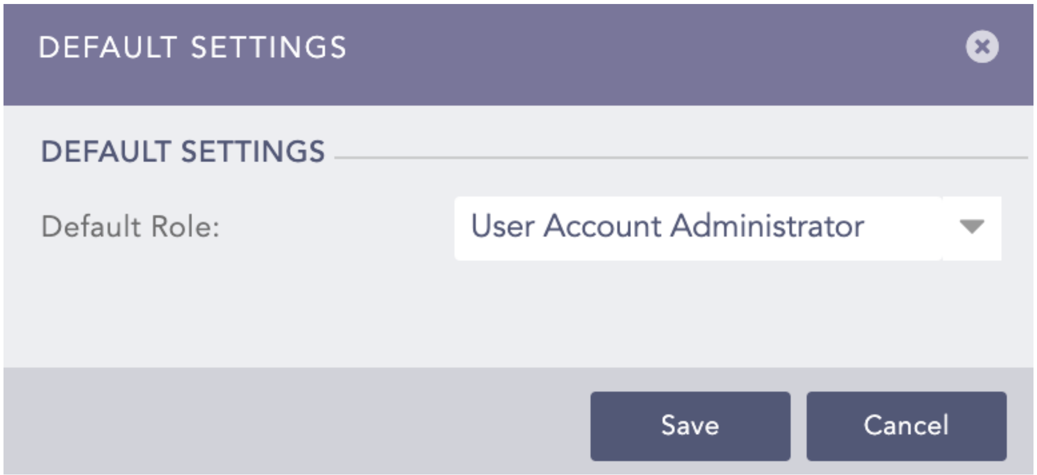
□	S.N.	Server Name	SSO Endpoint URL	Issuer (EntityID)	Actions
□	1	Shibboleth	[redacted]	saml-sso	

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

Fig. 6: 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**.

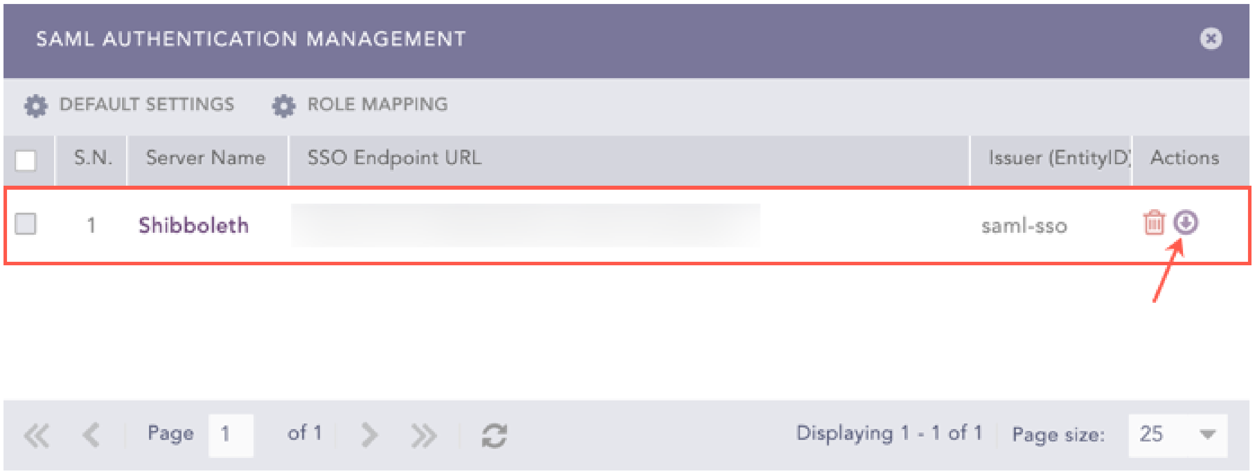


Default Role: User Account Administrator

Fig. 7: Default Settings

4.3 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**.



□	S.N.	Server Name	SSO Endpoint URL	Issuer (EntityID)	Actions
□	1	Shibboleth	[redacted]	saml-sso	

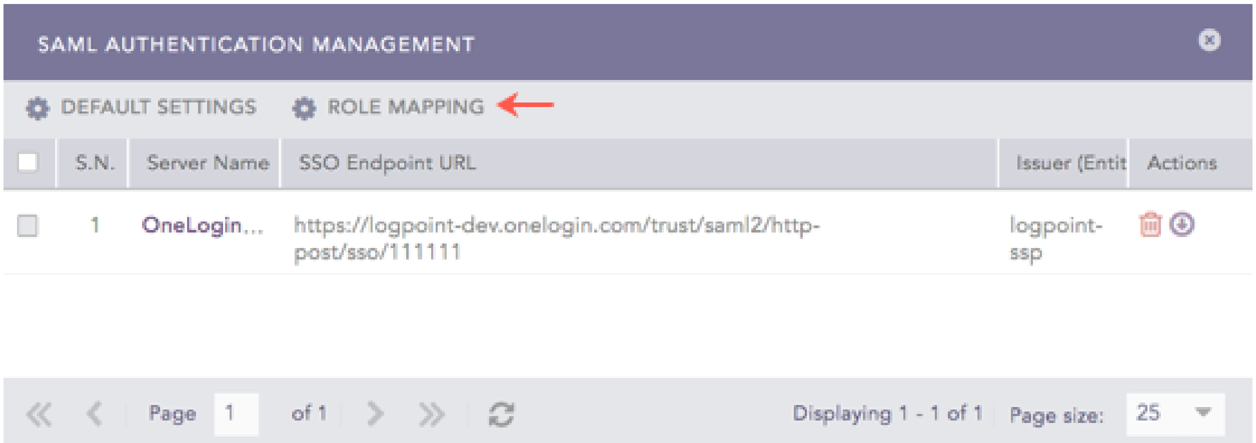
Fig. 8: Downloading Logpoint Metadata

4.4 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**.

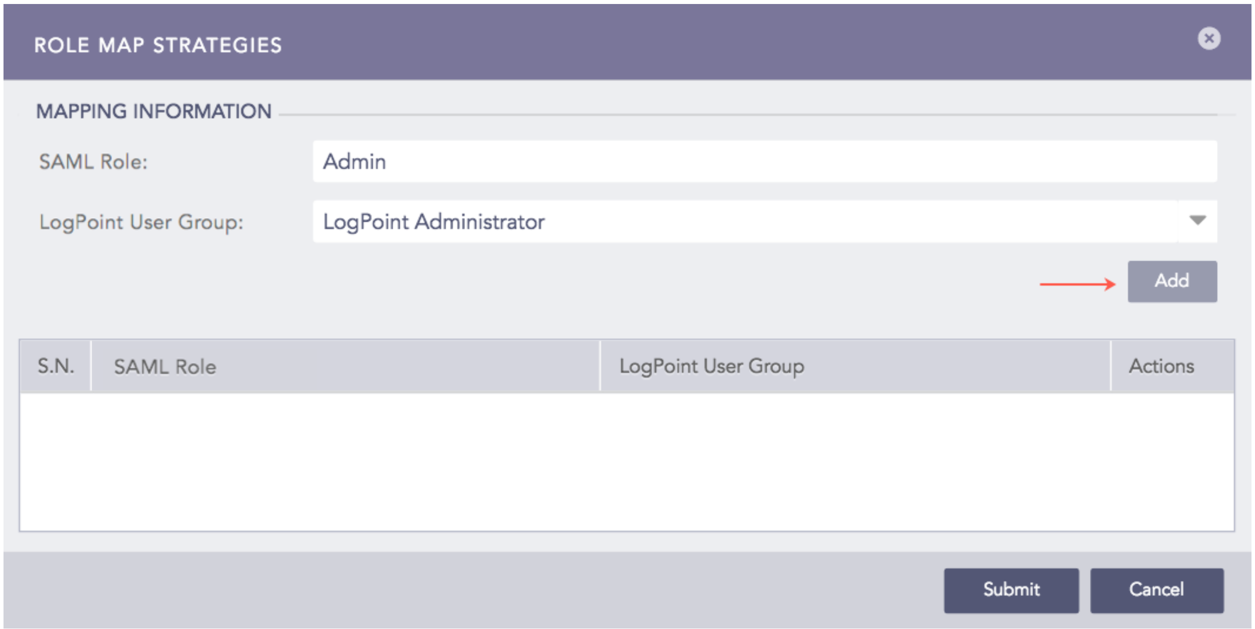


□	S.N.	Server Name	SSO Endpoint URL	Issuer (Entit	Actions
□	1	OneLogin...	https://logpoint-dev.onelogin.com/trust/saml2/http-post/sso/111111	logpoint-ssp	

Fig. 9: Role Mapping

4. Enter a **SAML Role**.

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



ROLE MAP STRATEGIES

MAPPING INFORMATION

SAML Role: Admin

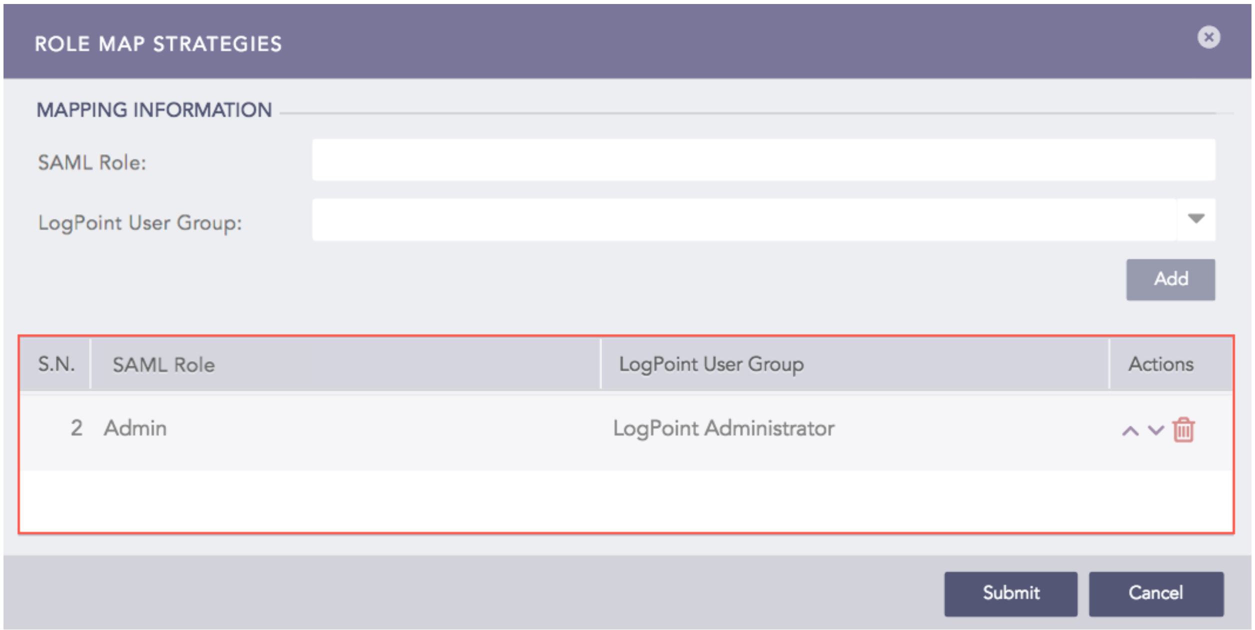
LogPoint User Group: LogPoint Administrator

S.N.	SAML Role	LogPoint User Group	Actions

Fig. 10: 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:

S.N.	SAML Role	LogPoint User Group	Actions
2	Admin	LogPoint Administrator	⌃ ⌄ 🗑

Fig. 11: SAML Roles

6. Click **Submit**.

CHAPTER

FIVE

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 in to Logpoint using the IdP server credentials. Otherwise, Logpoint opens the default login page of Logpoint Authentication.

To log in to Logpoint using SAML Authentication:

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

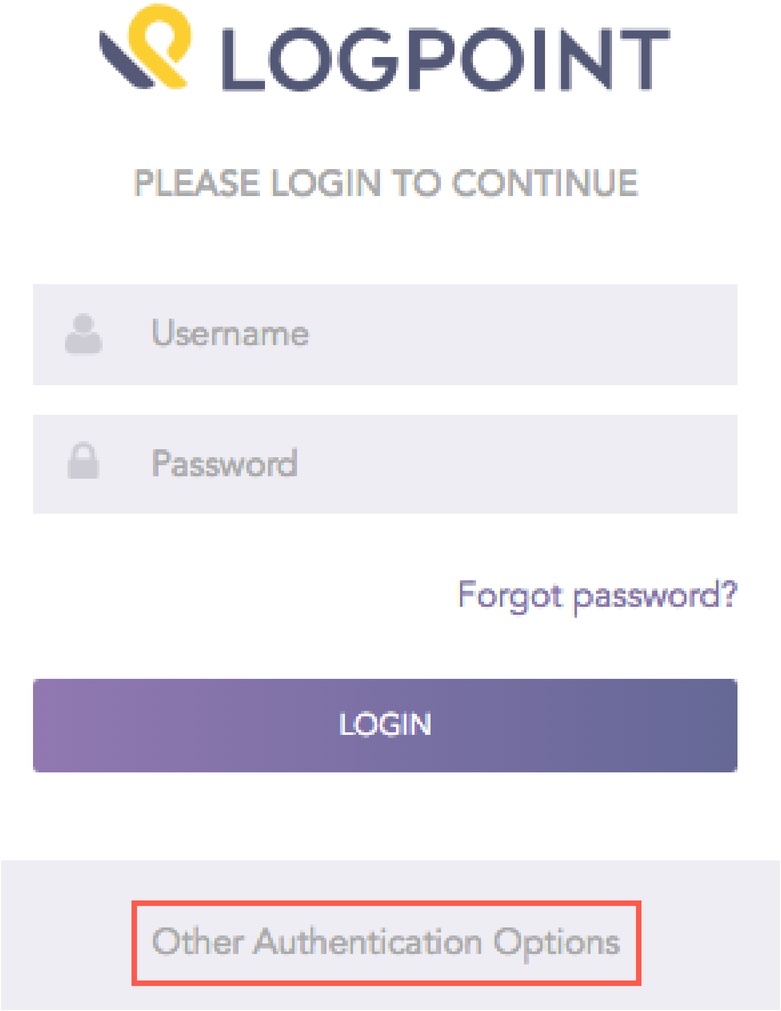


Fig. 1: Other Authentication Options

2. Select **SAML Authentication**.

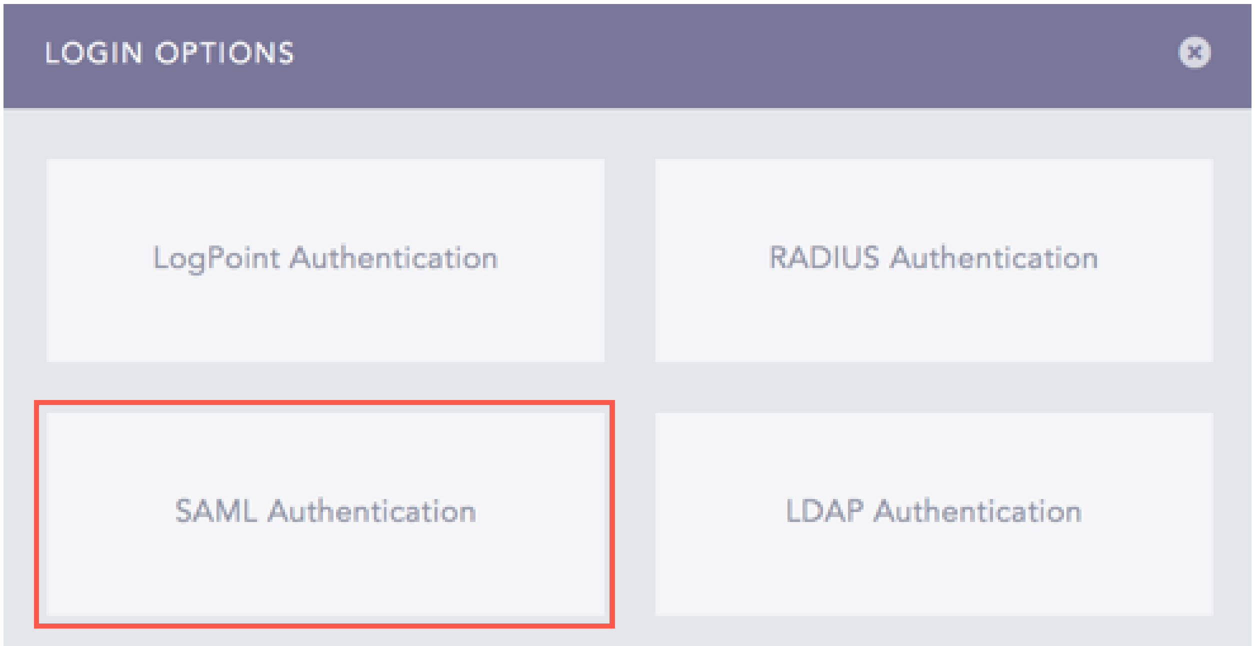


Fig. 2: Login Options

3. Click **Login**.

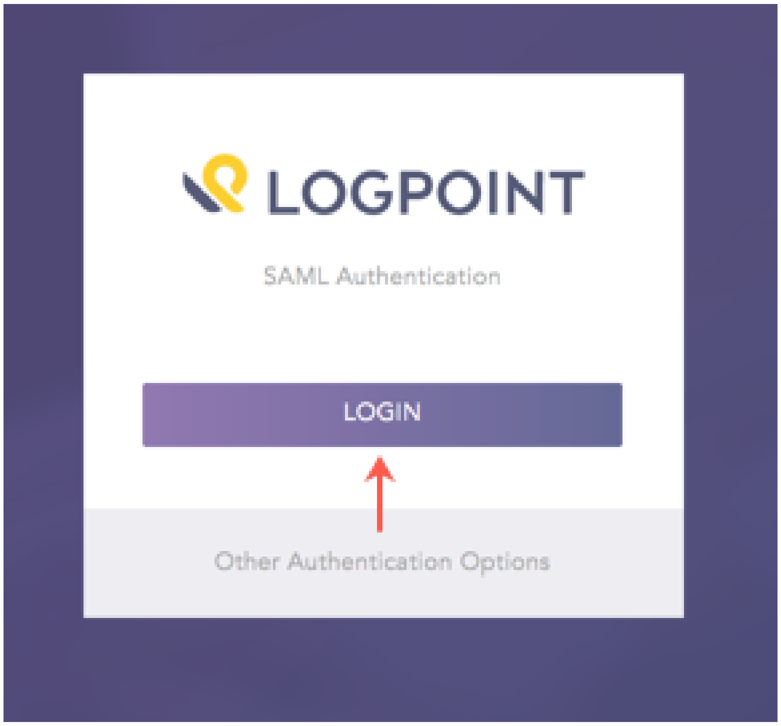
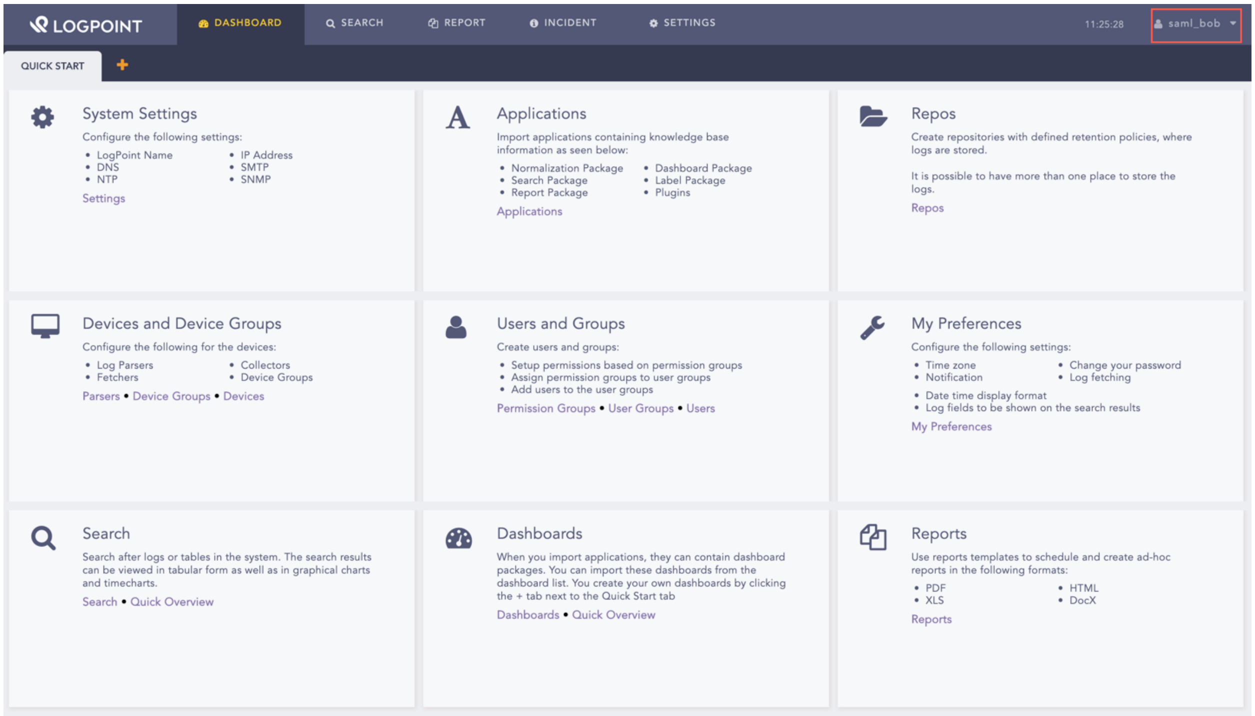


Fig. 3: SAML Authentication

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 "bob" with SAML Authentication, Logpoint updates your username to "saml_bob."



System Settings

Configure the following settings:

- LogPoint Name
- DNS
- NTP
- IP Address
- SMTP
- SNMP

Settings

Applications

Import applications containing knowledge base information as seen below:

- Normalization Package
- Search Package
- Report Package
- Dashboard Package
- Label Package
- Plugins

Applications

Repos

Create repositories with defined retention policies, where logs are stored.

It is possible to have more than one place to store the logs.

Repos

Devices and Device Groups

Configure the following for the devices:

- Log Parsers
- Fetchers
- Collectors
- Device Groups

Parsers • Device Groups • Devices

Users and Groups

Create users and groups:

- Setup permissions based on permission groups
- Assign permission groups to user groups
- Add users to the user groups

Permission Groups • User Groups • Users

My Preferences

Configure the following settings:

- Time zone
- Notification
- Change your password
- Log fetching
- Date time display format
- Log fields to be shown on the search results

My Preferences

Search

Search after logs or tables in the system. The search results can be viewed in tabular form as well as in graphical charts and timecharts.

Search • Quick Overview

Dashboards

When you import applications, they can contain dashboard packages. You can import these dashboards from the dashboard list. You create your own dashboards by clicking the + tab next to the Quick Start tab

Dashboards • Quick Overview

Reports

Use reports templates to schedule and create ad-hoc reports in the following formats:

- PDF
- XLS
- HTML
- DocX

Reports

Fig. 4: User Logged in with SAML Authentication

CHAPTER

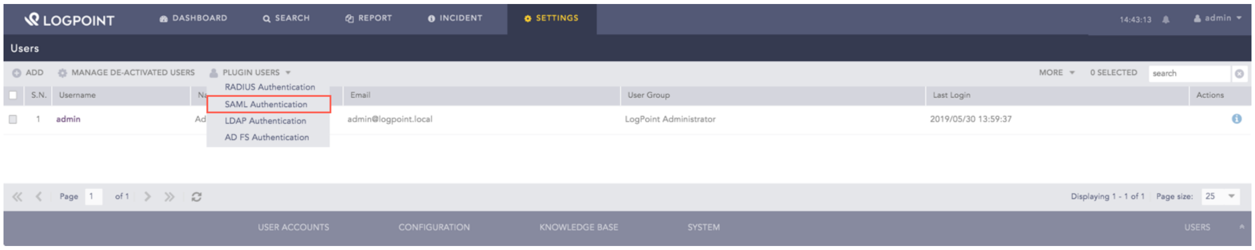
SIX

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:

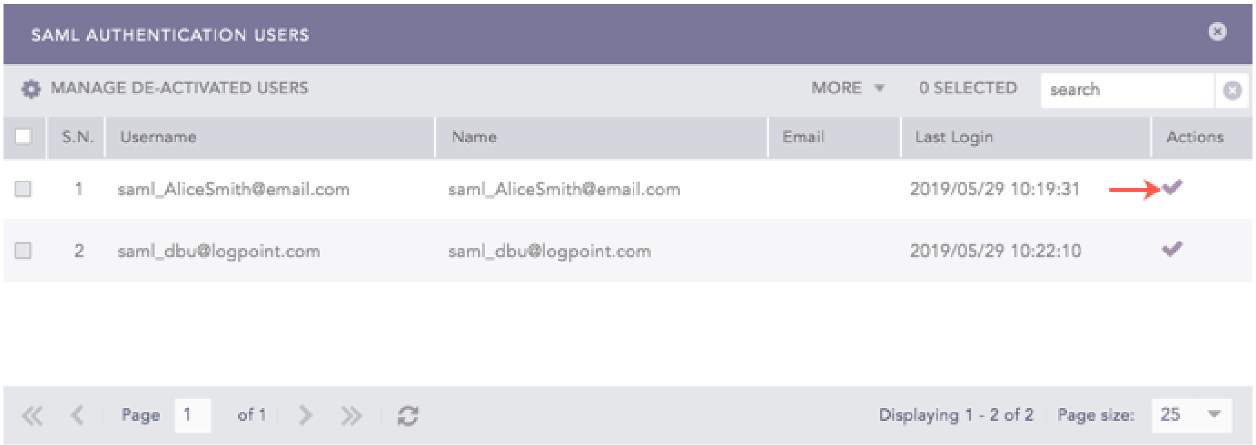
1. Go to *Settings >> User Accounts*.
2. Click **Users**.
3. In **Plugin Users**, click **SAML Authentication**. It lists all the SAML Authentication users who have logged into Logpoint.



□	S.N.	Username	Na	Email	User Group	Last Login	Actions
□	1	admin	Ad	admin@logpoint.local	LogPoint Administrator	2019/05/30 13:59:37	ⓘ

Fig. 1: Plugin Users

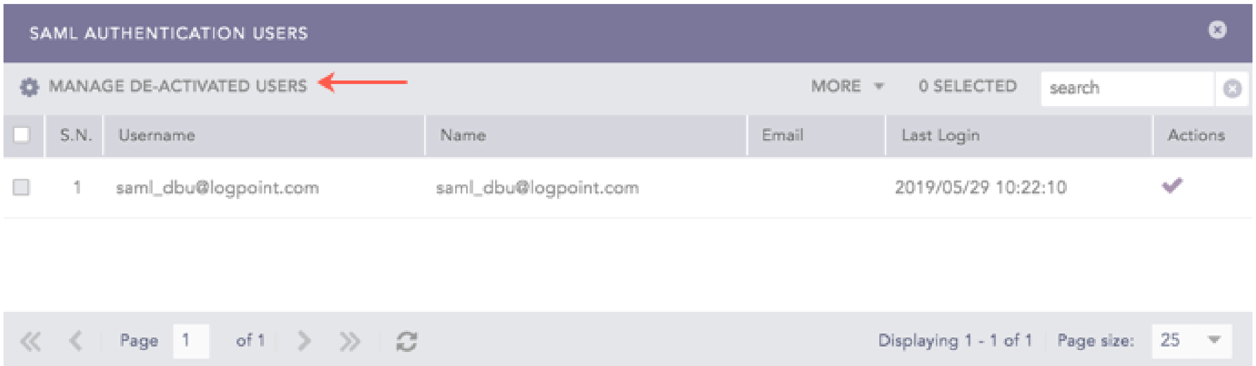
4. Click the **De-Activate User** icon in **Actions** to deactivate a user.



□	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	✓

Fig. 2: De-Activate SAML Authentication Users

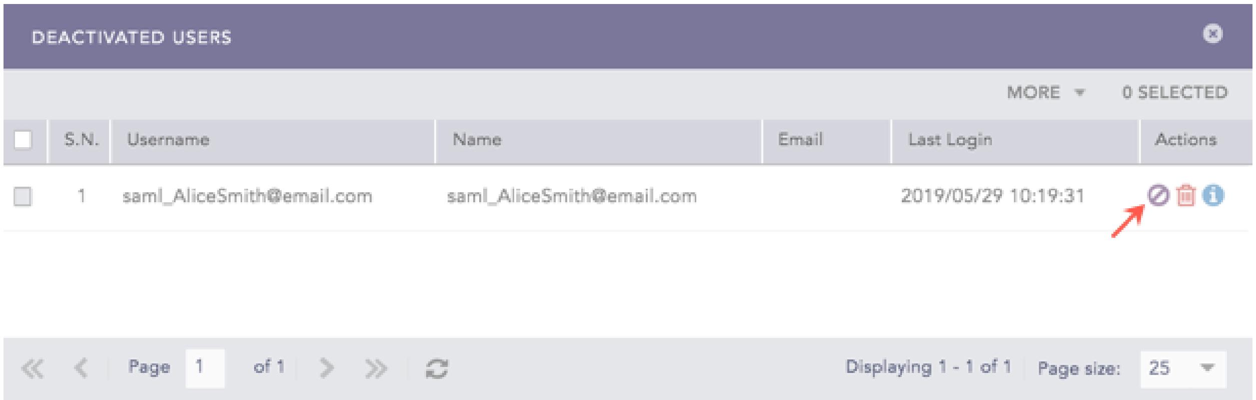
5. Click **Yes**.
6. Enter your credentials and click **Ok**.
7. Click **Manage De-Activated Users** to delete or activate the de-activated users.



□	S.N.	Username	Name	Email	Last Login	Actions
□	1	saml_dbu@logpoint.com	saml_dbu@logpoint.com		2019/05/29 10:22:10	✓

Fig. 3: Manage De-Activated SAML Authentication Users

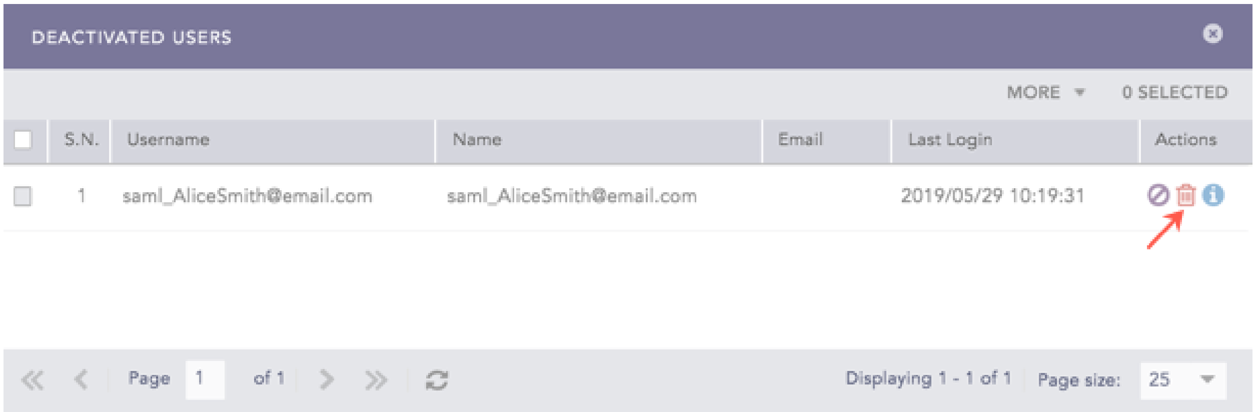
8. Click the **Activate** icon or the **Delete** icon to activate or delete the de-activated user.



DEACTIVATED USERS

□	S.N.	Username	Name	Email	Last Login	Actions
□	1	saml_AliceSmith@email.com	saml_AliceSmith@email.com		2019/05/29 10:19:31	

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



DEACTIVATED USERS

□	S.N.	Username	Name	Email	Last Login	Actions
□	1	saml_AliceSmith@email.com	saml_AliceSmith@email.com		2019/05/29 10:19:31	

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

CHAPTER

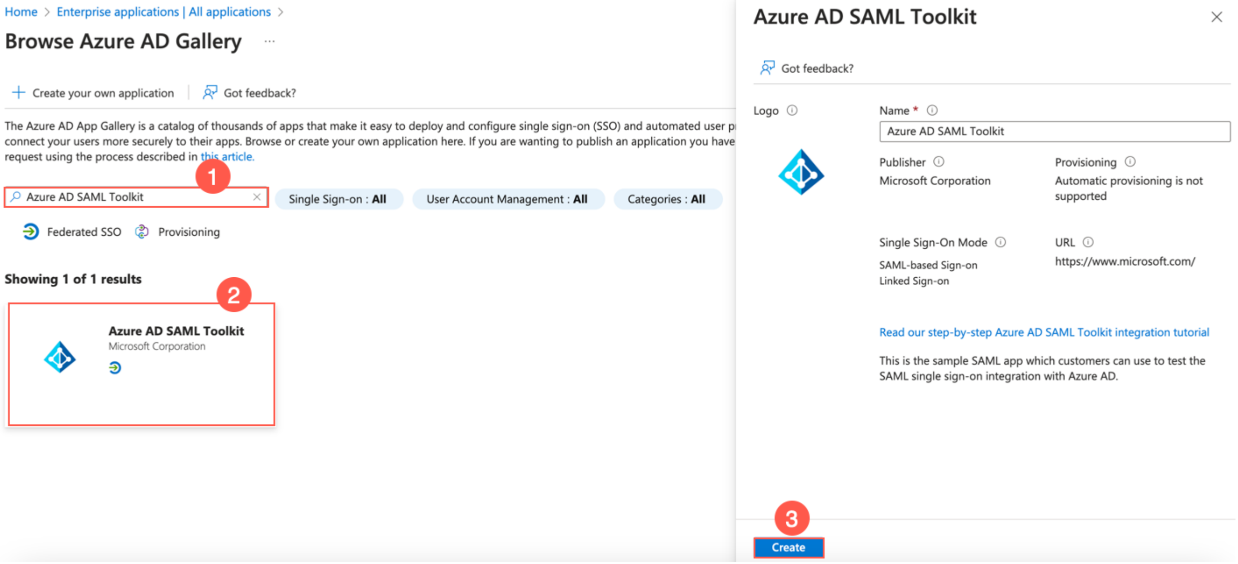
SEVEN

APPENDIX

To implement *Azure Active Directory* using *SAML*, first do the following configurations in Microsoft Azure Portal and then *configure* SAML Authentication in Logpoint.

7.1 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**.



The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user p
connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have
request using the process described in this article.

Azure AD SAML Toolkit

Showing 1 of 1 results

Name * : Azure AD SAML Toolkit

Publisher: Microsoft Corporation

Provisioning: Automatic provisioning is not supported

Single Sign-On Mode: SAML-based Sign-on, Linked Sign-on

URL: https://www.microsoft.com/

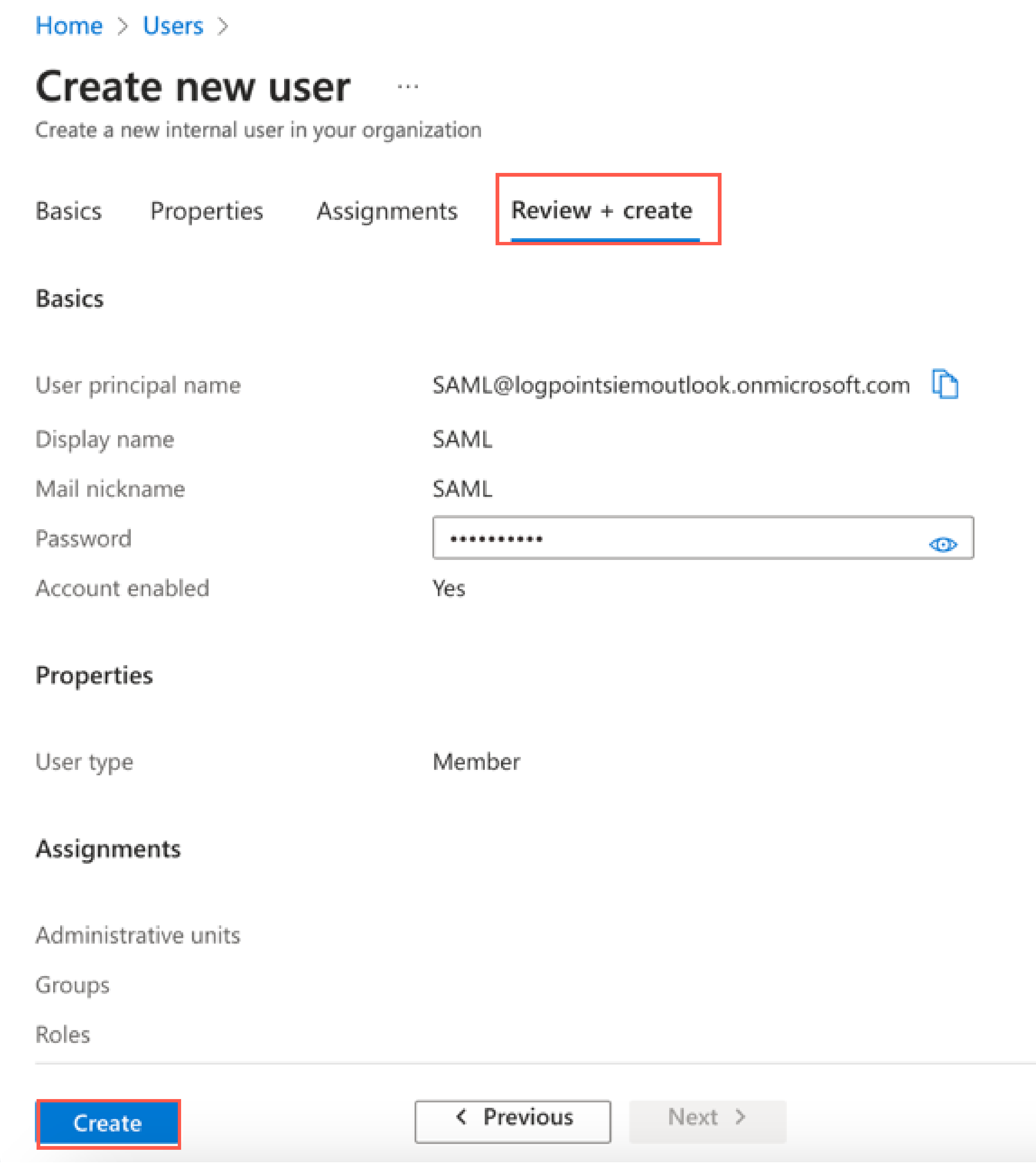
Read our step-by-step Azure AD SAML Toolkit integration tutorial

This is the sample SAML app which customers can use to test the SAML single sign-on integration with Azure AD.

Fig. 1: Adding Azure AD SAML Toolkit

7.2 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**.



Create new user

Create a new internal user in your organization

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

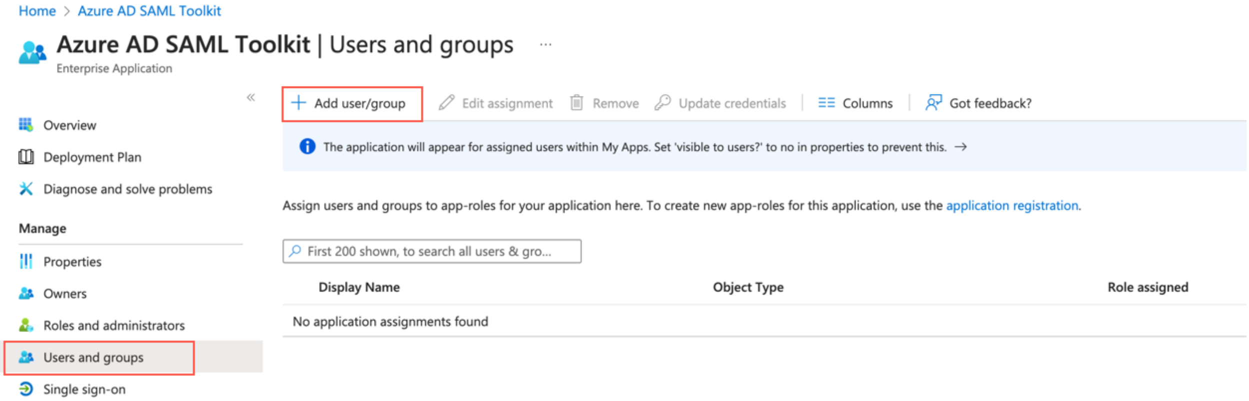
Groups

Roles

Fig. 2: Creating a New User

7.3 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**.



The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

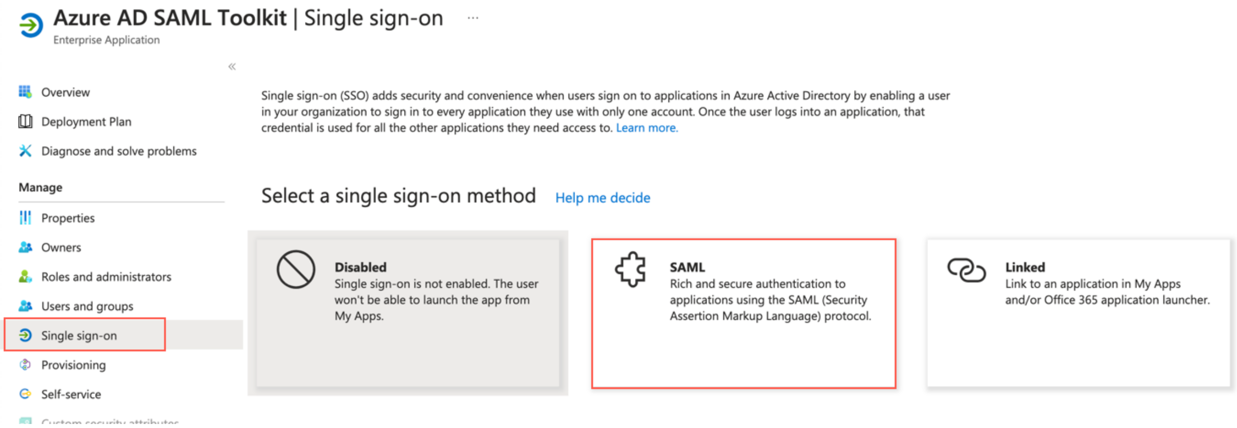
Display Name	Object Type	Role assigned
No application assignments found		

Fig. 3: Adding User/Group

4. Click **None selected** of 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**.

7.4 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**.



Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

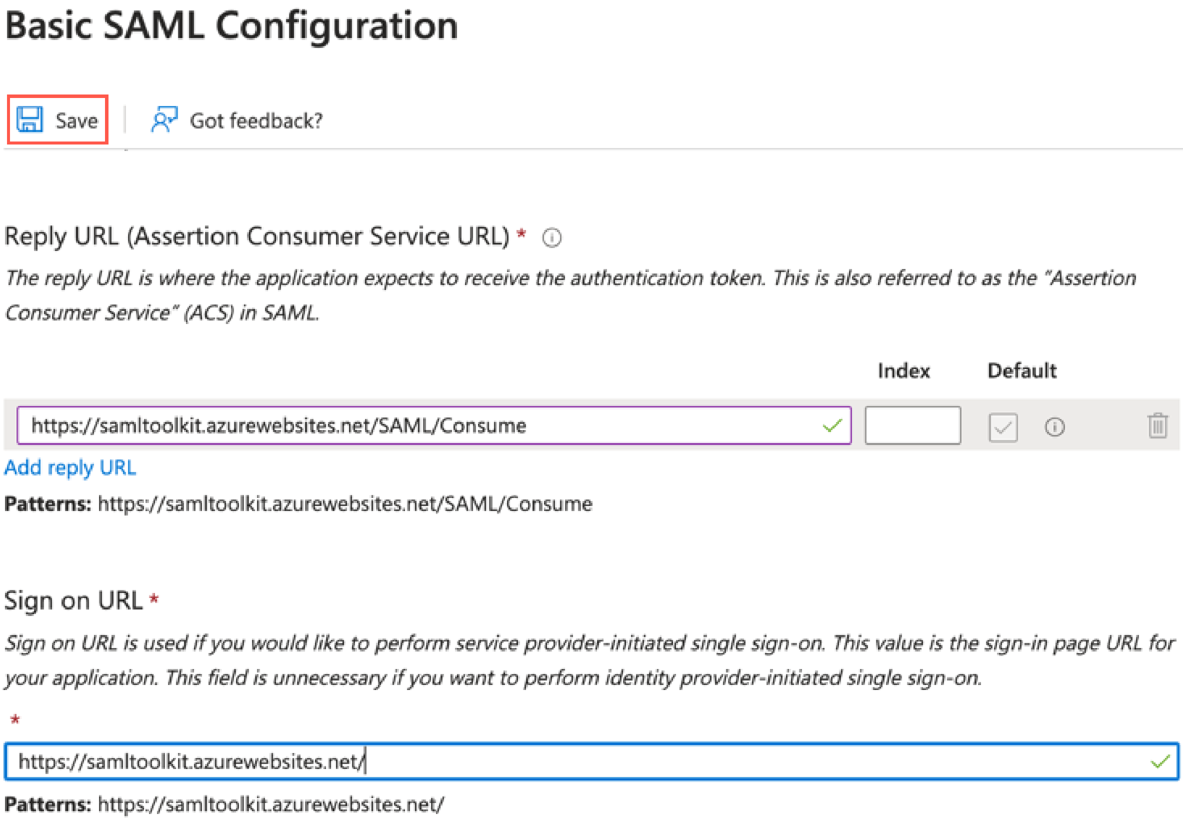
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

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**.



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.

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

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.

*

https://samltoolkit.azurewebsites.net/

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.