

Integrations

OAuthAuthentication

V6.0.1

CONTENTS

1 OAuth Authentication	1
2 Installing OAuth Authentication	2
3 Uninstalling OAuth Authentication	3
4 Configuring the OAuth Authentication	4
4.1 Configuring Default Settings	6
4.2 Mapping Roles	6
5 Login using OAuth Authentication	8
6 Manage OAuth Authentication Users	9

OAUTH AUTHENTICATION

OAuth Authentication enables you to log into Logpoint using *OAuth 2.0*. It uses authorization tokens to allow authenticated access to servers and systems.

INSTALLING OAUTH AUTHENTICATION

Prerequisite

Logpoint v7.6.0 or later.

To install OAuth Authentication:

1. Download the .pak file from the [Service Desk](#).
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 OAuth Authentication, you can find it under *Settings >> System Settings >> Plugins*.

UNINSTALLING OAUTH AUTHENTICATION

You must first remove OAuth Authentication configurations from Logpoint and then uninstall it.

To remove OAuth Authentication configurations:

1. Go to *Settings >> Configuration* from the navigation bar and click **Plugins**.
2. Click **Manage** of OAuth Authentication.
3. Click the **Delete** (🗑️) icon under **Actions**.

To uninstall OAuth Authentication:

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

CONFIGURING THE OAUTH AUTHENTICATION

1. Go to *Settings >> System Settings* from the navigation bar and click **Plugins**.
2. Search for OAuth Authentication and click **Manage**.
3. Click **ADD SERVER**.
4. Enter **Server Name**.
5. Enter the **Client Id**. It is the ID provided by *OAuth* to the registered clients.
6. Enter the **Client Secret**. It is a secret password created for *OAuth*.
7. Enter the OAuth **Authorization Endpoint**, **Token Endpoint** and **User Info Endpoint**.
8. Enter the **Redirect URL**. It is the Logpoint URL where *OAuth* redirects after verifying the access token and users information.
9. Enter the **Role Field**. It is used to extract roles from the *OAuth* response.

×

OAUTH SERVER INFORMATION

OAUTH SERVER

Server Name

Server

Client Id

123456

Client Secret

.....

Show

Authorization Endpoint

https://login.microsoftonline.com/xxx/oauth2/v2.0/authorize

Token Endpoint

https://login.microsoftonline.com/xxxxx/oauth2/v2.0/token

User Info Endpoint

https://xxmicrosoft.com/oidc/userinfo

Redirect URL

https://xxxx/pluggables/Authentication/OAuthAuthentication/login

Role Field

admin

Save

Cancel

Fig. 1: Configuring OAuth

10. Click **Save**.
11. Select a Logpoint user group as the **Default Role**. OAuth Authentication assigns the default user group to the OAuth users whose role are not mapped in the *Mapping Roles*.
12. Click **Save**. You can change the default settings from *Configuring Default Settings*.
13. Click **Yes** to select OAuth Authentication as the default authentication.

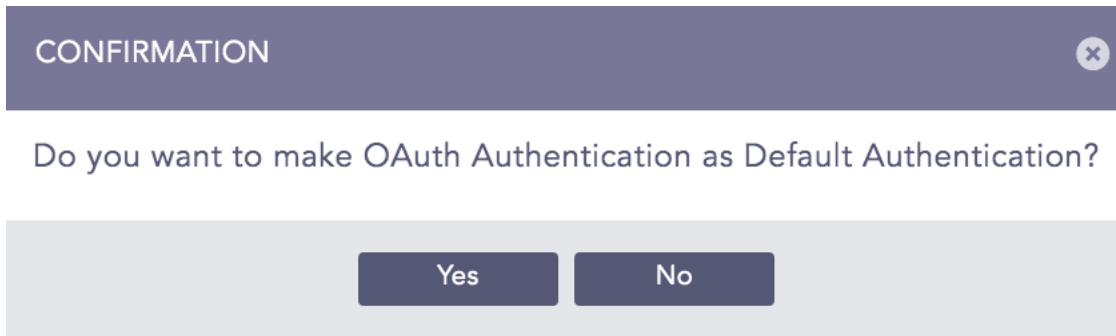


Fig. 2: OAuth Confirmation

Once you add an OAuth server, **OAuth Authentication Management** removes **Add Server** and includes **Roles Mapping**.

4.1 Configuring Default Settings

1. Click **Default Settings** in **OAuth Authentication Management**.
2. Select a Logpoint user group as the **Default Role**.

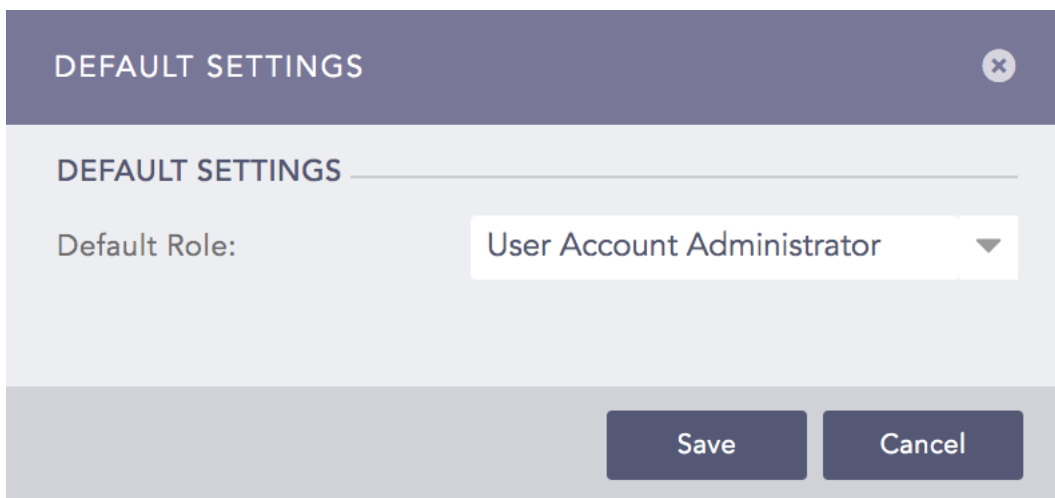


Fig. 3: Default Settings

3. Click **Save**.

4.2 Mapping Roles

You can map an OAuth role to a Logpoint user group to define access permission in Logpoint. You can map an OAuth role to one Logpoint user group only.

1. Click **Roles Mapping** in **OAuth Authentication Management**.
2. Enter an **OAuth Role**.
3. Select a **Logpoint User Group** to assign to the OAuth role.
4. Click **Add**.

ROLE MAP STRATEGIES

MAPPING INFORMATION

OAuth Role:

LogPoint User Group:

Add

S.N.	OAuth Role	LogPoint User Group	Actions
1	Admin	User Account Administrator	^ v

Submit

Cancel

Fig. 4: OAuth Role Mapping Added

LOGIN USING OAUTH AUTHENTICATION

Logpoint redirects you to the login page of the authorization server if you have selected OAuth Authentication as the default authentication. You can log in using the *OAuth* credentials. Otherwise, Logpoint opens the default login page of Logpoint Authentication.

To log into Logpoint using OAuth Authentication:

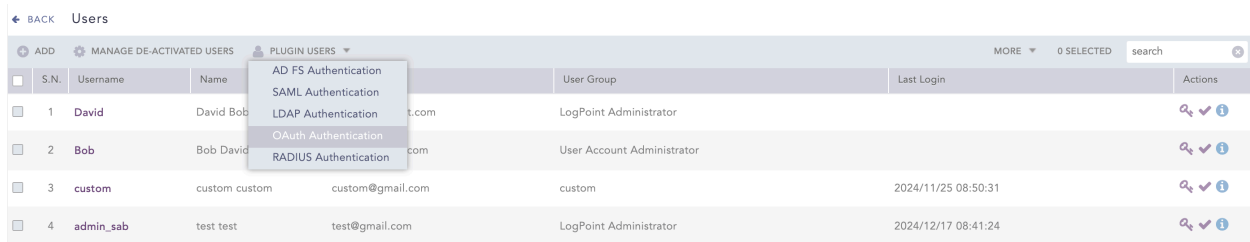
1. On the login page, click **Other Authentication Options**.
2. Select **OAuth Authentication**.
3. Log into Logpoint using the authorization server credentials. Once you log in with the authorization server credentials, Logpoint adds "*oauth_*" as a prefix to your username. For example, if you log in as "*bob*", Logpoint updates your username to "*oauth_bob*".

MANAGE OAUTH AUTHENTICATION USERS

Logpoint users with User Account Administrator and Logpoint Administrator access can manage OAuth users.

To manage OAuth users:

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



The screenshot shows a web interface for managing users. At the top, there's a navigation bar with 'BACK' and 'Users'. Below it, a toolbar contains 'ADD', 'MANAGE DE-ACTIVATED USERS', and a dropdown menu for 'PLUGIN USERS'. The dropdown menu is open, showing options: 'AD FS Authentication', 'SAML Authentication', 'LDAP Authentication', 'OAuth Authentication' (which is highlighted), and 'RADIUS Authentication'. Below the dropdown is a table with columns: S.N., Username, Name, User Group, Last Login, and Actions. The table lists four users: David, Bob, custom, and admin_sab.

S.N.	Username	Name	User Group	Last Login	Actions
1	David	David Bob	LogPoint Administrator		
2	Bob	Bob David	User Account Administrator		
3	custom	custom custom	custom	2024/11/25 08:50:31	
4	admin_sab	test test	LogPoint Administrator	2024/12/17 08:41:24	

Fig. 1: Plugin Users

3. Click the **De-Activate User** icon in **Actions** to deactivate a user.
4. Click **Yes**.
5. Enter your credentials and click **Ok**.
6. Click **Manage De-Activated Users**.
7. Click the **Activate User** or **Delete** icon to activate or delete the deactivated user.