

Integrations

OAuthAuthentication

V5.2.0

CONTENTS

1 OAuth Authentication Application	1
2 Installing the Application	2
2.1 Prerequisite	2
2.2 Installing the OAuth Authentication Application in LogPoint	2
2.3 Verifying the Installation	2
3 Configuring the Application	4
3.1 Configuring the OAuth Authentication	4
4 Login with OAuth Authentication	10
4.1 Logging in using OAuth Authentication in LogPoint	10
5 Manage OAuth Authentication Users	13
5.1 Managing OAuth Authentication Users	13
6 Uninstalling the Application	15
6.1 Uninstalling the OAuth Authentication Application in LogPoint	15

OAuth AUTHENTICATION APPLICATION

The OAuth Authentication application enables you to log into LogPoint using OAuth 2.0. The application uses authorization tokens to allow authenticated access to servers and applications.

INSTALLING THE APPLICATION

2.1 Prerequisite

LogPoint v6.12.0 or later

2.2 Installing the OAuth Authentication Application in LogPoint

1. Go to *Settings >> System >> Applications*.
2. Click **Import**.
3. **Browse** for the location of the downloaded pak file for the OAuth Authentication application.
4. Click **Upload**.

2.3 Verifying the Installation

1. Go to the LogPoint Login page.
2. Click **Other Authentication Options**. The panel includes the **OAuth Authentication** login option.

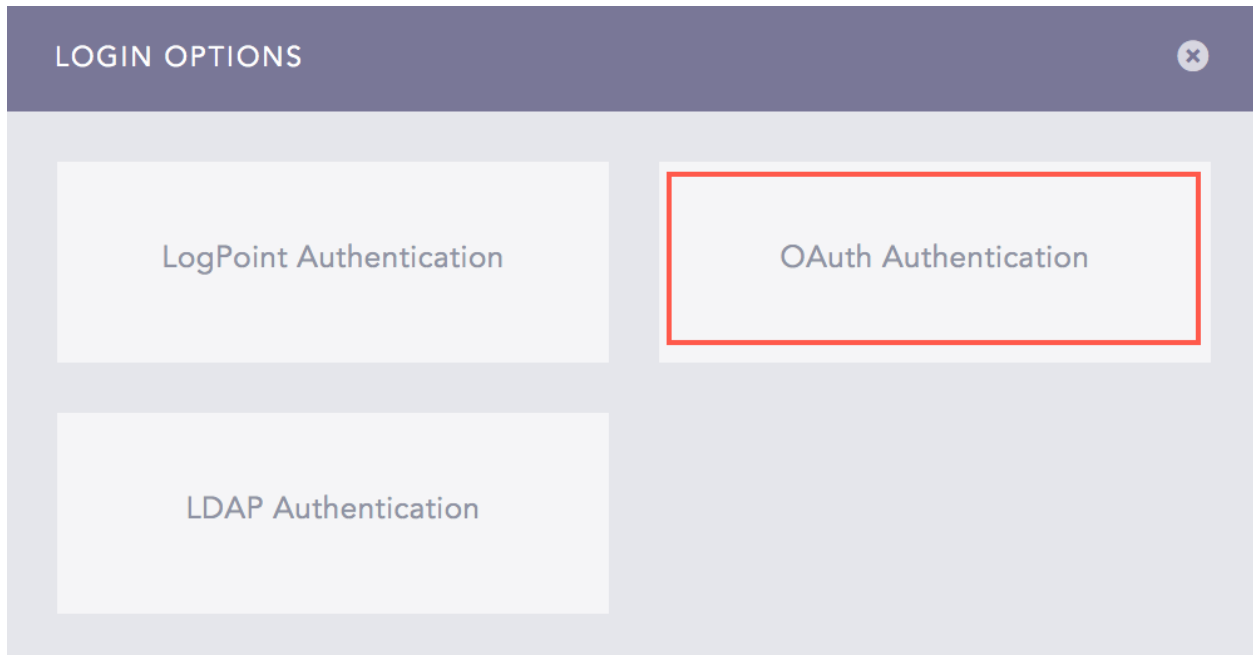


Fig. 1: OAuth Authentication Login Option

CONFIGURING THE APPLICATION

3.1 Configuring the OAuth Authentication

1. Go to *Settings >> System >> Plugins*.
2. Find **OAuth Authentication 5.2.0** and click **Manage**.

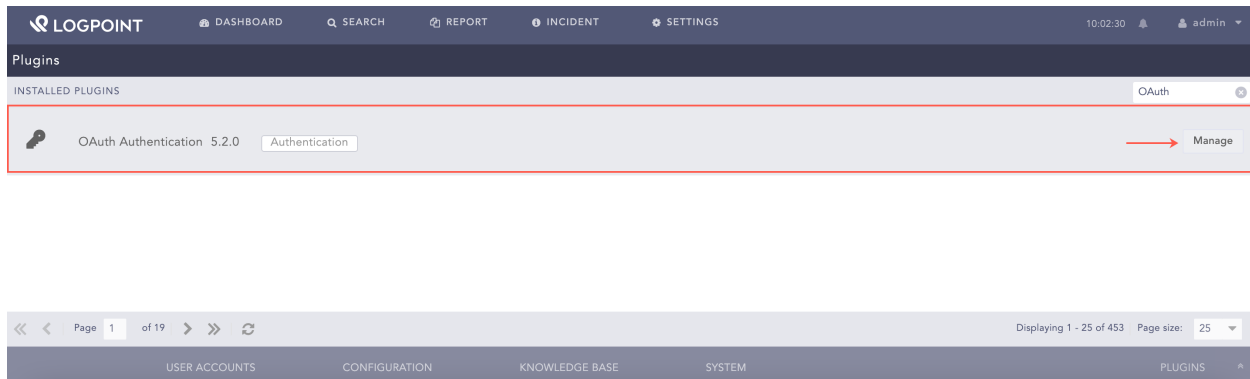


Fig. 1: Managing OAuth Authentication

3. Click **Add Server**.

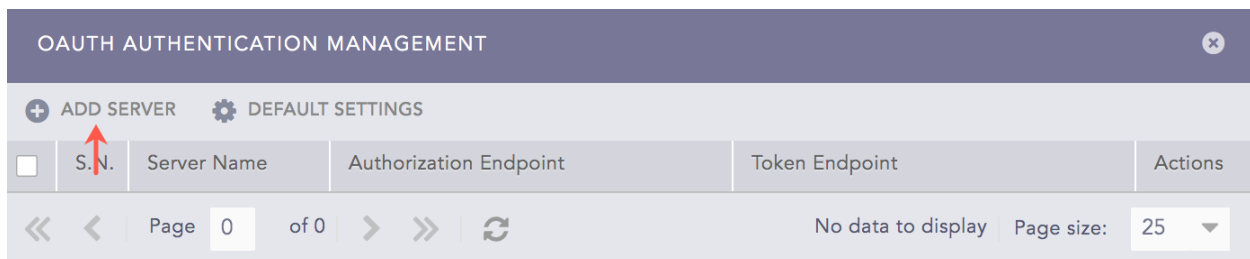


Fig. 2: Adding an OAuth Server

OAuth SERVER INFORMATION

×

OAuth SERVER

Server Name

AzureServer

Client Id

Client Secret

.....

Show

Authorization Endpoint

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

Token Endpoint

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

User Info Endpoint

https://graph.microsoft.com/oidc/userinfo

Redirect URL

https://192.168.2.3/pluggables/Authentication/OAuthAuthentication/login

Role Field

Save

Cancel

Fig. 3: OAuth Server Information Panel

4. Enter a unique **Server Name** for the authorization server.
5. Enter the **Client Id**. It is the application ID provided by the authorization server to the registered clients.
6. Enter the **Client Secret**. It is a secret password created for the application.
7. Enter the **Authorization Endpoint** of the server.
8. Enter the **Token Endpoint** of the server.

9. Enter the **User Info Endpoint** of the server.
10. Enter the **Redirect URL**. It is the LogPoint URL where the authorization server redirects after verifying the access token and users information.
11. Enter the **Role Field**. It is used to extract roles from the OAuth response.
12. Click **Save**.
13. Select a LogPoint user group as the **Default Role**. The application assigns the default user group to the OAuth users whose role are not mapped in the [Mapping Roles](#) section.
14. Click **Save**. You can change the default settings from the [Configuring Default Settings](#) section.
15. Click **Save**.
16. Click **Yes** to select OAuth Authentication as the default authentication. Otherwise, click **No**.

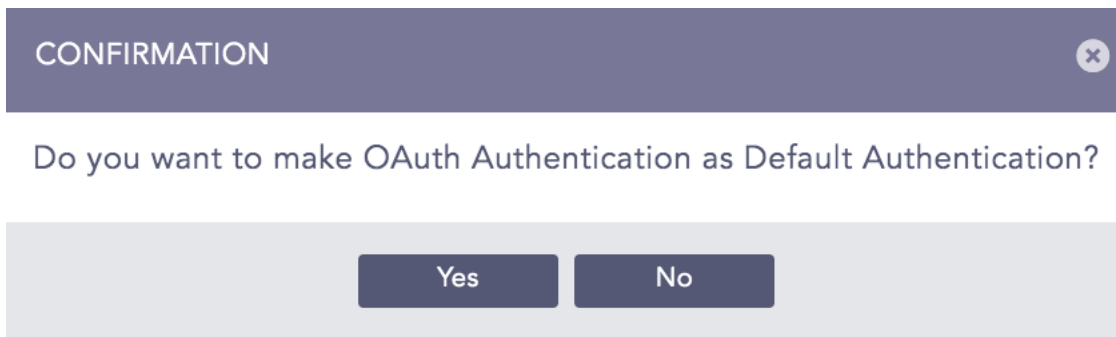


Fig. 4: OAuth Confirmation Panel

Note: Once you add an OAuth server, the **OAuth Authentication Management** panel removes the **Add Server** option and includes the **Roles Mapping** option.

3.1.1 Configuring Default Settings

1. Click **Default Settings** in the **OAuth Authentication Management** panel.

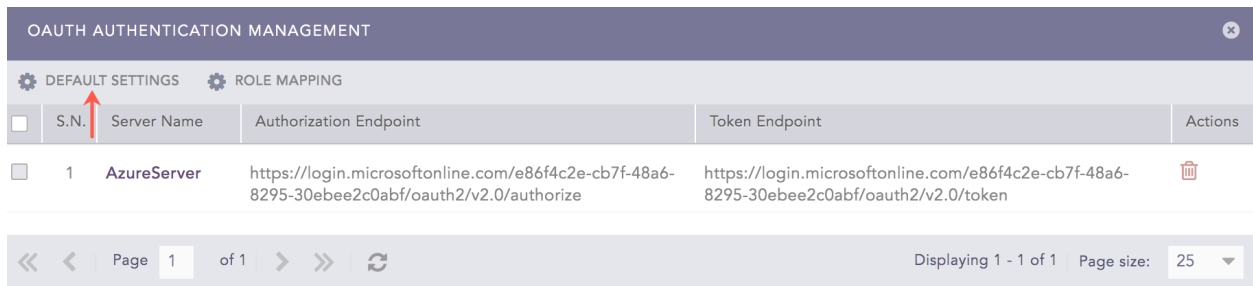


Fig. 5: OAuth Authentication Management Panel

2. Select a LogPoint user group as the **Default Role**.

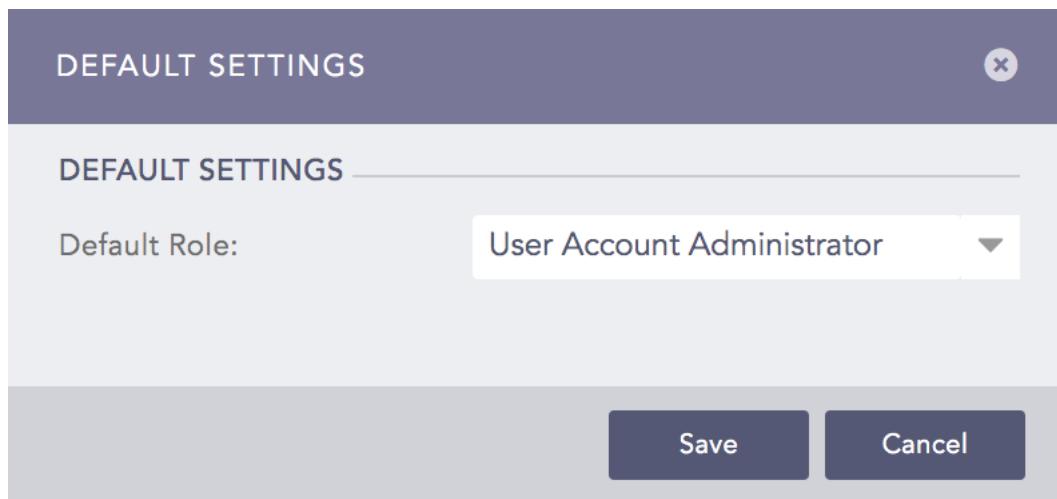


Fig. 6: Default Settings Panel

3. Click **Save**.

3.1.2 Mapping Roles

You can map an OAuth role to a LogPoint user group to define access permission in LogPoint.

Follow these steps to map an OAuth role to a LogPoint user group:

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

ROLE MAP STRATEGIES

MAPPING INFORMATION

OAuth Role:

Admin

LogPoint User Group:

User Account Administrator

Add

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

Submit

Cancel

Fig. 7: OAuth Role Mapping

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. 8: OAuth Role Mapping Added

Note: You can map an OAuth role to one LogPoint user group only.

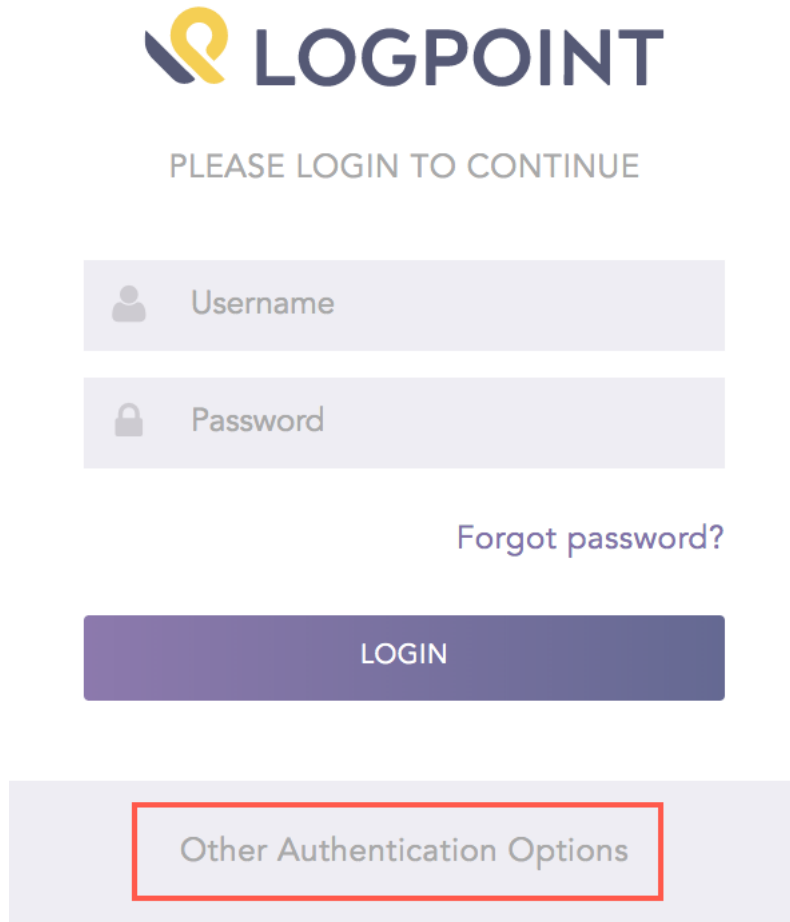
LOGIN WITH OAUTH AUTHENTICATION

4.1 Logging in using OAuth Authentication in LogPoint

If you have selected OAuth Authentication as the default authentication, LogPoint redirects you to the login page of the authorization server. You can log into LogPoint using the authorization server credentials.

Otherwise, LogPoint opens the default login page of LogPoint Authentication. Follow these steps to log into LogPoint using OAuth Authentication:

1. Click **Other Authentication Options**.



The image shows the LogPoint login interface. At the top is the LogPoint logo, which consists of a stylized yellow and blue icon followed by the word "LOGPOINT" in a bold, dark blue sans-serif font. Below the logo is the text "PLEASE LOGIN TO CONTINUE" in a light gray, all-caps sans-serif font. There are two input fields: the first is labeled "Username" with a gray user icon to its left, and the second is labeled "Password" with a gray lock icon to its left. Below these fields is a link that says "Forgot password?" in a purple, sans-serif font. Underneath the link is a dark purple rectangular button with the word "LOGIN" in white, all-caps, sans-serif font. At the bottom, there is a light gray rectangular area containing a button labeled "Other Authentication Options" in a gray, sans-serif font. This button is highlighted with a red rectangular border.

Fig. 1: 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" with the OAuth Authentication option, LogPoint updates your username to "oauth_bob".

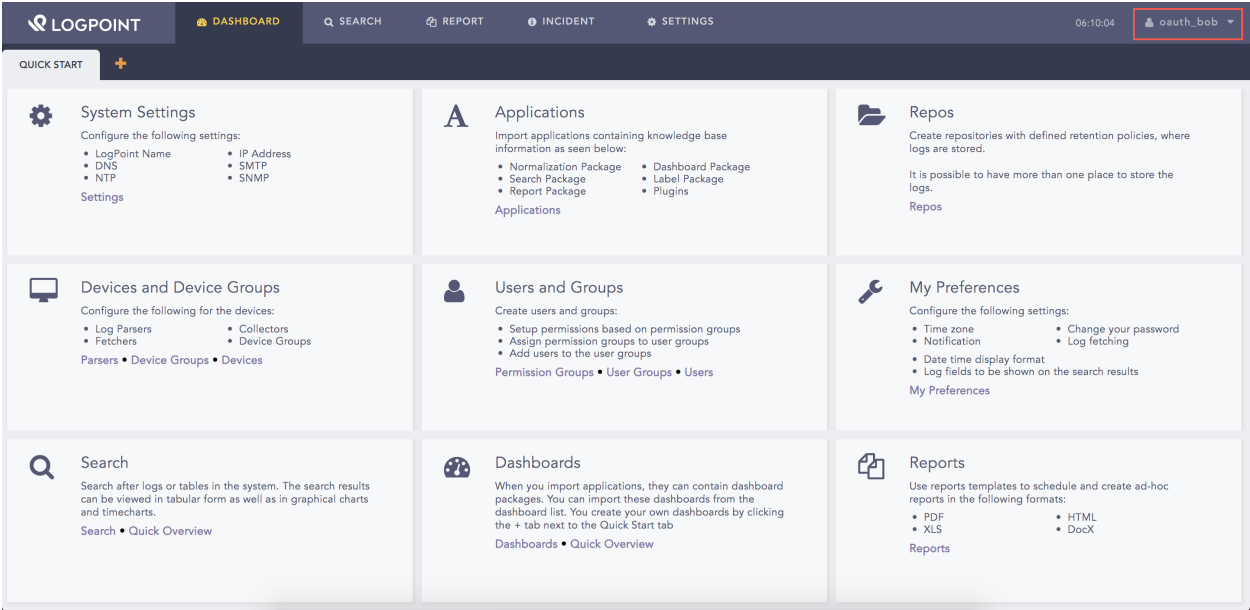


Fig. 2: User logged in with OAuth Authentication

MANAGE OAUTH AUTHENTICATION USERS

5.1 Managing OAuth Authentication Users

LogPoint users with sufficient privileges can manage OAuth users.

Follow these steps to manage OAuth users:

1. Go to *Settings >> User Accounts*.
2. Click **Users**.
3. In the **Plugin Users** drop-down, click **OAuth Authentication**. The panel enlists all the OAuth users who have logged into LogPoint.

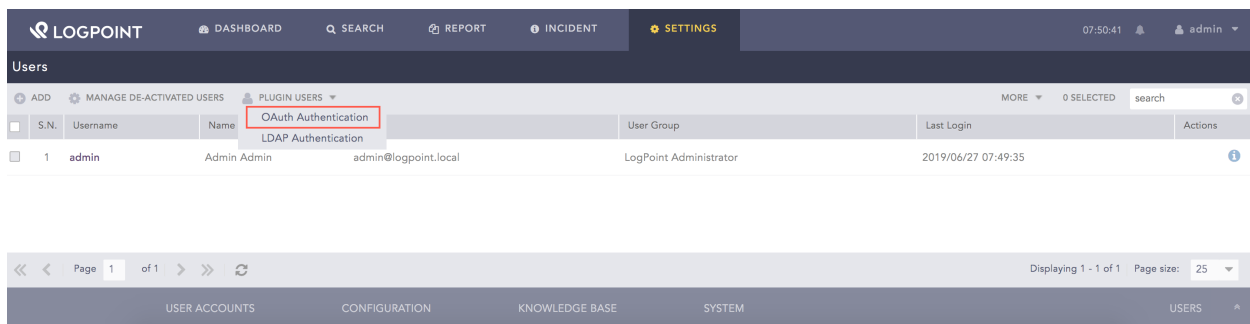


Fig. 1: Plugin Users

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

OAUTH AUTHENTICATION USERS						
MANAGE DE-ACTIVATED USERS			MORE ▾		0 SELECTED	
	S.N.	Username	Name	Email	Last Login	Actions
☐	1	oauth_bob	oauth_bob		2019/06/27 07:28:27	

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

Fig. 2: Deactivating OAuth Users

5. Click **Yes**.
6. Enter your credentials and click **Ok**.
7. Click **Manage De-Activated Users**.
8. Click the **Activate User** or **Delete** icon to activate or delete the deactivated user respectively.

DEACTIVATED USERS						
			MORE ▾		0 SELECTED	
	S.N.	Username	Name	Email	Last Login	Actions
☐	1	oauth_bob	oauth_bob		2019/06/27 07:28:27	

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

Fig. 3: Activating the Deactivated OAuth User

DEACTIVATED USERS						
			MORE ▾		0 SELECTED	
	S.N.	Username	Name	Email	Last Login	Actions
☐	1	oauth_bob	oauth_bob		2019/06/27 07:28:27	

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

Fig. 4: Deleting the Deactivated OAuth User

UNINSTALLING THE APPLICATION

6.1 Uninstalling the OAuth Authentication Application in LogPoint

1. Go to *Settings >> System >> Applications*.
2. Click the **Uninstall**  icon from the **Actions** column.

Note: You must remove the OAuth Authentication configuration to delete the application.
