

Contents

Overview

[Video Setup Guide](#)

[Features](#)

[Download Module](#)

1. Setup Drupal as OAuth Client

2. Setup Azure AD as an OAuth Provider

3. Integrating Drupal with Azure AD

4. Test Configuration of Drupal with Azure AD

[Premium Features/Settings](#)

[24*7 Active Support](#)

[Additional Resources](#)

[Our Other modules](#)

[Drupal OAuth / OpenID Single Sign On](#) / [Features and Module Pricing](#) / [Drupal OAuth / OpenID Providers](#)

Azure AD SSO Login with Drupal OAuth Client | Drupal SSO Login

Drupal Azure AD SSO integration will allow you to configure Single Sign-On (SSO) login between your Drupal site and Azure AD using OAuth/OpenID protocol. [Drupal OAuth 2.0/OpenID connect module](#) gives the ability to enable login using OAuth 2.0/OIDC Single Sign-On to Drupal Site. We provide the Drupal OAuth/OpenID Client module for Drupal 7, Drupal 8, and Drupal 9.

Here we will go through a guide to configure the SSO login between Drupal and Azure AD. By following these steps, users of Azure AD will be able to log into the Drupal site using their Azure AD credentials.

If you have any queries or if you need any sort of assistance in configuring the module, you can contact us at drupalsupport@xecurify.com. If you want, we can also schedule an online meeting to help you configure the Drupal [OAuth & OpenID Connect Login – OAuth2 Client SSO Login](#) module.

Video Setup Azure AD Single Sign-on Integration with Drupal OAuth/OpenID Client

You can refer the steps to Configure Azure AD SSO integration with the Drupal OAuth/OIDC Client module from the Video or Documentation given below:



Features and Pricing

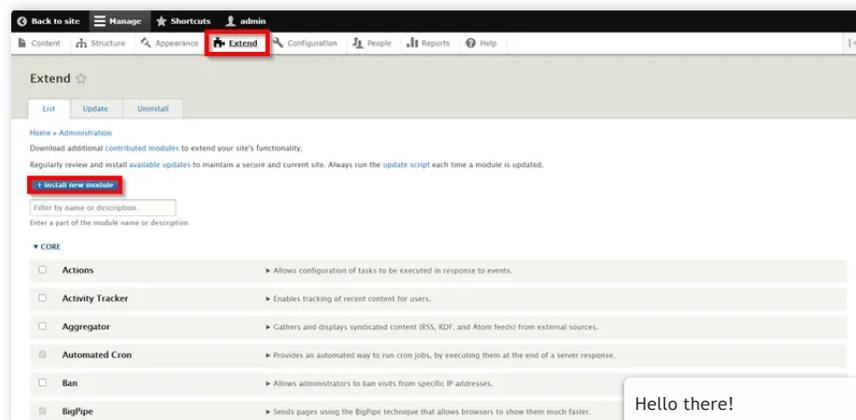
Know more about Drupal OAuth/OpenID Single Sign On from [here](#).

Pre-requisites: Download

You can download the Drupal OAuth/OpenID Single Sign On module from [here](#).

1. Setup Drupal as OAuth Client

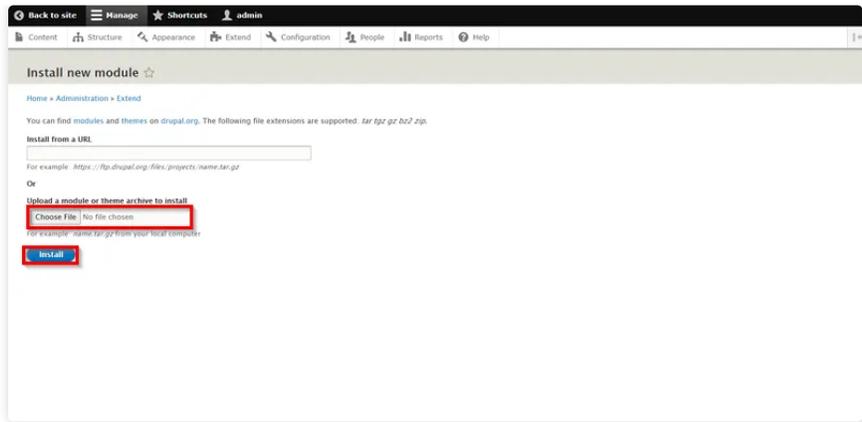
- Login in your Drupal site's admin console and click on **Extend** from the top navigation bar.
- Select the **Install new module** option to install a new module on your Drupal site.



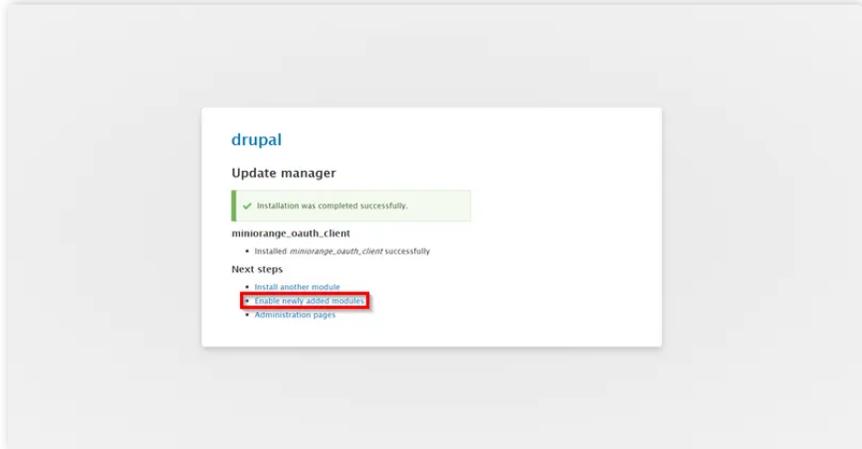
- Upload the downloaded zip file of the Module and click on the **Install** button to continue...

Hello there!
Need Help? We are right here!

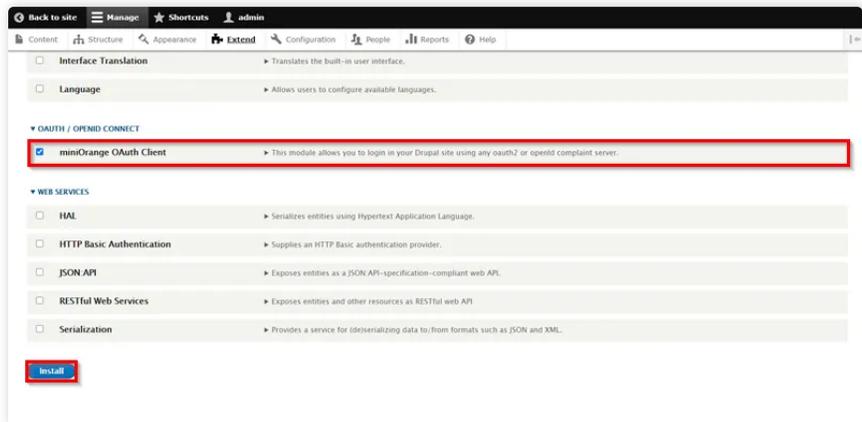




- Select **Enable newly added modules**.



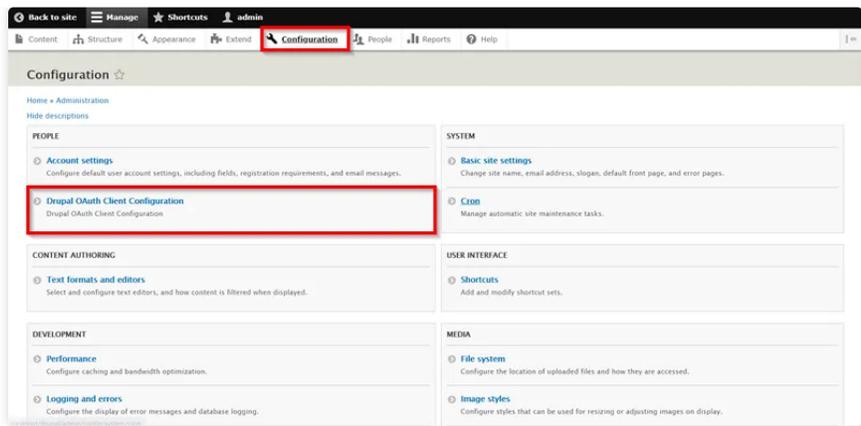
- Scroll down till you find **miniOrange OAuth Client**. Click on the checkbox next to it and click on the **Install** button to enable the module.



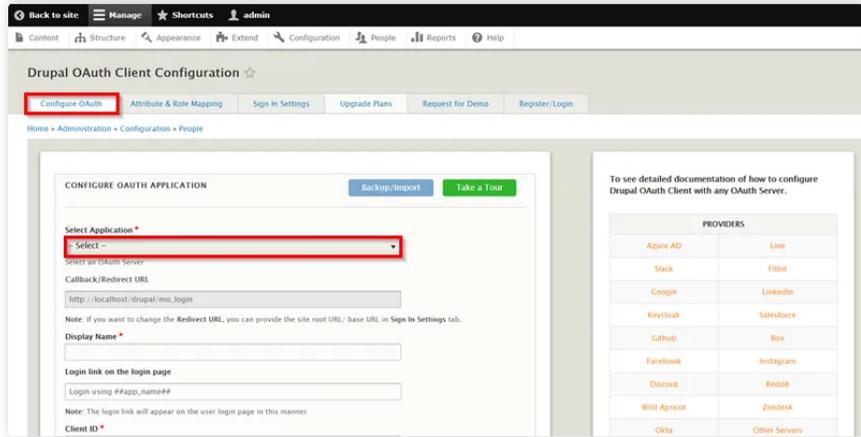
- Click on **Configuration** from the top navigation bar and Select **Drupal OAuth Client Configuration**.

Hello there!
Need Help? We are right here!



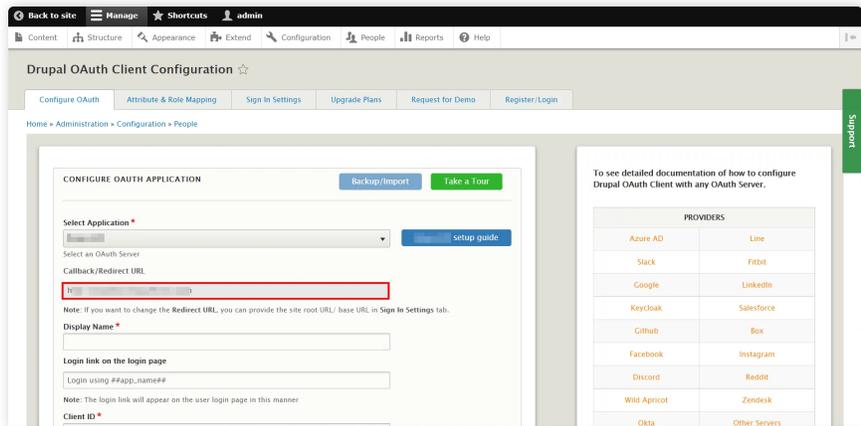


- In the **Configure OAuth** tab, select **OAuth Provider** from the Select Application dropdown.



Note: In case you do not find your OAuth Provider listed in the dropdown, please select Custom OAuth Provider and continue.

- Copy the **Callback URL** from the **Callback / Redirect URL** text field and keep it handy.

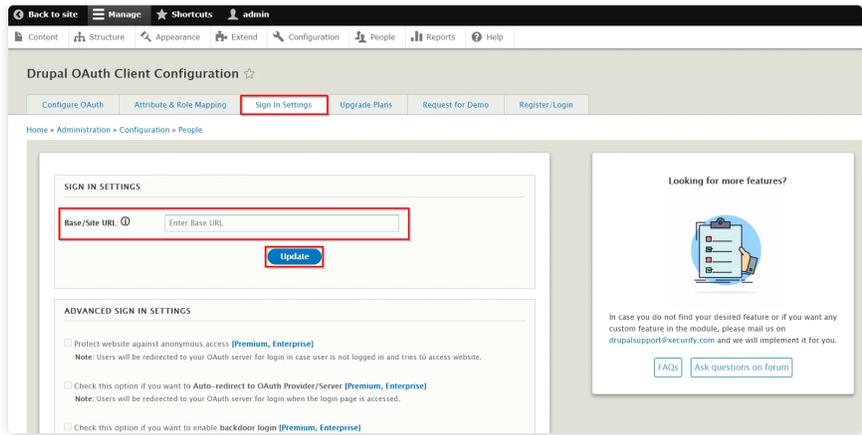


Please note: A few of the popular service providers like Azure AD, Azure B2C, Facebook etc. support only HTTPS Callback URL (However, HTTP URL will work in the case of localhost). So, currently, if your site is HTTP, you can change it to HTTPS by following the steps listed down below :

- Go to the **Sign In Settings** tab.
- In the Base /Site URL text field, enter your Drupal site's base/root URL with HTTPS (For eg. if your site is http://abc.com, you will need to save this value: https://abc.com).
- Click on the **Update** button.

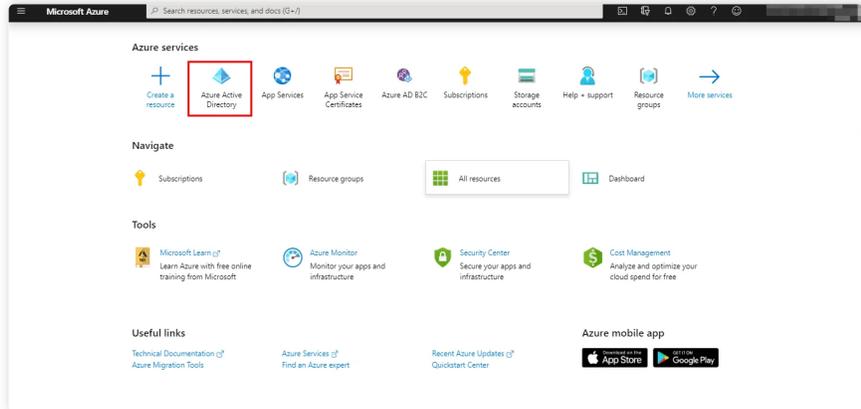
Hello there!
Need Help? We are right here!



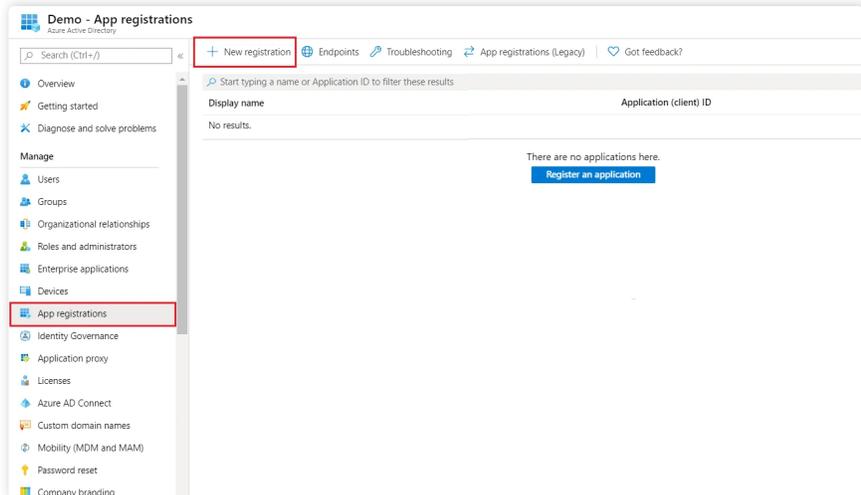


2. Setup Azure AD as an OAuth Provider

- Sign in to [Azure portal](#).
- Click on **Azure Active Directory** from **Azure services**.



- In the left-hand navigation pane, click the **App registrations** service, and click **New registration**.



- When the Create page appears, enter your application's registration information:

Name :	Name of your application.
Application type :	<ul style="list-style-type: none"> • Select "Native" for client applications that are installed locally on a device. This setting is used for OAuth public native clients • Select "Web app / API" for client applications and resource/API applications that are installed on a secure server. This setting is used for OAuth confidential web clients and the application can also expose both a client and resource/API.
Sign-on	<ul style="list-style-type: none"> • For "Web app / API" applications, provide the base URL of your app. eg, <code>https://<domain-name>/mo_logi</code>

Hello there!
Need Help? We are right here!



URL : n might be the URL for a web app running on your local machine. Users would use this URL to sign in to a web client application.

- For "Native" applications, provide the URI used by Azure AD to return token responses. Enter a value specific to your application. eg, `https://localhost/drupal`

Register an application

* Name
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (Default Directory only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

[By proceeding, you agree to the Microsoft Platform Policies](#)

3. Integrating Drupal with Azure AD

- When finished, click **Register**. Azure AD assigns a unique Application ID to your application. Copy **Application ID** and the **Directory ID**, this will be your **Client ID** and **Tenant ID** respectively.

The screenshot shows the 'TestOAuth' application registration overview in the Azure AD portal. The left-hand navigation pane includes 'Overview', 'Quickstart', 'Manage', 'Branding', 'Authentication', 'Certificates & secrets', 'Token configuration (preview)', 'API permissions', and 'Expose an API'. The main content area displays the following details:

- Display name: TestOAuth
- Supported account types: My organization only
- Application (client) ID: [Redacted]
- Redirect URIs: 1 web, 0 public client
- Directory (tenant) ID: [Redacted]
- Application ID URI: Add an Application ID URI
- Object ID: [Redacted]
- Managed application in ...: TestOAuth

- Go to **Certificates and Secrets** from the left navigaton pane and click on **New Client Secret**. Enter description and expiration time and click on **ADD** option.

Hello there!
Need Help? We are right here!



TestOAuth - Certificates & secrets

Search (Ctrl+/) <<

- Overview
- Quickstart
- Manage
 - Branding
 - Authentication
 - Certificates & secrets**
 - Token configuration (preview)
 - API permissions
 - Expose an API
 - Owners
 - Roles and administrators (Previ...
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Add a client secret

Description
Secret Key

Expires
 In 1 year
 In 2 years
 Never

Add **Cancel**

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as

+ New client secret

Description	Expires	Value
No client secrets have been created for this application.		

- Copy value. This will be your **Secret key**.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value
Secret Key	12/30/2020	[REDACTED]

- Azure AD Endpoints and scope:

Scope:	openid email profile
Authorize Endpoint:	https://login.microsoftonline.com/[tenant-id]/oauth2/v2.0/authorize
Access Token Endpoint:	https://login.microsoftonline.com/[tenant-id]/oauth2/v2.0/token
Get User Info Endpoint:	https://graph.microsoft.com/beta/me

4. Test Configuration of Drupal with Azure AD

- After successfully saving the configurations, please click on the **Test Configuration** button to test the connection between Drupal and Azure AD.

Back to site | Manage | Shortcuts | admin

Content | Structure | Appearance | Extend | Configuration | People | Reports | Help

Scope *

Scope decides the range of data that you will be getting from your OAuth Provider

Authorize Endpoint *

Access Token Endpoint *

Get User Info Endpoint *

Send Client ID and secret in: ⓘ

Header Body

Enable Login with OAuth

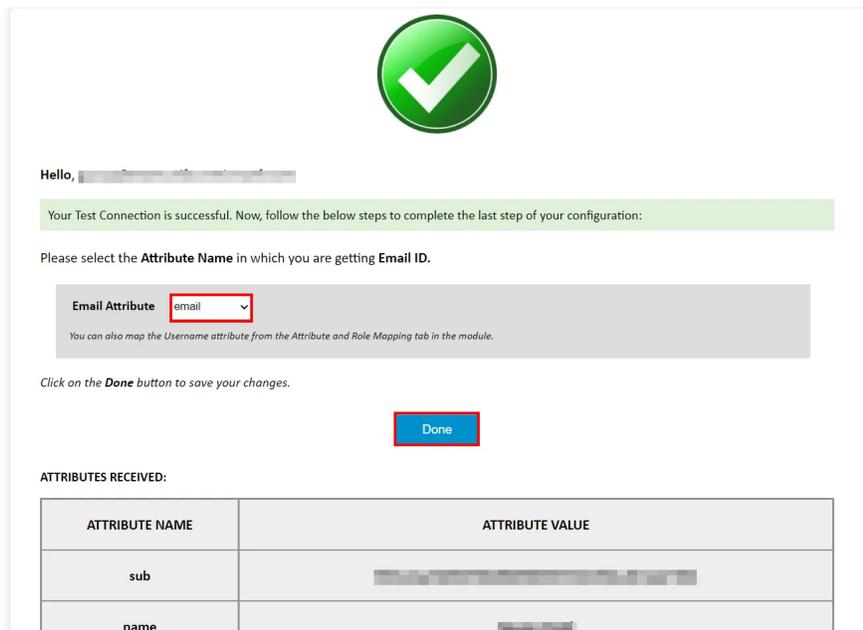
Save Configuration **Test Configuration** **Reset Configuration**

Instructions to add login link to different pages in your Drupal site:

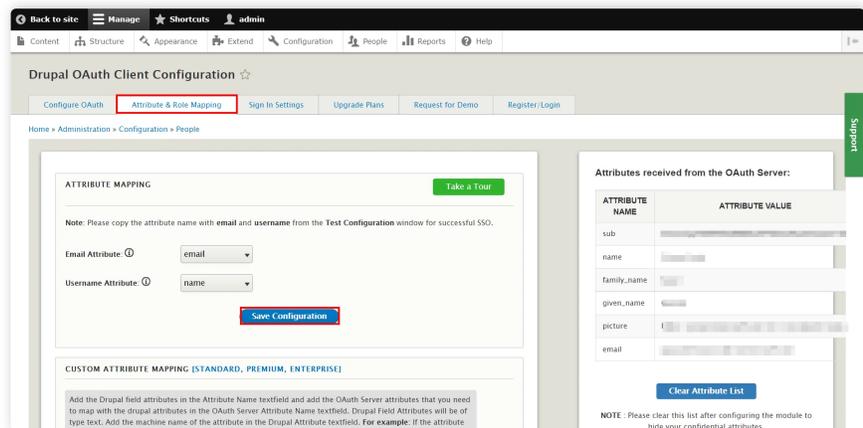
- This **Test Configuration window** will provide you with a list of the attributes that are available in the user's profile.
- Select the Email Attribute from the dropdown menu in which the user's email ID is obtained.

Hello there!
Need Help? We are right here!





- Now, in the **Attribute & Role Mapping** tab, you can also choose the Username Attribute from the dropdown and click on the **Save Configuration** button.



Please note: Mapping the Email Attribute is mandatory for your login to work.

- Now log out and go to your Drupal site's login page. You will automatically find a Login with Azure AD link there. If you want to add the SSO link to other pages as well, please follow the steps given in the image below :

Instructions to add login link to different pages in your Drupal site:

After completing your configurations, by default you will see a login link on your drupal site's login page. However, if you want to add login link somewhere else, please follow the below given steps:

- Go to **Structure -> Blocks**
- Click on **Add block**
- Enter **Block Title** and the **Block description**
- Under the **Block body** add the following URL to add a login link:

** Click here to Login**

- From the text filtered dropdown select either **Filtered HTML** or **Full HTML**
- From the division under **REGION SETTINGS** select where do you want to show the login link
- Click on the **SAVE block** button to save your settings

24*7 Active Support

If you face any issues or if you have any questions, please feel free to reach out to us at drupalsupport@securify.com. In case you want some additional features to be included in the module, please get in touch with us, and we can get that custom-made for you. Also, If you want, we can also schedule an online meeting to help you configure the Drupal OAuth/OpenID Single Sign On module.

Additional Resources

- What is OAuth 2.0?
- What is OpenID Connect?

Hello there!
Need Help? We are right here!



- [Frequently Asked Questions \(FAQs\)](#)

Our Other modules

[SAML SP](#) | [SAML IDP](#) | [2FA](#) | [OAuth/OIDC Client](#) | [LDAP/AD Login](#) | [OAuth Server](#) | [OTP Verification](#) | [Website Security](#) | [Rest API Authentication](#) | [SCIM User Provisioning](#)



+1 978 658 9387 (US)
+91 97178 45846 (India)

✉ info@xecurify.com

STAY CONNECTED



[SIGN UP FREE](#)

Product

- [Single Sign On](#)
- [Identity Brokering](#)
- [OAuth / OpenID Connect Server](#)
- [Multi Factor Authentication](#)
- [Adaptive Authentication](#)
- [User Provisioning](#)
- [Directory Services](#)

Solutions

- [SAML Solutions](#)
- [OAuth Solutions](#)
- [2FA Solutions](#)
- [Mobile Solutions](#)
- [Directory Integrations](#)
- [Federation Integrations](#)
- [Windows Solutions](#)
- [SSO Connectors](#)
- [Secure Browser SSO](#)
- [View All](#)

Why minorange

- [Our Success Stories](#)
- [Content Library](#)
- [Videos](#)
- [FAQs](#)
- [Forum](#)
- [Company](#)
- [Overview](#)
- [News](#)
- [Partners](#)
- [Customers](#)
- [Contact Us](#)

© Copyright 2022 miniOrange. All Rights Reserved.

Hello there!
Need Help? We are right here!

