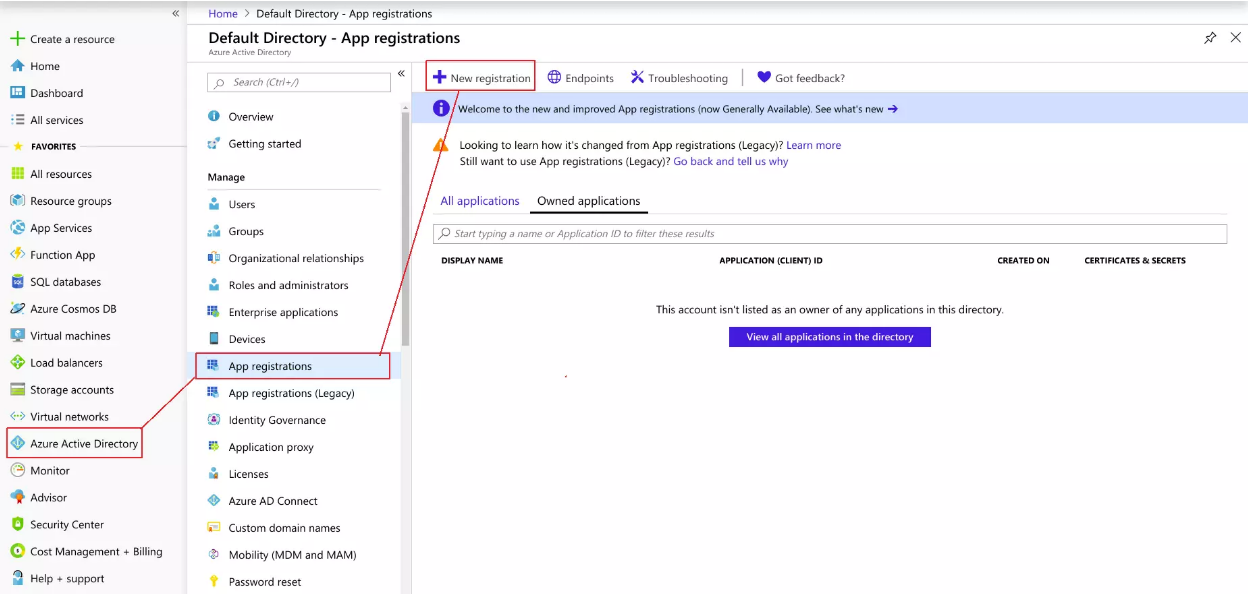
Azure AD SAML SSO with Joomla

Miniorange provides the best SAML Single Sign-On (SSO) solution to Azure active directory (AD)/ Office 365 SSO. SSO reduces the number of attack surfaces because users only log in once each day and only use one set of credentials. Reducing login to one set of credentials improves enterprise security. When employees have to use separate passwords for each app, they usually don't. Single sign-on (SSO) is a highly secure user authentication process. SSO lets the users access multiple applications with a single account credential and sign out instantly with one click. Mini orange Joomla plugin supports SSO. To provide single sign-on services for your domain, Joomla acts as a service provider (SP) through the SAML (Secure Assertion Markup Language) standard.

Steps to configure Azure AD Single Sign-On (SSO) Login into Joomla

Step 1: Setup Azure AD as IDP (Identity Provider)

- Log in to **Azure AD Portal**
- Select **Azure Active Directory** ⇒ **App Registrations**. Click on **New Application Registration**.



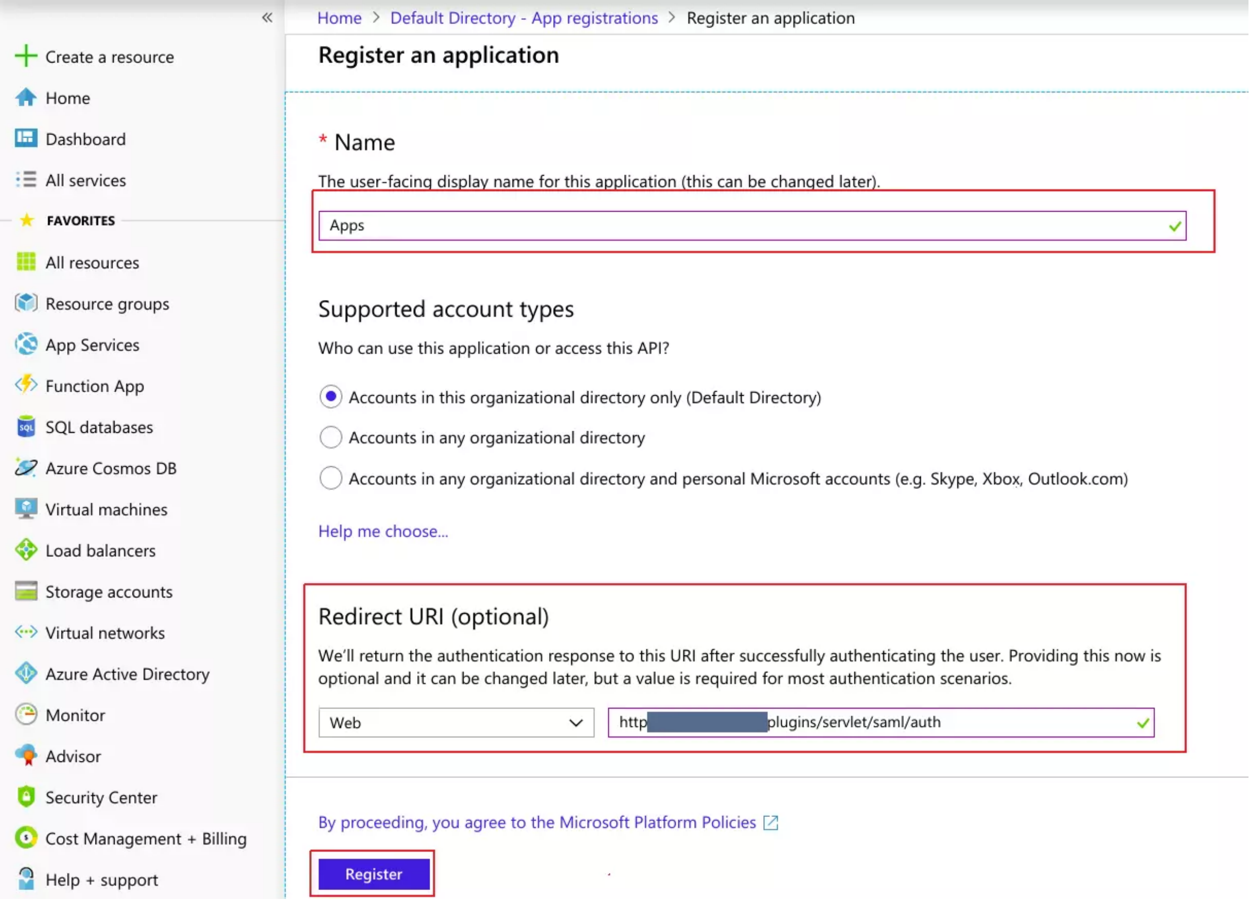
Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more
Still want to use App registrations (Legacy)? Go back and tell us why

DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON	CERTIFICATES & SECRETS

This account isn't listed as an owner of any applications in this directory.

- Assign a Name and choose the account type. In the Redirect URI field, provide the ACS URL provided in the **Service Provider Info** tab of the plugin and click on the **Register** button.



Register an application

* Name

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

Apps ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

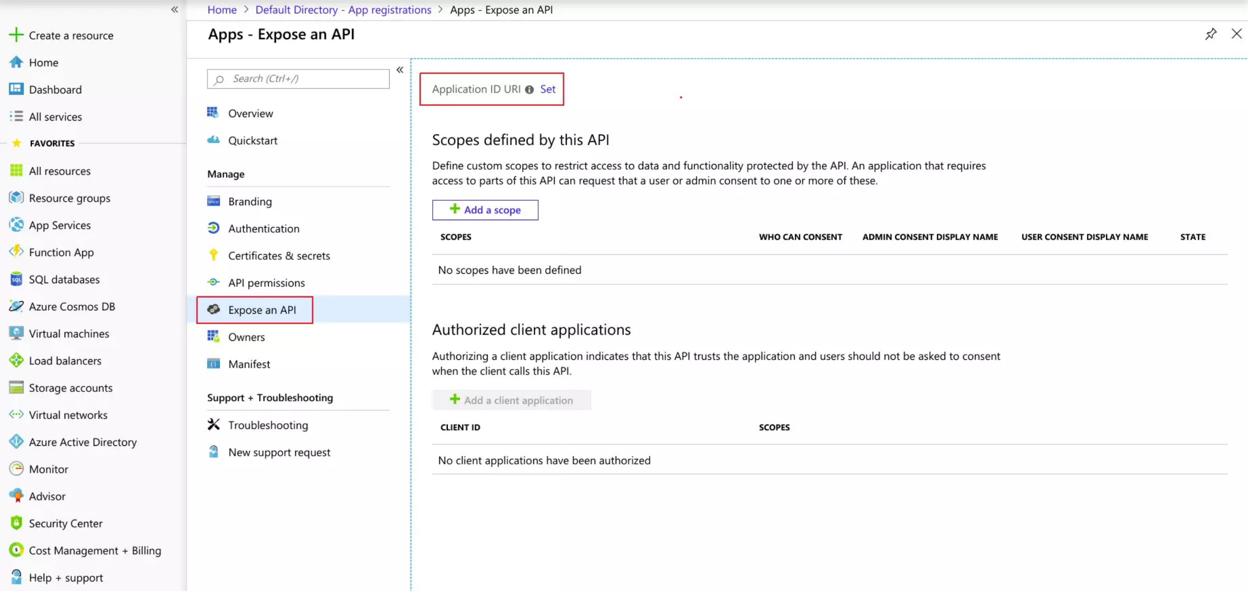
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | http[redacted]plugins/servlet/saml/auth ✓

By proceeding, you agree to the Microsoft Platform Policies

- Now, navigate to **Expose an API** menu option and click the **Set** button and replace the APPLICATION ID URI with the plugin's SP Entity ID
  Here, enter the SP Entity ID value from the Service Provider Metadata tab of the plugin.

  NOTE: Please ensure that the SP Entity ID value from the Service Provider Metadata tab doesn't have a trailing slash('/'). If SP Entity ID has a trailing slash then update it by removing the trailing slash from the SP EntityID / Issuer field under the Service Provider Metadata tab of the plugin, enter the updated value at Azure and click on the Save button.



Apps - Expose an API

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

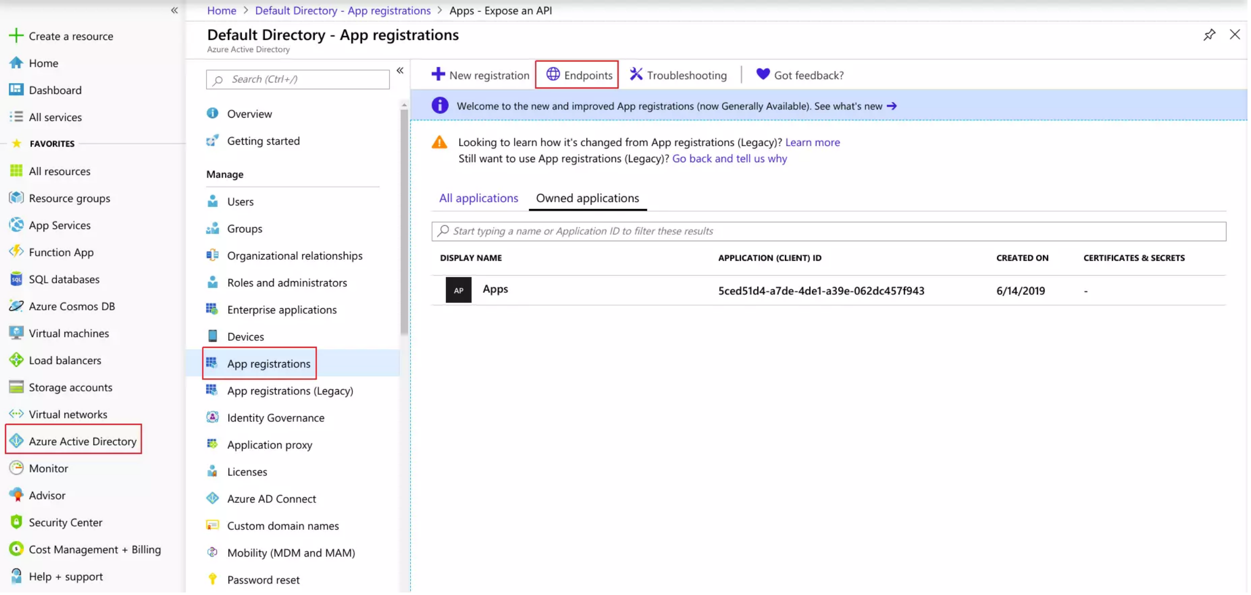
SCOPES	WHO CAN CONSENT	ADMIN CONSENT DISPLAY NAME	USER CONSENT DISPLAY NAME	STATE
No scopes have been defined				

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

CLIENT ID	SCOPES
No client applications have been authorized	

- Go back to the **Azure Active Directory** ⇒ **App Registrations** window and click on the **Endpoints** link.



Default Directory - App registrations

Azure Active Directory

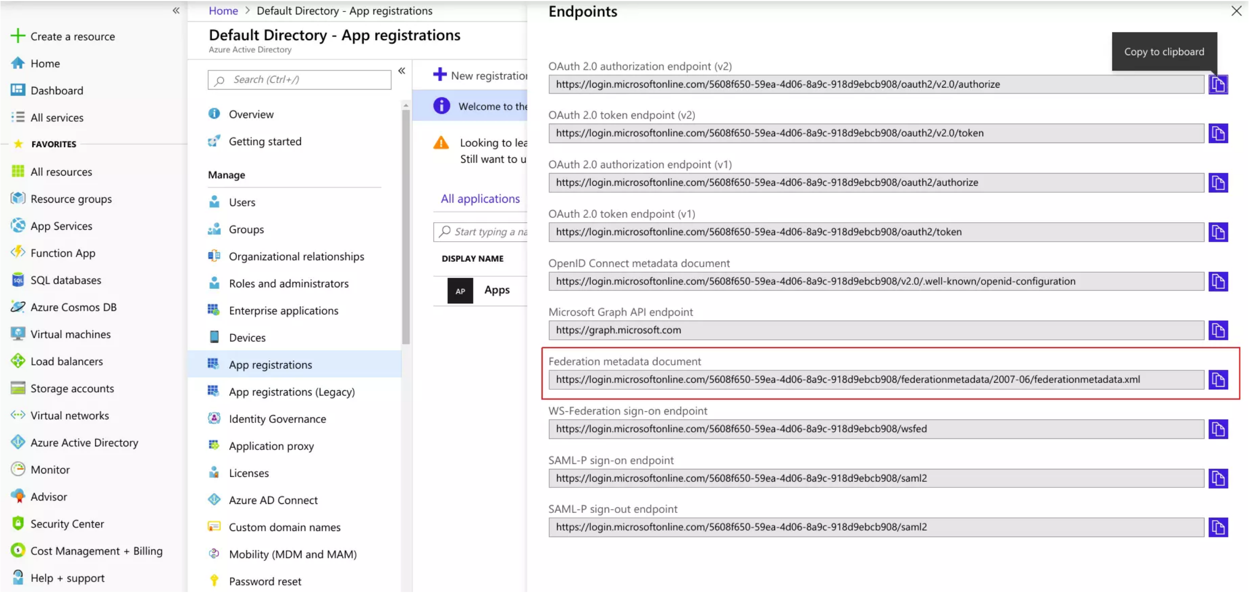
Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more

Still want to use App registrations (Legacy)? Go back and tell us why

DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON	CERTIFICATES & SECRETS
AP Apps	5ced51d4-a7de-4de1-a39e-062dc457f943	6/14/2019	-

- This will open up a window with multiple URLs listed there. Copy the **Federation Metadata Document** URL. This will be required while configuring the SAML plugin.



Endpoints

OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/5608f650-59ea-4d06-8a9c-918d9ebcb908/oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/5608f650-59ea-4d06-8a9c-918d9ebcb908/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/5608f650-59ea-4d06-8a9c-918d9ebcb908/oauth2/authorize

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/5608f650-59ea-4d06-8a9c-918d9ebcb908/oauth2/token

OpenID Connect metadata document
https://login.microsoftonline.com/5608f650-59ea-4d06-8a9c-918d9ebcb908/v2.0/.well-known/openid-configuration

Microsoft Graph API endpoint
https://graph.microsoft.com

Federation metadata document
https://login.microsoftonline.com/5608f650-59ea-4d06-8a9c-918d9ebcb908/federationmetadata/2007-06/federationmetadata.xml

WS-Federation sign-on endpoint
https://login.microsoftonline.com/5608f650-59ea-4d06-8a9c-918d9ebcb908/wsfed

SAML-P sign-on endpoint
https://login.microsoftonline.com/5608f650-59ea-4d06-8a9c-918d9ebcb908/saml2

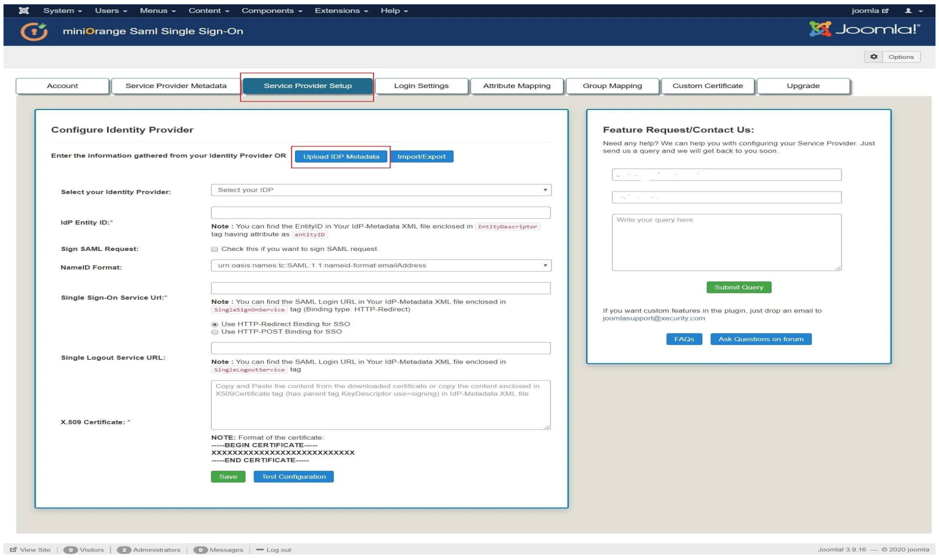
SAML-P sign-out endpoint
https://login.microsoftonline.com/5608f650-59ea-4d06-8a9c-918d9ebcb908/saml2

Step 2: Configuring Joomla as Service Provider (SP)

- In the Joomla SAML plugin, go to **Service Provider Setup** Tab. There are three ways to configure the plugin:

By Metadata URL :

- Click on Upload IDP Metadata.



Configure Identity Provider

Enter the information gathered from your Identity Provider OR

Select your Identity Provider: Select your IDP

IdP Entity ID:*

Note : You can find the EntityID in Your IdP-Metadata XML file enclosed in `EntityDescriptor` tag having attribute as `entityID`

Sign SAML Request: □ Check this if you want to sign SAML request.

NameID Format: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Single Sign-On Service Url:*

Note : You can find the SAML Login URL in Your IdP-Metadata XML file enclosed in `SingleSignOnService` tag (Binding type: HTTP-Redirect)

● Use HTTP-Redirect Binding for SSO
○ Use HTTP-POST Binding for SSO

Single Logout Service URL:

Note : You can find the SAML Login URL in Your IdP-Metadata XML file enclosed in `SingleLogoutService` tag

X.509 Certificate: *

Copy and Paste the content from the downloaded certificate or copy the content enclosed in X509Certificate tag (has parent tag KeyDescriptor use=signing) in IdP-Metadata XML file

NOTE: Format of the certificate:
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----

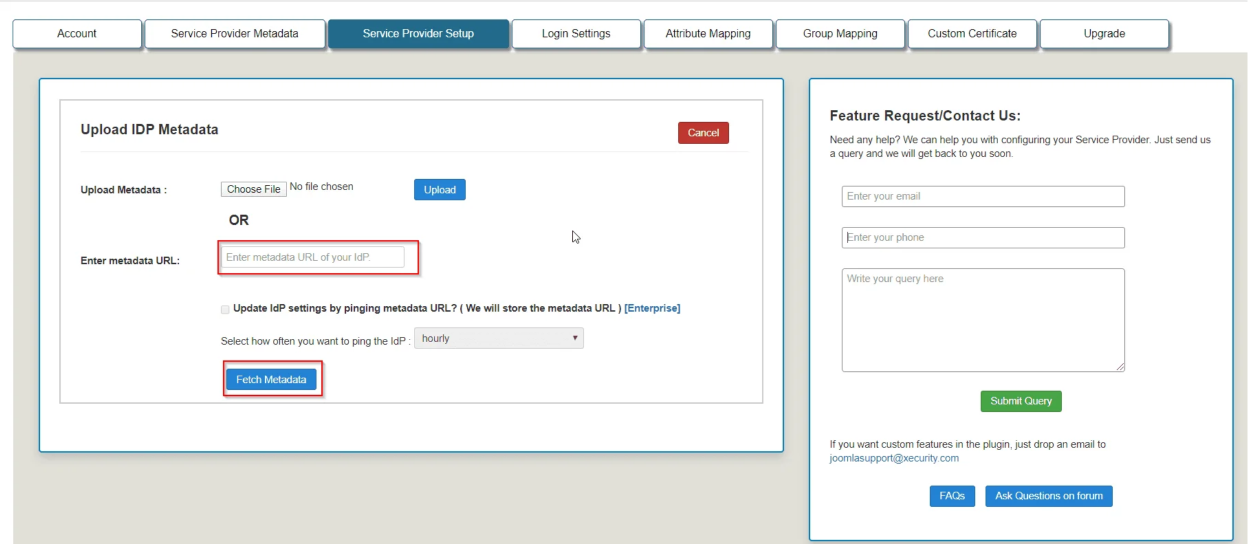
Feature Request/Contact Us:

Need any help? We can help you with configuring your Service Provider. Just send us a query and we will get back to you soon.

Write your query here

If you want custom features in the plugin, just drop an email to joomlasupport@xecurity.com

- Enter Metadata URL **(Copy from IDP app)** and click on Fetch Metadata.



Upload IDP Metadata

Upload Metadata : No file chosen

Enter metadata URL: Enter metadata URL of your IdP

□ Update IdP settings by pinging metadata URL? (We will store the metadata URL) [Enterprise]

Select how often you want to ping the IdP : hourly

Feature Request/Contact Us:

Need any help? We can help you with configuring your Service Provider. Just send us a query and we will get back to you soon.

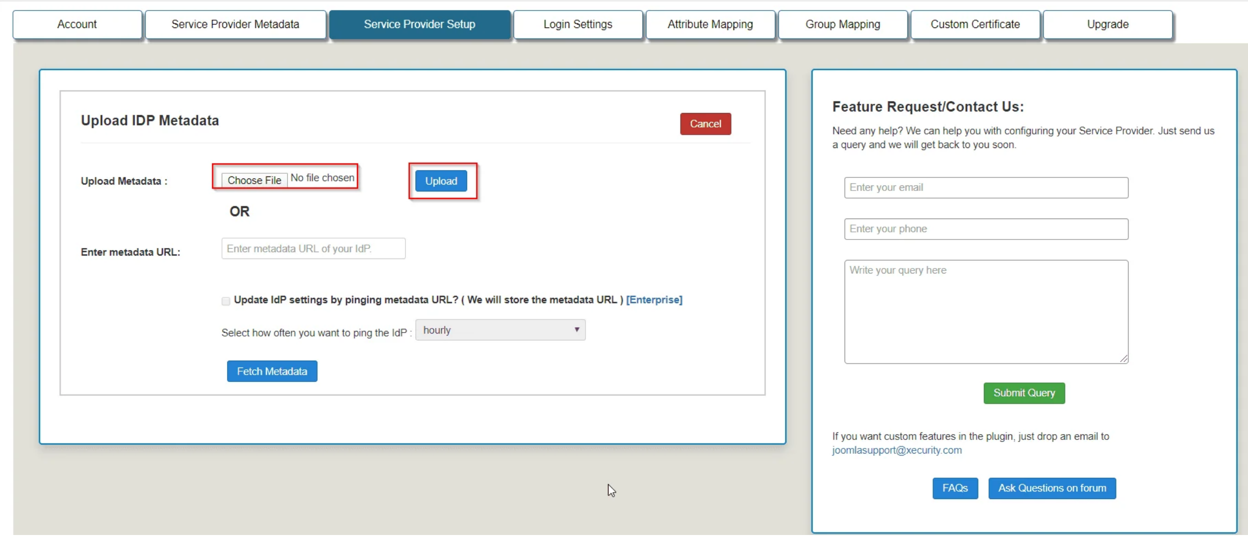
Enter your email

Enter your phone

Write your query here

If you want custom features in the plugin, just drop an email to joomlasupport@xecurity.com

- **By Uploading Metadata File:**
  - Click on Upload IDP Metadata.
  - Choose metadata file and click on Upload.



Upload IDP Metadata

Upload Metadata : No file chosen

Enter metadata URL: Enter metadata URL of your IdP

□ Update IdP settings by pinging metadata URL? (We will store the metadata URL) [Enterprise]

Select how often you want to ping the IdP : hourly

Feature Request/Contact Us:

Need any help? We can help you with configuring your Service Provider. Just send us a query and we will get back to you soon.

Enter your email

Enter your phone

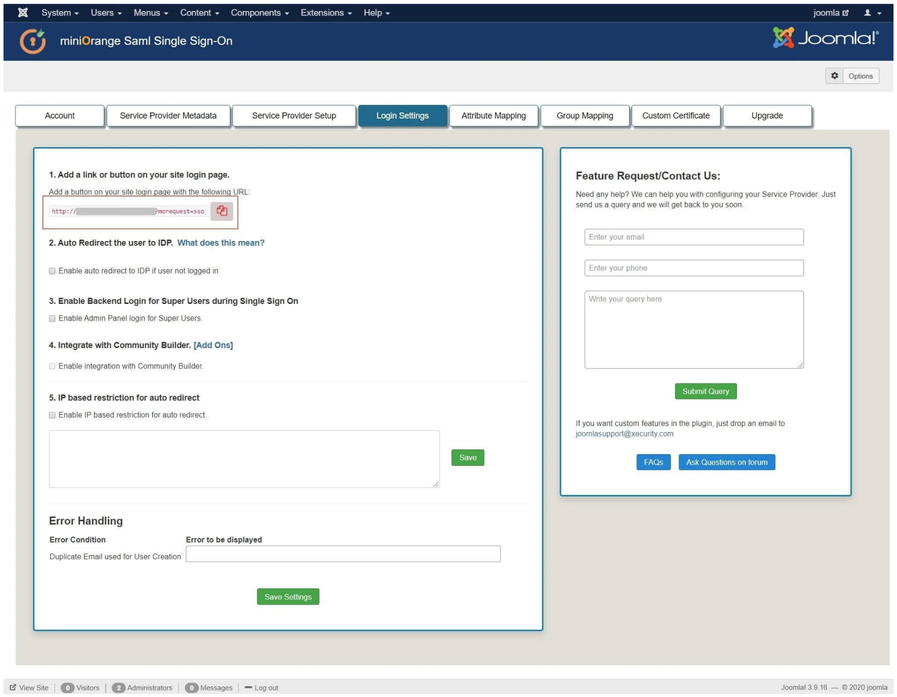
Write your query here

If you want custom features in the plugin, just drop an email to joomlasupport@xecurity.com

- **Manual Configuration :**
  - Copy **SAML Entity ID, SAML Single-Sign-On Endpoint URL, and x.509 certificate** from Federation Metadata document and paste it in **IdP Entity ID or Issuer, Single Sign-on Service URL, x.509 Certificate** fields respectively in the plugin.

IdP Entity ID or Issuer	SAML Entity ID in the Federation Metadata document
Single Sign-On Service URL	SAML Single-Sign-On Endpoint URL in the Federation Metadata document
X.509 Certificate	x.509 Certificate in the Federation Metadata document

Add a button on your site login page with the following URL:



1. Add a link or button on your site login page.

Add a button on your site login page with the following URL:

`http://[redacted]?morequest=sso`

2. Auto Redirect the user to IDP. What does this mean?

□ Enable auto redirect to IDP if user not logged in

3. Enable Backend Login for Super Users during Single Sign On

□ Enable Admin Panel login for Super Users.

4. Integrate with Community Builder. [Add Ons]

□ Enable integration with Community Builder.

5. IP based restriction for auto redirect

□ Enable IP based restriction for auto redirect.

Error Handling

Error Condition	Error to be displayed
Duplicate Email used for User Creation	

Feature Request/Contact Us:

Need any help? We can help you with configuring your Service Provider. Just send us a query and we will get back to you soon.

If you want custom features in the plugin, just drop an email to joomlasupport@xecurity.com

Step 3: Attribute Mapping (It is Optional to fill this). This is a Premium feature.

- Attributes are user details that are stored in your Identity Provider.
- Attribute Mapping helps you to get user attributes from your Identity Provider (IdP) and map them to Joomla user attributes like firstname, lastname etc.
- While auto registering the users in your Joomla site these attributes will automatically get mapped to your Joomla user details.
- In the Joomla SAML plugin, go to the **Attribute Mapping** tab and fill in all the fields.

Username:	Name of the username attribute from IdP (Keep NameID by default)
Email:	Name of the email attribute from IdP (Keep NameID by default)
Group/Role:	Name of the Role attribute from Identity Provider(IdP)

- You can check the **Test Configuration** Results under **Service Provider Setup** tab to get a better idea of which values to map here.

Step 4: Group Mapping (It is Optional to fill this). This is a Premium feature.

- Joomla uses a concept of Roles, designed to give the site owner the ability to control what users can and cannot do within the site.
- Role mapping helps you to assign specific roles to users of a certain group in your Identity Provider (IdP).
- While auto registering, the users are assigned roles based on the group they are mapped to.

Step 5: Redirection & SSO Links.

- Go to the **Login Settings** tab. There are multiple features available in this tab like **Auto redirect the user to Identity Provider** and **Enable Backed Login for Super Users**. To use these features, click on the respective checkboxes.

You have successfully completed your **miniOrange SAML 2.0 SP** configurations. Still, if you are facing any difficulty please mail us on **joomlasupport@xecurify.com**