

Configure Matomo for Single Sign-On

Configuring Matomo for single sign-on (SSO) enables administrators to manage users of Citrix Gateway service. Users can securely log on to Matomo by using the enterprise credentials.

To configure Matomo for SSO by using SAML:

1. In a browser, type <https://matomo.org/start-30-day-free-analytics-trial/> and press **Enter**.
2. Enter your Matomo admin account credentials (**Your email address** and **Your website address**) and click **Start improving your websites now**.

Your email address

Your website address

Your Analytics subdomain will be **.matomo.cloud**

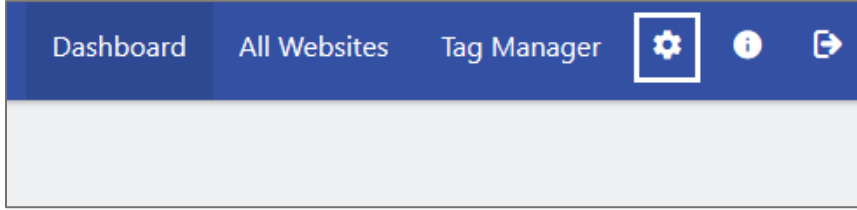
By signing up for a free trial, I hereby accept the [terms and conditions](#).

(Optional) I also accept the [Data Processing Agreement](#) for GDPR compliance.

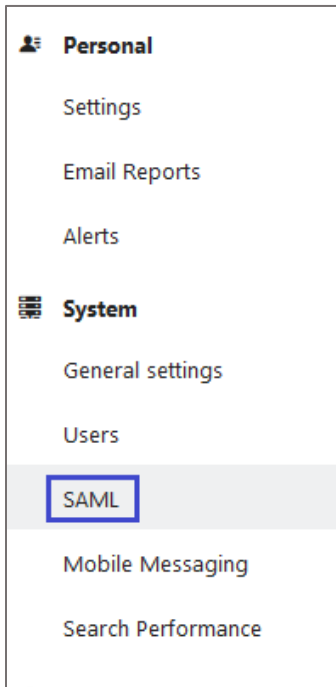
Your information will be used to create an account on our cloud service. For more information please consult our [privacy policy](#).

» Start improving your websites now

- In the dashboard page, click the settings icon in the top-right corner.



- In the left pane, click **SAML**.



- In the **Identity Provider Settings** section, click **Import values from IdP metadata** or enter the values for the following fields and click **SAVE**.

Required Information	Description
Entity ID	IdP issuer URL
Single Sign On Service URL	IdP logon URL
Single Log Out Service URL	IdP logout URL
X.509 Certificate	Copy and paste the IdP certificate. Note: The IdP metadata is provided by Citrix and can be accessed from the link below: <a href="https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/<app_id>/idp_metadata.xml">https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/<app_id>/idp_metadata.xml

Identity Provider Settings

[Import values from IdP metadata](#)

Entity ID
 Identifier of the IdP entity. (must be a URI)

Single Sign On Service Url
 SSO endpoint info of the IdP. URL target of the IdP where the SP will send the Authentication Request.

Single Log Out Service Url
 SLO endpoint info of the IdP. URL target of the IdP where the SP will send the Logout Request/Response.

X.509 Certificate
 Public x509 certificate of the IdP. ('X.509 certificate')

6. In the **Attribute Mapping Settings** section, enter the values for the following fields:

Required Information	Description
Login (username)	IdP username
Email	IdP email
Alias	IdP alias

Attribute Mapping Settings

Login (username)
 Name of the attribute from the SAMLResponse sent by the IdP that contains the username

Email
 Name of the attribute from the SAMLResponse sent by the IdP that contains the email

Alias
 Name of the attribute from the SAMLResponse sent by the IdP that contains the alias

7. Click **SAVE**.