# Configure IT Glue for Single Sign-On

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

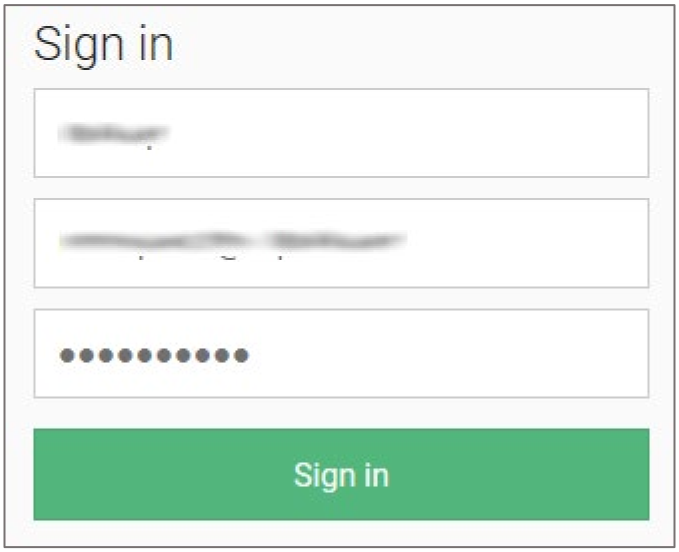
### Prerequisite

Browser Requirements: Internet Explorer 11 and above

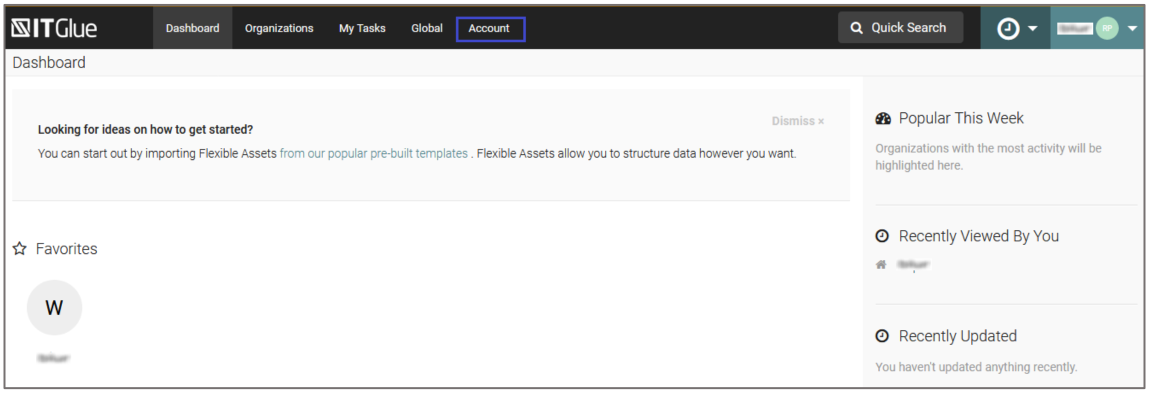
### To configure IT Glue for SSO by using SAML:

1. In a browser, type <customer_domain>.itglue.com and press **Enter**.

2. Type your IT Glue admin account credentials (**Subdomain**, **Email address**, and **Password**) and click **Sign in**.



3. In the dashboard page, click **Account**.



**Looking for ideas on how to get started?**

You can start out by importing Flexible Assets from our popular pre-built templates . Flexible Assets allow you to structure data however you want.

Popular This Week

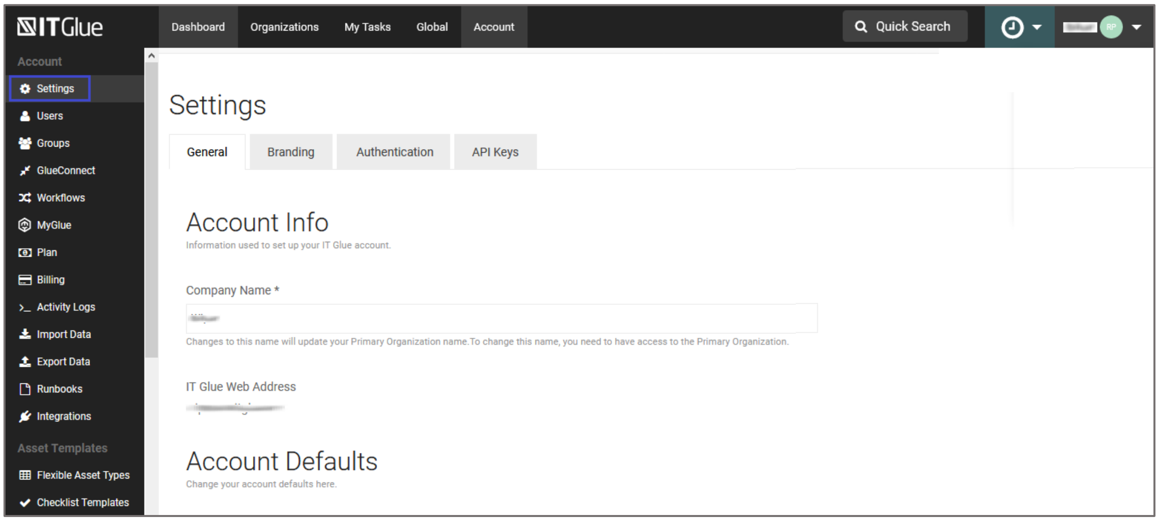
Organizations with the most activity will be highlighted here.

Recently Viewed By You

Recently Updated

You haven't updated anything recently.

4. In the left pane, click **Settings** under **Account**.



Settings

Account Info

Information used to set up your IT Glue account.

Company Name *

[redacted]

Changes to this name will update your Primary Organization name.To change this name, you need to have access to the Primary Organization.

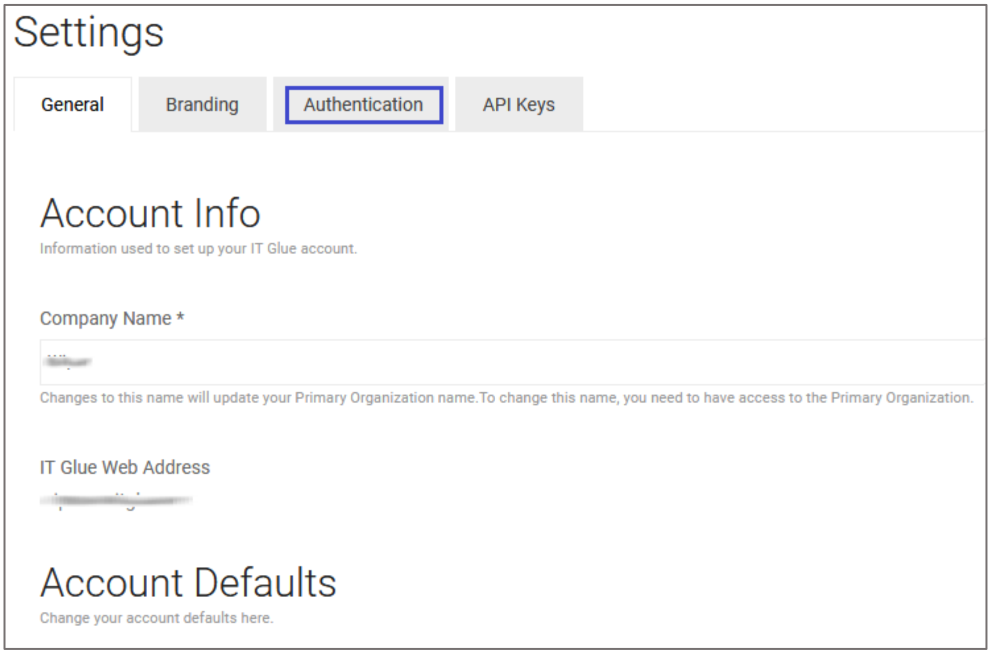
IT Glue Web Address

[redacted]

Account Defaults

Change your account defaults here.

5. In the **Settings** page, click the **Authentication** tab.



Settings

Account Info

Information used to set up your IT Glue account.

Company Name *

[redacted]

Changes to this name will update your Primary Organization name.To change this name, you need to have access to the Primary Organization.

IT Glue Web Address

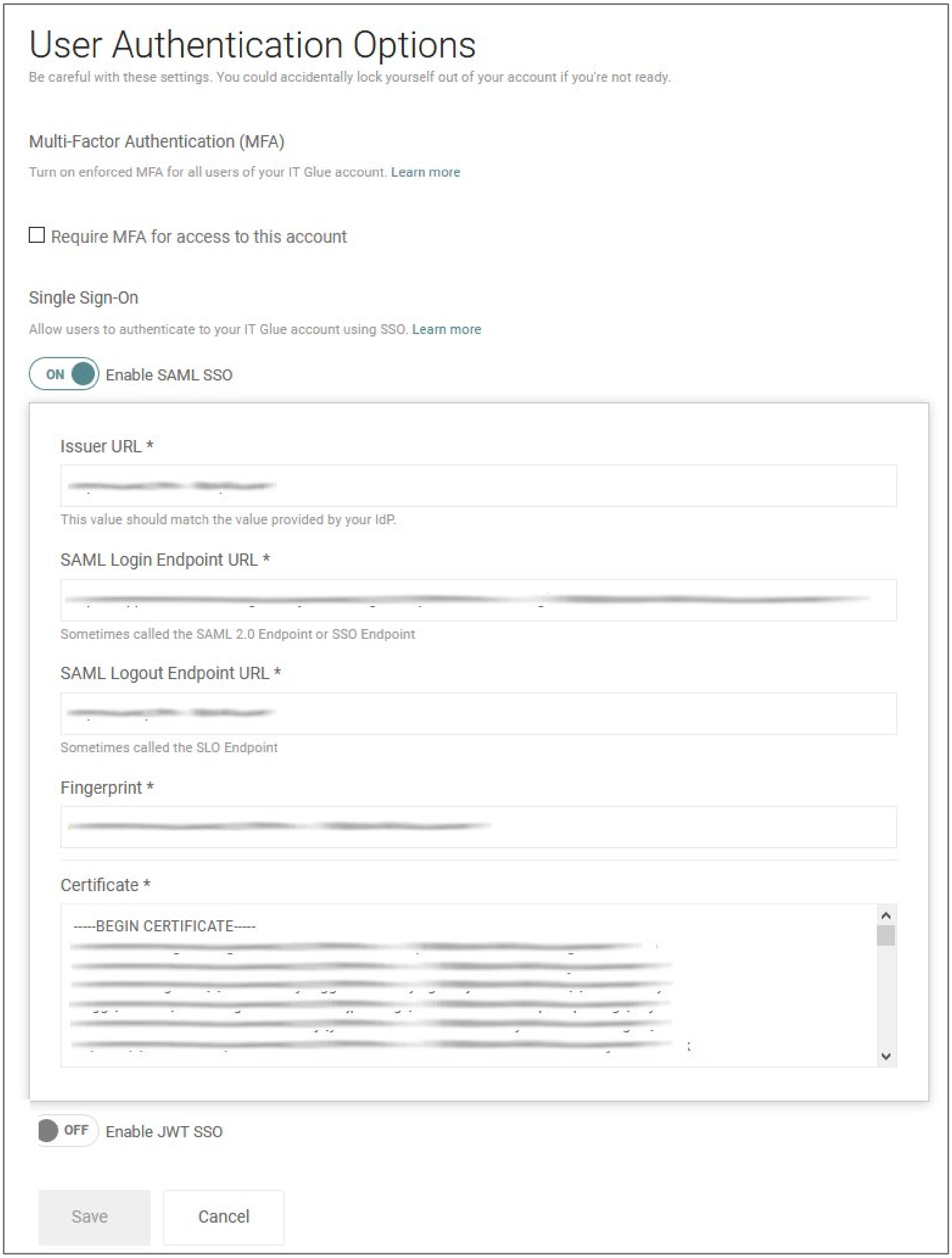
[redacted]

Account Defaults

Change your account defaults here.

6. In the **User Authentication Options** page, turn on the **Enable SAML SSO** toggle button and enter the values for the following fields:

| **Required Information** | **Description** |
|---|---|
| Issuer URL* | Issuer URL |
| SAML Login Endpoint URL* | IdP logon URL |
| SAML Logout Endpoint URL* | IdP logout URL |
| Fingerprint* | SHA1 certificate fingerprint |
| Certificate* | Copy and paste the IdP certificate. The IdP certificate must begin and end with<br>- - - - -Begin Certificate- - - - - and - - - - -End Certificate- - - - -<br>**Note:** The IdP metadata is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app.<br>https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml |



User Authentication Options

Be careful with these settings. You could accidentally lock yourself out of your account if you're not ready.

Multi-Factor Authentication (MFA)

Turn on enforced MFA for all users of your IT Glue account. Learn more

□ Require MFA for access to this account

Single Sign-On

Allow users to authenticate to your IT Glue account using SSO. Learn more

ON ● Enable SAML SSO

Issuer URL *

[redacted]

This value should match the value provided by your IdP.

SAML Login Endpoint URL *

[redacted]

Sometimes called the SAML 2.0 Endpoint or SSO Endpoint

SAML Logout Endpoint URL *

[redacted]

Sometimes called the SLO Endpoint

Fingerprint *

[redacted]

Certificate *

-----BEGIN CERTIFICATE-----
[redacted]

● OFF Enable JWT SSO

7. Finally, click **Save**.