

Configure ScreenSteps for Single Sign-On

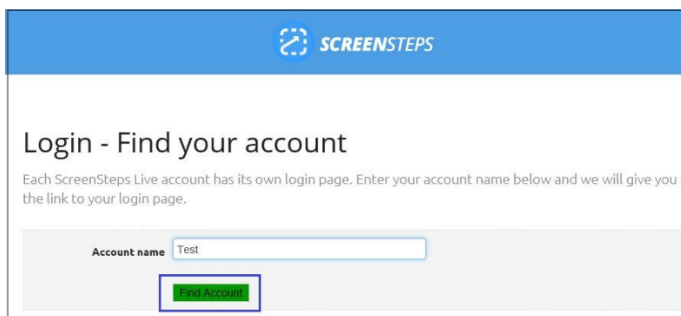
Configuring ScreenSteps for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to ScreenSteps by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure ScreenSteps for SSO by using SAML:

1. In a browser, type <https://screenstepslive.com>, and press **Enter**.
2. To locate your admin account, type your **Account name** and click **Find Account**.



The screenshot shows the 'Login - Find your account' page on the ScreenSteps Live website. The page has a blue header with the ScreenSteps logo and the text 'SCREENSTEPS'. Below the header, the title 'Login - Find your account' is displayed. Underneath the title, there is a sub-header: 'Each ScreenSteps Live account has its own login page. Enter your account name below and we will give you the link to your login page.' Below this text is a form with a label 'Account name' and a text input field containing the word 'Test'. Below the input field is a green button labeled 'Find Account', which is highlighted with a blue border in the image.

3. After locating the account, log on to the ScreenSteps account with your credentials (**Username** and **Password**).

test

Please Log In

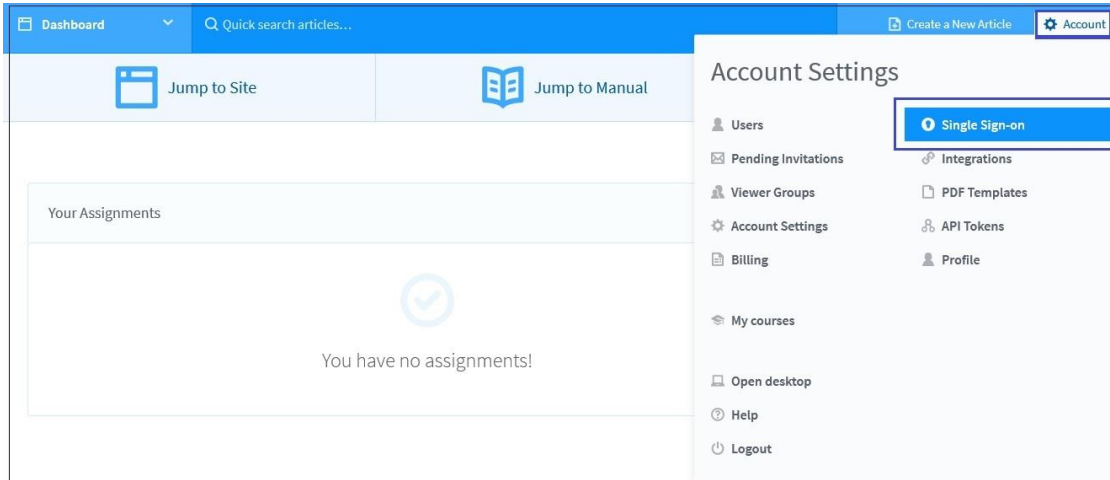
Username:

Password:

Remember me

[I forgot my password](#)

- To create **Single Sign-On Endpoint**, click the **Account** menu that is present at the top-right corner of the screen, and select **Single Sign-On**.



- Click **Create Single Sign-on Endpoint**.
- To create **Single Sign-On Endpoint**, enter the values for the following fields as explained in the following table:

Field	Description
Title	Citrix ADC
Mode	Select SAML from the drop-down list.
Remote Login URL	IdP logon URL
Remote Logout URL	IdP logout URL

 A screenshot of a form titled 'Create Single Sign-on Endpoint'. The form contains four input fields: 'Title' (text input), 'Mode' (dropdown menu with 'SAML' selected), 'Remote Login URL' (text input), and 'Log out URL' (text input). At the bottom left of the form is a blue 'Create' button.

- After providing all the relevant details, click **Create**.
Note: A confirmation message indicating that the SSO Endpoint is created appears.
- In the **Edit Single Sign-On Endpoint** section, click **SAML Certificate**, upload the certificate and click **Update**. To obtain the certificate, refer the following table:

Field name	Description
Certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- Note: The IdP metadata URL is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app. <a href="https://gateway.cloud.com/idp/saml/<citrixcloudcust id>/<app id>/idp_metadata.xml">https://gateway.cloud.com/idp/saml/<citrixcloudcust id>/<app id>/idp_metadata.xml

9. After configuring the single sign-on Endpoint, copy both the SAML URLs, and test them in the testing site.

URLs

SAML Consumer URL

[Copy](#)

SAML Test URL

[Copy](#)