

Configuring Assembla

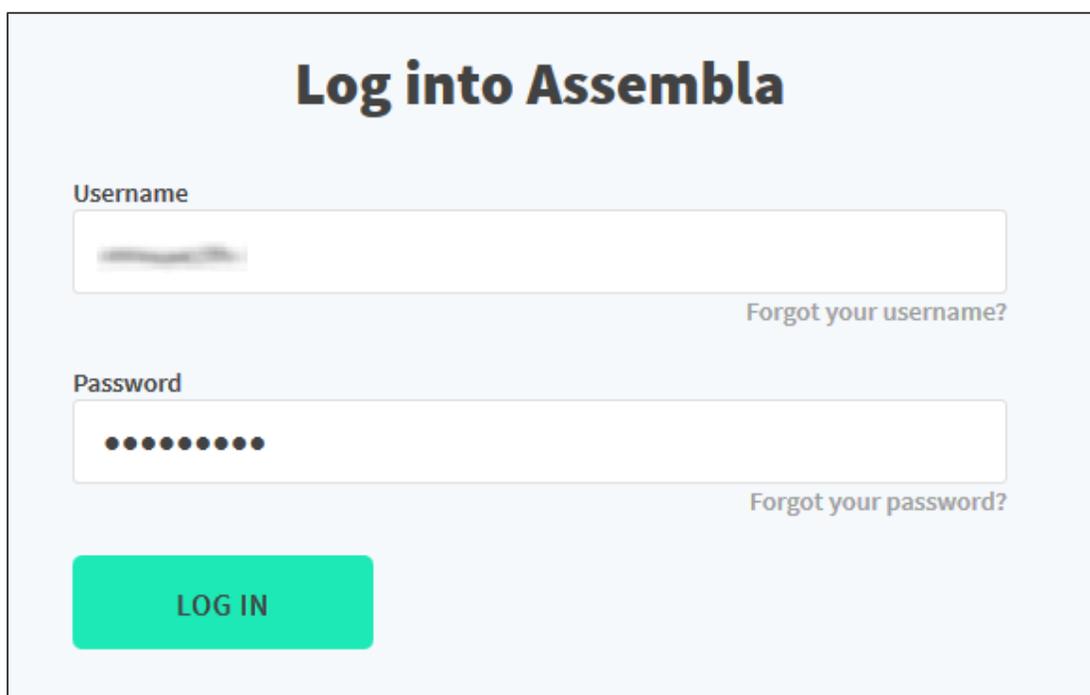
Configuring Assembla for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Assembla by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure Assembla for SSO by using SAML:

1. In a browser, type <https://www.assembla.com/home> and press **Enter**.
2. Type your Assembla admin account credentials (**Username** and **Password**) and click **LOG IN**.



Log into Assembla

Username

Forgot your username?

Password

Forgot your password?

LOG IN

3. To access the login page of SAML for authentication, paste <https://<customer domain>.assembla.com/p/admin> link in a browser and press **Enter**.
4. In the **SAML authentication** section of the admin dashboard, select the **Enable** check box and enter the values for the following fields.

Field Name	Description
SAML Assertion Consumer Service URL	IdP Logon URL
Security Certificate	Upload the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- Note: The IdP Certificate is provided by Citrix and can be accessed from the following link: https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml
Security Certificate Fingerprint	Copy and paste the IdP certificate fingerprint from the https://www.samltool.com/fingerprint.php link, select Algorithm and CALCULATE FINGERPRINT .

SAML authentication

If you have a SAML (Secure Assertion Markup Language) Identity Provider, then you can force portfolio members to login through that. Just check the checkbox and fill out the fields. Only URL and either certificate or its fingerprint fields are required. [Please see our documentation for more information.](#)

Enable

Lifetime of a user session in hours (Note: Changes will apply after current session will expire).

SAML Assertion Consumer Service URL. Your Identity Provider will ask for it.

This is the URL of your Identity Provider that the authentication requests will be sent to.

Fingerprint represents your certificate. Please ask your SAML Identity Provider for that. It will look something like E7:5C:78:A5:54:5D:6A:9E:11:02:CD:33:B3:B0:6A:CE:D7:B2:61:86

Your X.509 Certificate.

Note: Either certificate fingerprint or X.509 Certificate can be used to update the SAML settings.

5. Finally, click **Update SAML settings**.

Note: User access has to be enabled by the admin for users to access the workspace.