

Configure LiveChat for Single Sign-On

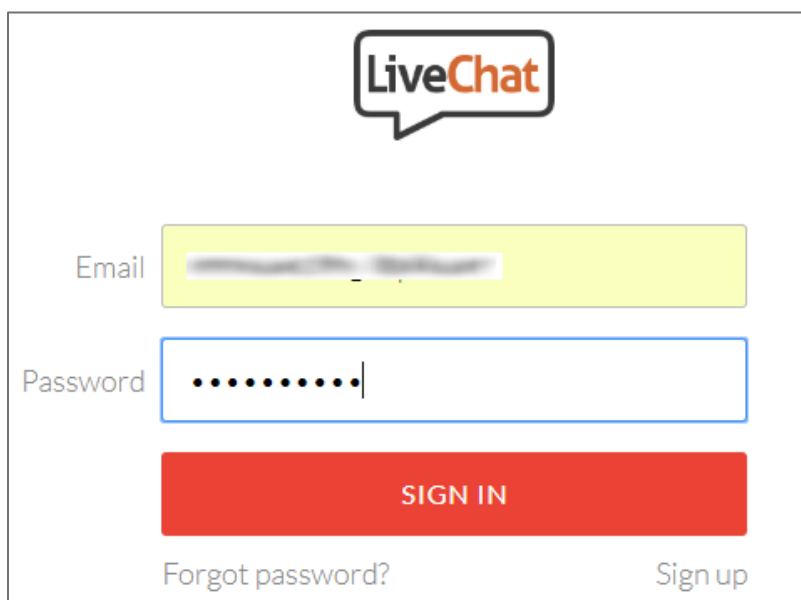
Configuring LiveChat for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to LiveChat by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

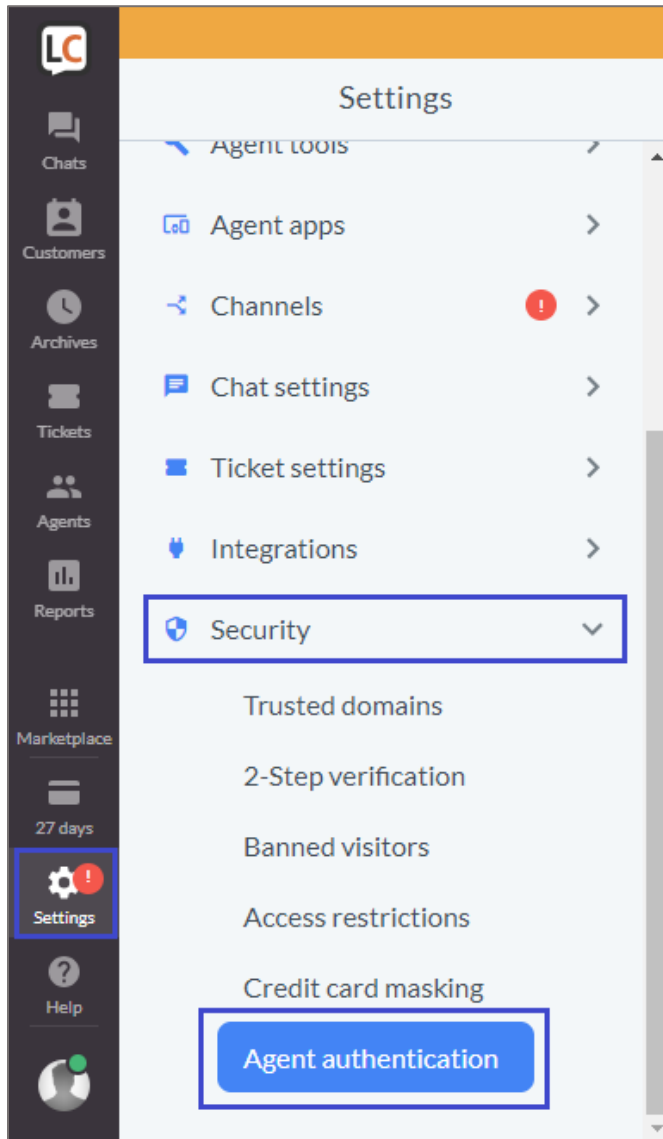
To configure LiveChat for SSO by using SAML:

1. In a browser, type <https://www.livechatinc.com/applications/> and press **Enter**.
2. Type your LiveChat admin account credentials (**Email** and **Password**) and click **SIGN IN**.



The screenshot displays the LiveChat login interface. At the top center is the LiveChat logo, which consists of the word "LiveChat" in a sans-serif font inside a speech bubble outline. Below the logo are two input fields: an "Email" field with a yellow background and a "Password" field with a blue border. The password field contains several black dots. Below these fields is a prominent red button with the text "SIGN IN" in white capital letters. At the bottom of the form, there are two links: "Forgot password?" on the left and "Sign up" on the right.

3. In the left panel, click **Settings** and select **Security** > **Agent authentication** from the drop-down list.



- In the **Your own SAML implementation** tile, move the cursor to the right end and click **configure** from the pop up text that appears.

Agent authentication

Choose an authentication method

You can choose how agents log into LiveChat. By default, all agents authenticate with their LiveChat credentials. Make the process easier and more secure for everyone by choosing Single Sign-On as your login method. [Learn more...](#)

Your login method

Your own SAML implementation

configure
disable

Choose other login method

LiveChat

Okta

OneLogin

- In the **Your own SAML implementation configuration** page, enter the values for the following fields:

Field Name	Description
Identity Provider Single Sign-On URL	IdP logon URL
X.509 certificate	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate-----</p> <p>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. <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</p>



Your own SAML implementation configuration

To complete the setup, copy the Identity Provider Single Sign-On URL and the X.509 certificate (including lines with "BEGIN" and "END") and paste them into the corresponding fields.

1 Identity Provider Single Sign-On URL

2 X.509 certificate

```
-----BEGIN CERTIFICATE-----  
-----END CERTIFICATE-----
```

Save changes

or cancel

6. Finally, click **Save changes**.