

Configure ContractSafe for Single Sign-On

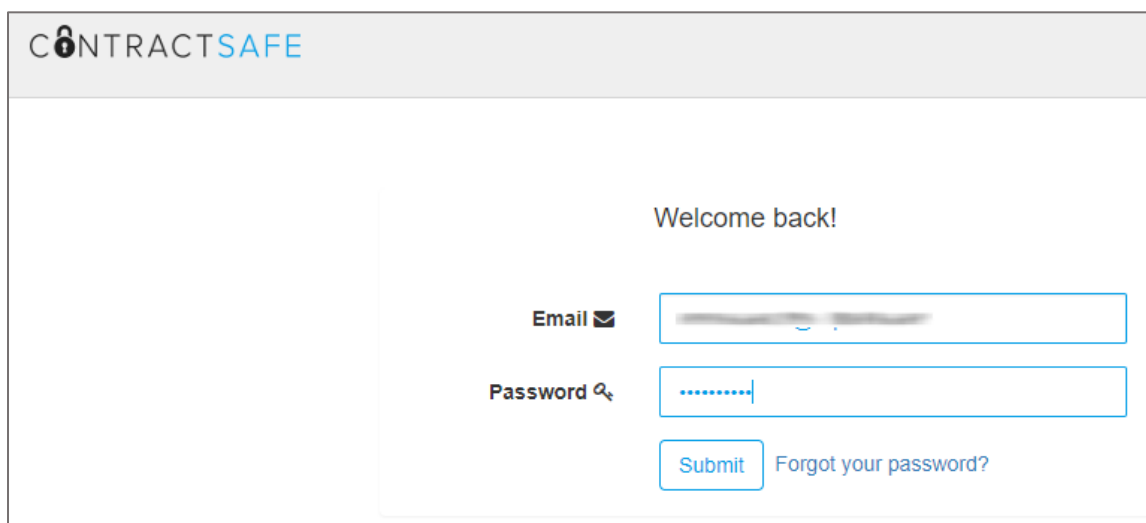
Configuring ContractSafe for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to ContractSafe by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above


To configure ContractSafe for SSO by using SAML:


1. In a browser, type <https://app.contractsafe.com/> and press **Enter**.
2. Type your ContractSafe admin account credentials (**Email** and **Password**) and click **Submit**.



CONTRACTSAFE

Welcome back!

Email 

Password 

[Forgot your password?](#)

3. In the dashboard page, click the user account icon in the top-right corner and select **Settings**.

The screenshot shows the ContractSafe dashboard. At the top, there is a navigation bar with the logo, 'Dashboard' and 'Contracts' tabs, a search bar, and an 'Add Contracts' button. A user profile icon in the top right corner has a dropdown menu open, with 'Settings' highlighted. Below the navigation bar, a yellow banner states: 'You are currently using a 7 day free trial account. Click [HERE](#) to upgrade your account.' The main content area is divided into two columns. The left column contains a 'Welcome to ContractSafe!' message with a 'Close This Guide' button, a list of four benefits, and sections for 'Getting Started' and 'Need help?'. The right column is titled 'Recent Activity' and has tabs for 'User', 'Contracts', and 'Deletions'. It lists several 'Quick Start Guide' updates with timestamps.

4. In the **Settings** page, click **Security & Integrations**.

The screenshot shows the 'Settings' page. At the top left, there is a gear icon and the text 'Settings:'. Below this, there are two columns of buttons: 'Users', 'Custom Fields & Templates', 'Folders & Tags', and 'Contracts List' on the left; and '[AI]ssistant', 'Login', 'Email Settings', and 'Security & Integrations' on the right. The 'Security & Integrations' button is highlighted with a blue border. Below the buttons, there are three sections: 'My Company (This is your primary legal entity.)' with a text input field containing 'your company name'; 'Date Format (This is the setting for all users on your account.)' with a dropdown menu showing 'MM/dd/yyyy 11/26/2018'; and 'Download all Documents and Data:' with two buttons: 'Documents' and 'Data'.

- In the **Security and Integrations** pop-up window, click the **Single Sign-On** toggle button to enable SSO.

Security and Integrations

Two-factor authentication

Two-factor authentication is not enabled for your account. Enable two-factor authentication for enhanced account security.

Single Sign-On

This will enable a SAML2 Single Sign-on for your account (like Active Directory or OKTA).

DocuSign

This will enable DocuSign connect for your account.

Salesforce

This will enable a Salesforce endpoint for your account.

IP Whitelisting

IP whitelisting has not been enabled for your organization. All IP addresses will be allowed.

Cancel
Save

- Enter the values for the following fields:

Required Information	Description
Email Identifier name	Issuer email address
Identity Provider Metadata	<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.</p> <p><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>

- You can also choose to upload the metadata file in XML format.

Note: The IdP metadata is provided by Citrix and can be accessed from the link below:
https://gateway.cloud.com/idp/saml/<citrixcloudcust id>/<app id>/idp_metadata.xml

Security and Integrations

Two-factor authentication



Two-factor authentication is not enabled for your account. Enable two-factor authentication for enhanced account security.

Single Sign-On



SAML2 Single Sign-on is enabled.

Saml2 Single Sign On URL (This is used in your Okta settings.) [Remove](#)

https://app.contractsafe.com/saml2_auth/

Email Identifier name (The issuer email address variable name)

Identity Provider Metadata (URL to dynamic configuration metadata.)

OR

Upload your saml metadata file (xml file containing configuration metadata.)

idp_metadata.xml [Remove](#)

DocuSign



This will enable DocuSign connect for your account.

Salesforce



This will enable a Salesforce endpoint for your account.

IP Whitelisting



IP whitelisting has not been enabled for your organization. All IP addresses will be allowed.

Cancel

Save

8. Finally, click **Save**.