Supplyframe

Supplyframe CPQ
SSO Setup Guide

Company Confidential

Single Sign-On (SSO) Setup Guide

Supplyframe CPQ supports SAML 2.0-based Single Sign-On (SSO), enabling users to authenticate through the customer's identity provider with a unified set of credentials. This implementation provides seamless integration with existing authentication infrastructure while maintaining enterprise-grade security standards.

Supported environments include:

- Stage: https://cpq.stage.supplyframe.app
- Production: https://cpq.supplyframe.app

1. Prerequisites

Before initiating SSO implementation, verify the following requirements are met:

Technical Requirements

- **Identity Provider Compatibility:** Customer’s IdP must support SAML 2.0 protocol
- **Custom Subdomain:** A dedicated subdomain will be provisioned for the customer organization

Account Requirements

- **Active CPQ Account**: Active customer account must exist in target environment (production or staging)
- **Account Owner Registration**: Customer's designated Account Owner must be invited to the account and must have completed the registration process
- **Credential Verification**: Customer’s Account Owner must confirm access using CPQ email and password credentials

After verifying all requirements are met, SSO implementation consists of Supplyframe platform configuration, and subsequent customer identity provider integration, which must be handled by the customer.

2. Supplyframe Configuration Steps

The following configuration steps must be completed by the Supplyframe team before customers can configure their identity provider details.

Step 1: Environment Selection

Determine target environment for SSO implementation:

- Stage: For testing and validation (recommended first)
- Production: For live user authentication

Step 2: Subdomain Provisioning

Determine the customer's preferred subdomain prefix, for example:

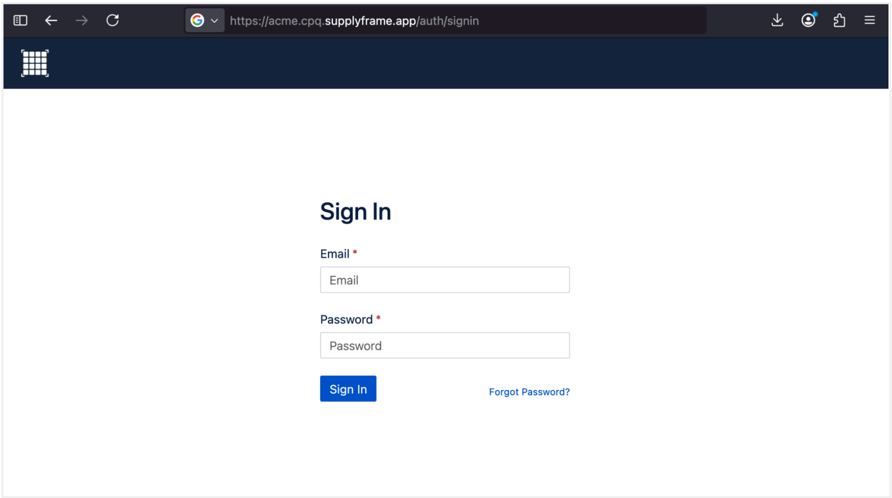
- Stage example: https://acme.cpq.stage.supplyframe.app/
- Production example: https://acme.cpq.supplyframe.app/

Contact Supplyframe Operations team at ops@supplyframe.com with the following information:

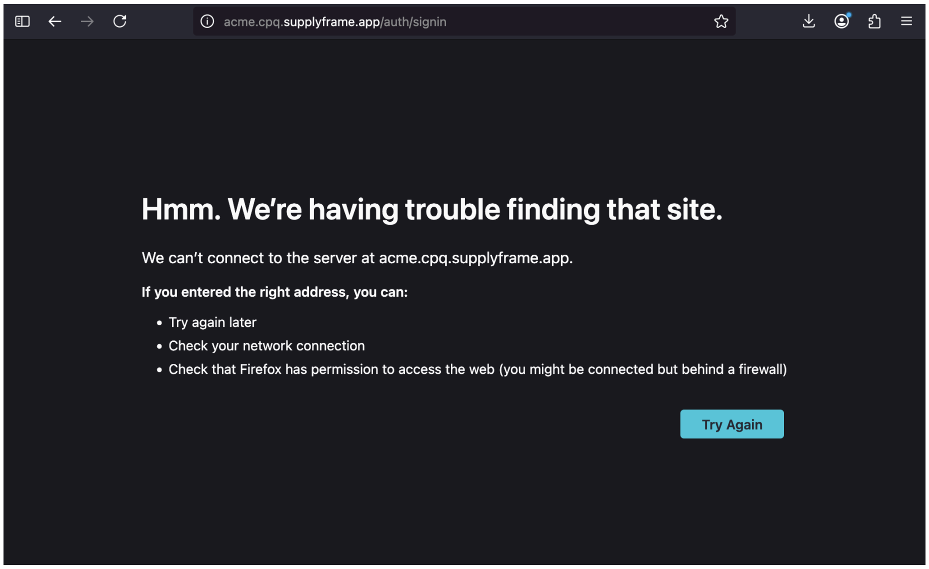
- Subdomain prefix
- Target environment
- Implementation timeline

Step 3: Subdomain Validation

After the Operations team confirms setup is complete, navigate to the assigned subdomain URL and verify that it takes you to the Supplyframe CPQ ***Sign In*** page:



If you are unable to open the page, the subdomain was not configured properly:



Hmm. We're having trouble finding that site.

We can't connect to the server at acme.cpq.supplyframe.app.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Escalate to the Operations team if the subdomain is inaccessible.

Step 4: Super Admin SSO Configuration

Contact the Support team with the following details to request Super Admin Panel configuration of SSO for the customer account:

- Customer account
- Configured subdomain URL
- Target environment
- Implementation timeline

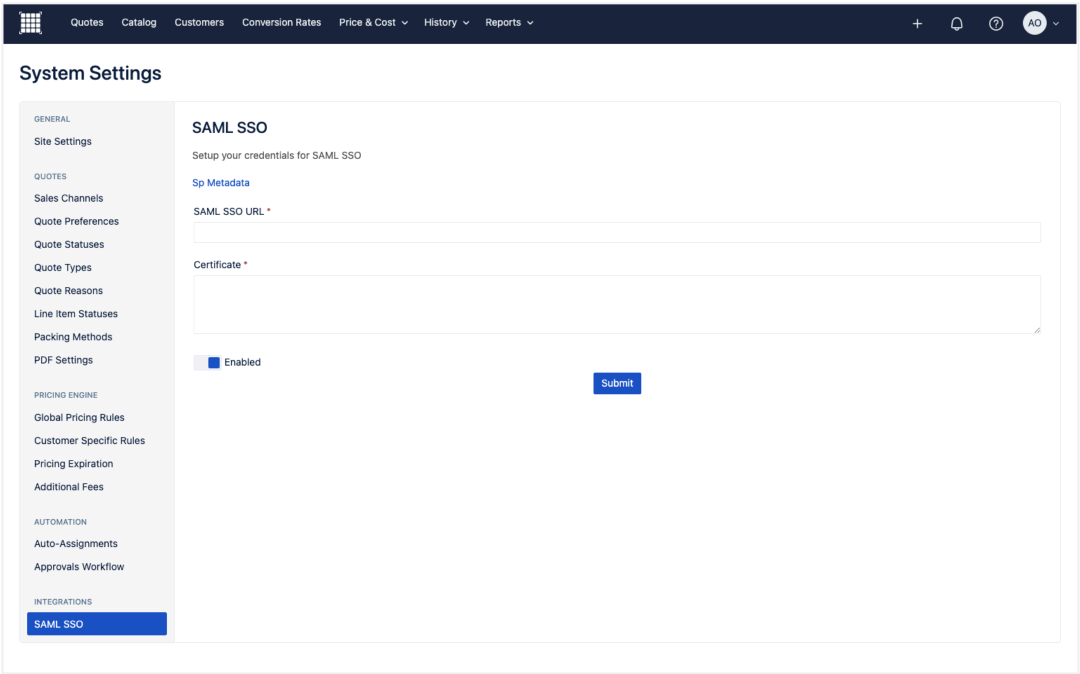
The Super Admin will activate SSO for the customer account and input the subdomain into the account configuration.

3. Customer Account Owner Configuration Steps

These final ***Identity Provider Integration*** steps must be completed specifically by the ***Account Owner*** of the CPQ account (not other admin users) and cannot be completed by Supplyframe.

Step 1: Download SP Metadata

Prompt the Account Owner to access the ***SAML SSO*** page in ***System Settings***:



System Settings

SAML SSO

Setup your credentials for SAML SSO

Sp Metadata

SAML SSO URL *

Certificate *

☑ Enabled

The Account Owner must click the blue Sp Metadata (Service Provider) link and download the details to their computer.

The metadata contain details about our CPQ solution that are required for our customer's Identity Provider (IdP) to integrate with our system:

- Entity ID (unique identifier for the SP)
- Assertion Consumer Service (ACS) URL (where the IdP sends authentication responses)
- Supported SSO protocols and bindings (e.g., SAML 2.0)
- SP signing certificate (if applicable, for signing requests)

Step 2: Identity Provider Configuration

The Account Owner will share the SP Metadata with their IT team, who will then provide details that the Account Owner must populate in the CPQ ***SAML SSO*** page.

Enter the ***SAML SSO URL*** (this should be the IdP URL, not the CPQ subdomain that Supplyframe provisions for customers) and ***Certificate*** details, then select ***Enable*** to complete the SSO setup process.

Step 3: Add Users To Account (Account Owner)

The Account Owner is now ready to go to CPQ's ***Organization*** page and add users into their CPQ account.

4. Troubleshooting

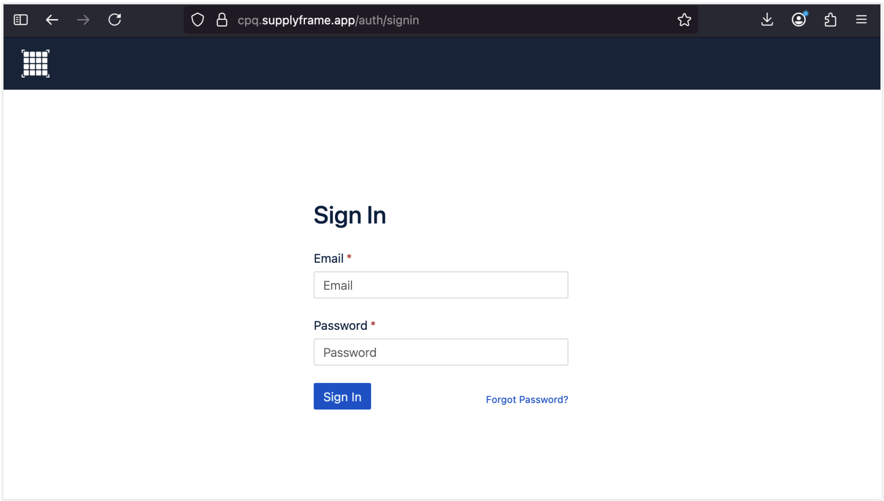
After completing ***Step 2: Identity Provider Configuration*** in the section above, it may be possible that the Account Owner populated the incorrect ***SAML SSO URL*** or incorrect ***Certificate*** details.

If the ***Enable*** button was turned on and saved, Account Owners may not be able to log into their account because the next time any user that belongs to that customer's account attempts to access CPQ, our solution will route them to the Identity Provider login page, and when they try to login, they will be unsuccessful.

In this scenario, there are two options for troubleshooting:

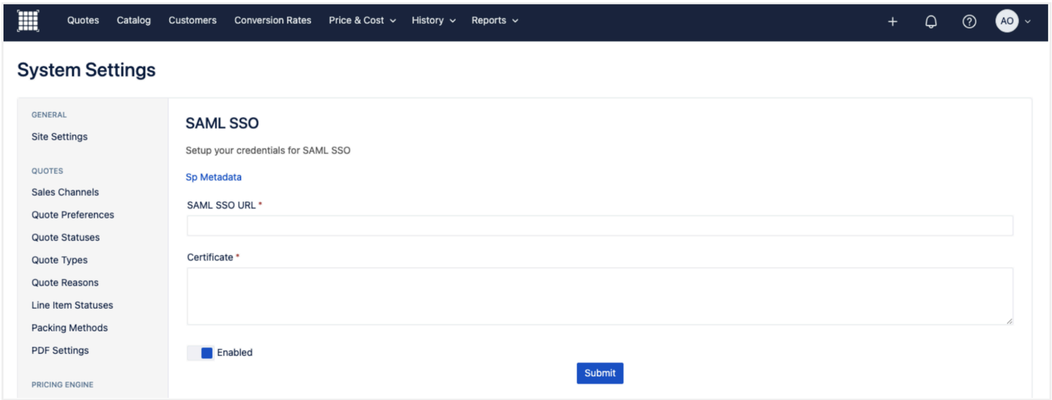
Option 1: Account Owner Login Via Main CPQ URL

When SSO is enabled, Account Owners have the ability to log into CPQ by going to the main URL (cpq.supplyframe.app - not the subdomain), and entering their CPQ credentials.



Note that no other user in the account will have this option available to them - only Account Owners will be able to login through this route.

Once the Account Owner has gained access to their CPQ account, they will be able to correct the ***SAML SSO URL*** and/or the ***Certificate***, or turn off SSO entirely by de-selecting the ***Enabled*** toggle.



System Settings

SAML SSO

Setup your credentials for SAML SSO

Sp Metadata

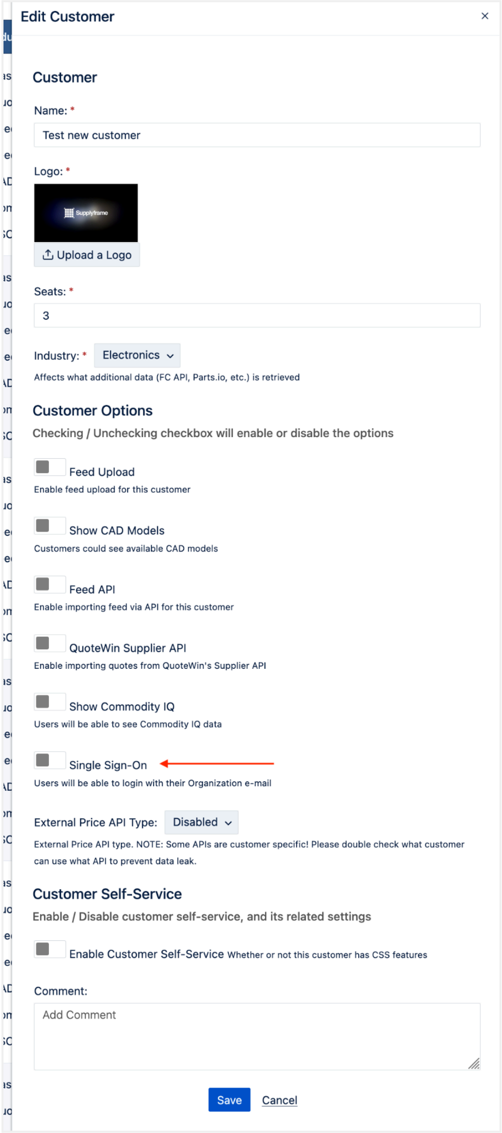
SAML SSO URL *

Certificate *

Enabled

Option 2: Super Admin Disables SSO In Super Admin Panel

The second available option is to reach out to the Support team and request that they access the ***Super Admin Panel*** for CPQ and turn off the SSO setting in the customer's configuration side panel:



Edit Customer ×

Customer

Name: *
Test new customer

Logo: *

Upload a Logo

Seats: *
3

Industry: * Electronics
Affects what additional data (FC API, Parts.io, etc.) is retrieved

Customer Options

Checking / Unchecking checkbox will enable or disable the options

□ Feed Upload
Enable feed upload for this customer

□ Show CAD Models
Customers could see available CAD models

□ Feed API
Enable importing feed via API for this customer

□ QuoteWin Supplier API
Enable importing quotes from QuoteWin's Supplier API

□ Show Commodity IQ
Users will be able to see Commodity IQ data

□ Single Sign-On
Users will be able to login with their Organization e-mail

External Price API Type: Disabled
External Price API type. NOTE: Some APIs are customer specific! Please double check what customer can use what API to prevent data leak.

Customer Self-Service

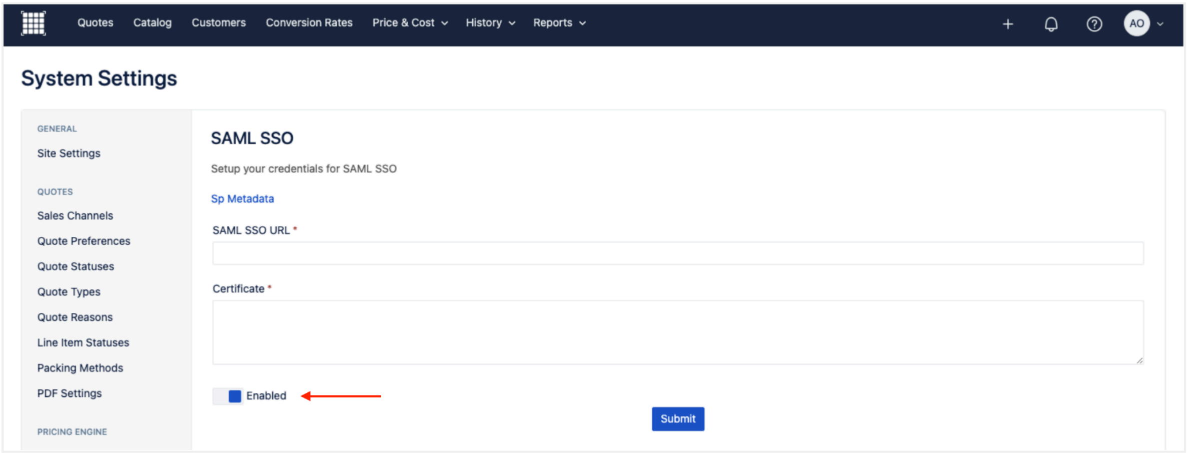
Enable / Disable customer self-service, and its related settings

□ Enable Customer Self-Service Whether or not this customer has CSS features

Comment:
Add Comment

Save Cancel

When this setting is turned off from the Super Admin panel, the SSO ***Enabled*** button within the customer's account will also be toggled off:



System Settings

SAML SSO

Setup your credentials for SAML SSO

SAML SSO URL *

Certificate *

Enabled

This means that the next time users that belong to this account can access our solution by opening the main CPQ URL (cpq.supplyframe.app) and login with their CPQ credentials.

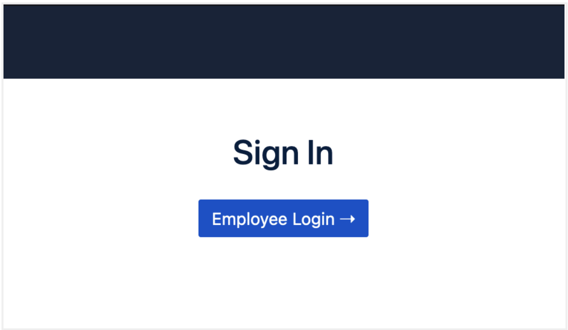
5. Example SSO Login Flow

Note that the details below will differ depending on the customer. For demo purposes below, we've used our own identity provider, so the login experience observed during testing may differ from the final customer-facing experience, as it will ultimately use the customer's specific IdP and authentication flow.

The SSO flow begins when a user accesses the application through the customer's designated subdomain (eg. acme.cpq.supplyframe.app).

This subdomain serves as the entry point and allows the application to identify the appropriate customer configuration, including the linked IdP.

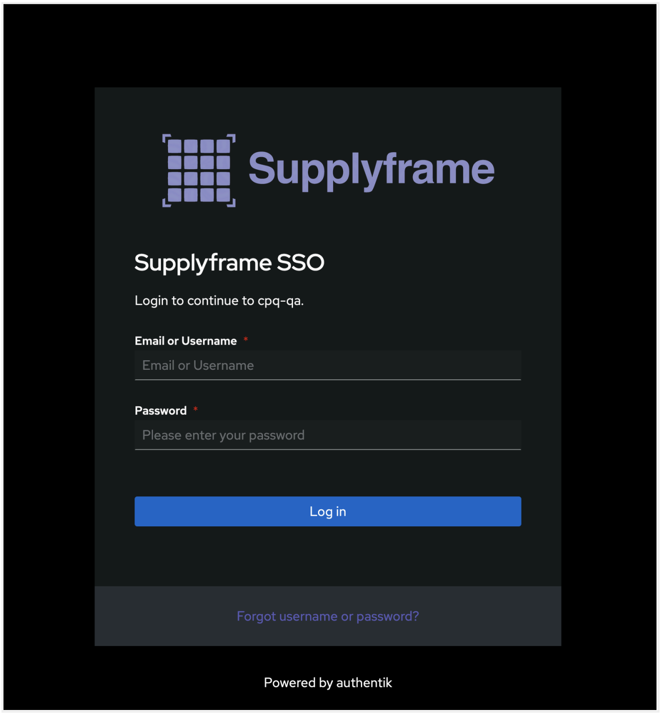
Unauthenticated users accessing the application via a customer subdomain will be automatically redirected to the configured IdP for authentication.



Sign In

When the user selects ***Employee Login***, CPQ initiates a SAML authentication request and redirects the user to the configured IdP.

At the IdP, the user is presented with a login page to enter their credentials. This step verifies the user's identity against the organization's authentication system.



Supplyframe SSO

Login to continue to cpq-qa.

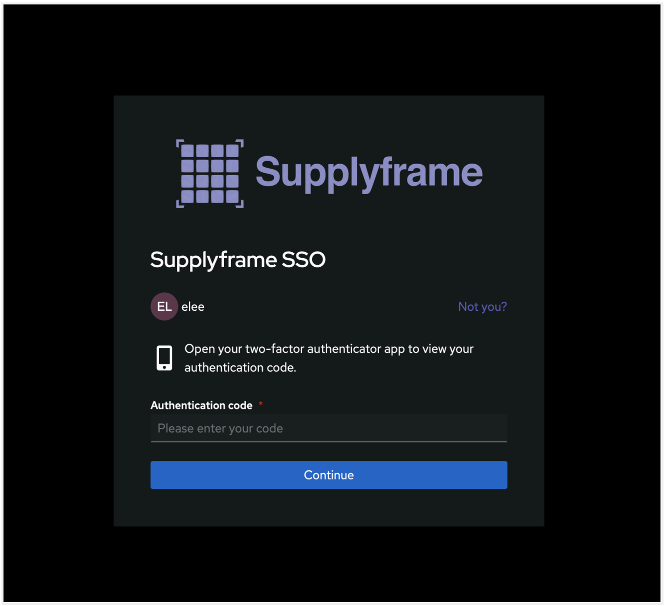
Email or Username *

Email or Username

Password *

Please enter your password

If the credentials are successfully validated, the IdP may require the user to complete additional security steps, such as Multi-Factor Authentication (MFA), depending on the organization's authentication policies.



Supplyframe SSO

EL elee

Not you?

Open your two-factor authenticator app to view your authentication code.

Authentication code *

Please enter your code

Continue

Once the authentication process is completed, the user is redirected back to the CPQ application with a SAML assertion confirming their identity and granting access. The user is now signed in and can use Supplyframe CPQ.