Single Sign-On

PURPOSE

To demonstrate the Single Sign-On (SSO) functionality on CS Lucas.

BACKGROUND

Single sign-on enables users to log in to various apps and resources using a single set of credentials. This simplifies the user experience and enhances security for the business.

CS Lucas supports the “Service provider-initiated” mode of login. This means that user access CS Lucas by navigating to a specifically provided URL by the company (see details in the workflow below).

WHY IS THIS IMPORTANT?

Setting up Single Sign-On will bypass the native CS Lucas user authentication process. Instead, users will be authenticated by the client enterprise identity provider.

PRE-REQUISITE

You must have an identity provider that supports the SAML 2.0 protocol.
The user ID in the identity provider must match the user ID in CS Lucas.

SETUP STEPS

1. Request SSO setup from CS Lucas.
2. CS Lucas will provide a metadata file containing parameters and a security certificate to configure the identity provider.
3. After the identity provider’s configuration is completed, it will generate the corresponding configuration metadata. Provide this information to CS Lucas.

4. Create a test user in the identity provider for testing purposes.
5. After a successful test, CS Lucas will provide a URL for user login.
6. Save this URL as a bookmark and begin using it for logging in.

WORKFLOW

With SSO, the user navigates to a URL provided by CS Lucas. This initiates a background communication between the CS Lucas system and the business's identity provider (or third-party identity provider). Subsequent actions depend on the authentication state of the browser session:

1. If the browser session is not authenticated, the user will be redirected to the identity provider's login page. Upon successful authentication, the user will then be redirected to the CS Lucas welcome page.

2. If the browser session is already authenticated, the user will be immediately directed to the CS Lucas welcome page.

Note:
Please be aware of the following limitations in the native CS Lucas security features when SSO is activated:

– Deactivated user
– IP restrictions
– Multi-factor authentication

These user authentication processes will be bypassed and managed by the client enterprise identity provider.

FREQUENTLY ASKED QUESTIONS

RELATED INFORMATION

CHANGE HISTORY

Date	By	Changes
11-Jan-2024	TS	Created.