

VCOO-163 Log in

Epic	Security
Document status	DRAFT
Document owner	@ Crystal Wang
Designer	
Tech lead	
QA	

User Story Description

As a Generalist SME

I want to log in
So that I can authenticate and begin interacting with the tool

Acceptance Criteria

1. The user is able to access log in option on the landing page
2. The user is able to view credentials fields and 'log in' CTA
3. The user is able to enter credentials and click on 'log in' CTA
 - a. Note: The user's CWB digital bank account credentials will act as a SSO for this portal's access
4. If the user is already authenticated onto CWB digital banking account, the user will be directly authenticated on the VCOO portal (without the need to re-enter the credentials)
5. The user is able to view error messages when entered wrong credentials
6. The user is able to be authenticated using the right credentials and start interacting with the tool

Assumptions:

1. For beta version, we will select certain SME business banking clients and will be sending direct URL to them to access the VCOO portal.
2. Selected SME clients ideally will be existing clients who have 12 months+ data to share.
3. Requirement like accepting T&Cs will be captured under onboarding stories
4. MFA method will follow what already exists for Okta

Specs by Example & Business Rules

#	Given	When	Then	Business Rules
1	The user wishes to log in	The user clicks on the direct URL has been given to them	The user is led to the log in flow	
2	The user is on the log in page	The user enters right credentials and clicks on log in CTA	The user is authenticated and able to start using the tool	
3	The user is on the log in page	The user enters wrong credentials and clicks on log in button	The user is asked to retry	<input type="checkbox"/> error state business rules need to be defined

Dependencies

1. Deloitte to confirm with Temenos where we stand with Okta developments and integration
2. Who is the Octa SPOC (Single Point Of Contact)? Any documentation to share (existing integration standards, guidelines, endpoints, API documentation, any process)
3. How is Okta working (security, white list of IP, any firewall requirements, tenant, environment)?

Our understanding: Visualizer > Fabric > Okta for SSO > Fabric > Visualizer

Story Point Estimation

Story Points:

Data Fields

- Username/ Account #
- Password

Technical Conditions (Architecture)

UX/UI Designs & Considerations

<https://www.figma.com/file/ar67OGMgaAnvtN4rPoGyPy/CWB-Virtual-COO-Prototype-DEV-Handoff?node-id=3454%3A1862>

General Ability Considerations

- The GA version should be able to have OpenID option for other integrations in the future
- The GA version should have API configuration for log in
- The GA version should be adoptable for different authentication method (i.e.: different MFA steps)