Customer Identity Access Management (CIAM) Documentation

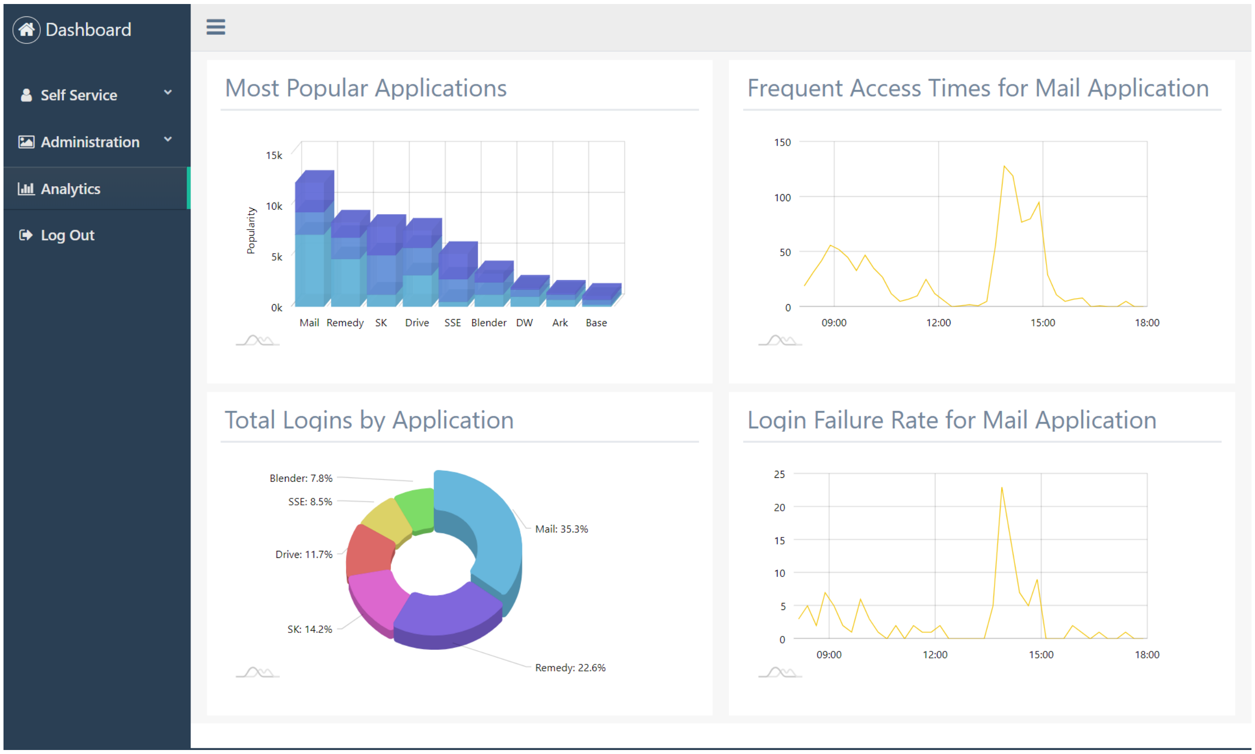
Release 1.0

**Customer Identity
Access Management (CIAM)**

Mar 12, 2020

User Self-Service

CIAM Dashboard is dashboard for Customer Identity and Access Management platform. It is usually integrated with a Single Sign-On (SSO) solutions where applications are protected. The landing portal displays notifications and shortcuts to all protected applications. There is also an analytics page for administrators to monitor statistics like popular applications by departments, total logins by applications, frequent access times for a particular application and login failure rate for a particular application etc.



CHAPTER 1

Introduction

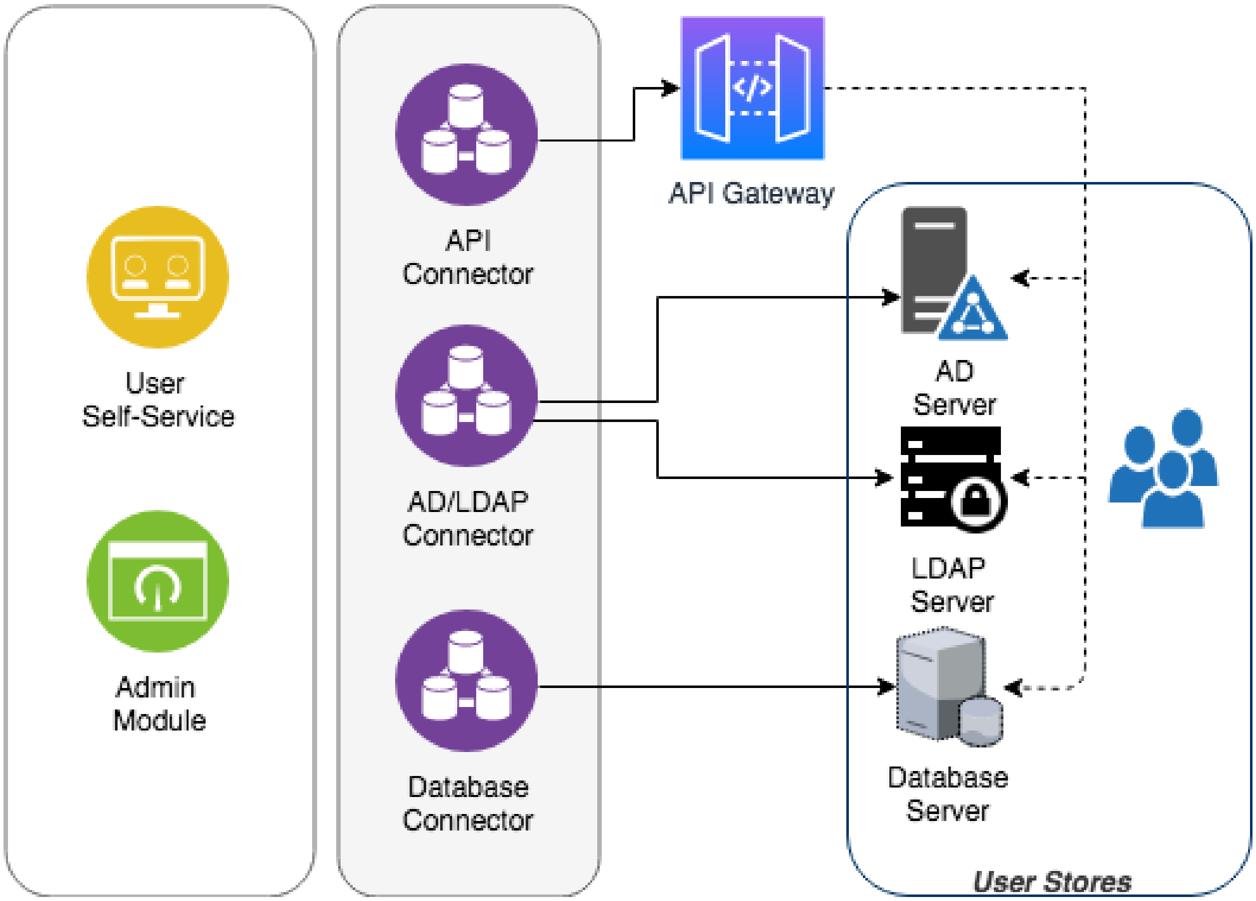
The purpose of this document is to provide the changes made/new features included in this release of the IC.SG CIAM User Self-Service.

1.1 Background

User Self-Service is self-service portal for users who require forget password and password reset services. It is part of the offering from the next-generation Customer Identity & Access Management (CIAM) Dashboard designed users to access protected applications in a single page application.

1.2 Architecture

User Self-Service (USS) is built to integrate with Microsoft Active Directory, any LDAPv3-compliant server and any database server. In addition, for ease of integration, USS has ready-built interfaces to integrate with any API Gateway.


API Gateway
API Connector
User Self-Service
AD Server
AD/LDAP Connector
LDAP Server
Admin Module
Database Connector
Database Server
User Stores

CHAPTER 2

Installation

2.1 Check Prerequisites

Before installing, ensure that you have the following:

- Google account
- **JAVA Development Kit (JDK)**
  - **Supported Versions**

Vendor	Version
OpenJDK	8
Oracle JDK	8

- **Web Application Container**

Web Container	Version
Apache Tomcat	8.5

- **User Store**
  - **Supported User Stores**

Vendor	Version
Microsoft Active Directory	2012, 2016
Wren:DS server	3.0
OpenLDAP server	2.4
389 Directory server	1.4
MySQL Database server	5.7
MariaDB Database server	10.3, 10.4

This guide assumes basic knowledge of tomcat and the databases used.

2.2 Register recaptcha key

1. Go to google's recaptcha creation page
2. **Fill in the form**

Field	Value	Meaning
Label	CIAM	the name for you to identify the site by
Re-CAPTCHA type	Invisible reCAPTCHA Badge	what kind of challenge users will receive when using your site
Domains	e.g. localhost, your-domain-name.com	the domain name of the site that will be protected (including subdomains)
Owners	*leave blank*	people who will have access to these settings

3. Click save

Note: Keep this window open, you will need the sitekey soon

2.3 Deploy the WAR file to Tomcat

Deploy the provided WAR file to the installed Tomcat. Make sure the web application is exploded into Tomcat's webapp folder.

2.4 Enter site-key into the actual html file for forgot password

Note: There are plans to simplify the recaptcha set up process.

You can follow the the latest progress here

1. Open the file at **<tomcat_folder>/web-apps/ciam/forget-password.html**
2. Look for the element with the id "reset-password-button"
3. Change its data-sitekey attribute to the sitekey shown in step 3.

2.5 Enter connection parameters for Database and User Store into the Properties file

1. Open the file at **<tomcat_folder>/web-apps/ciam/WEB-INF/classes/application.properties**
2. Update the parameters for Database, SMTP Server and API Gateway accordingly

2.6 Start Tomcat and Test

Start tomcat and access the URL http://<server_ip>:<port>/ciam/forget-password.html

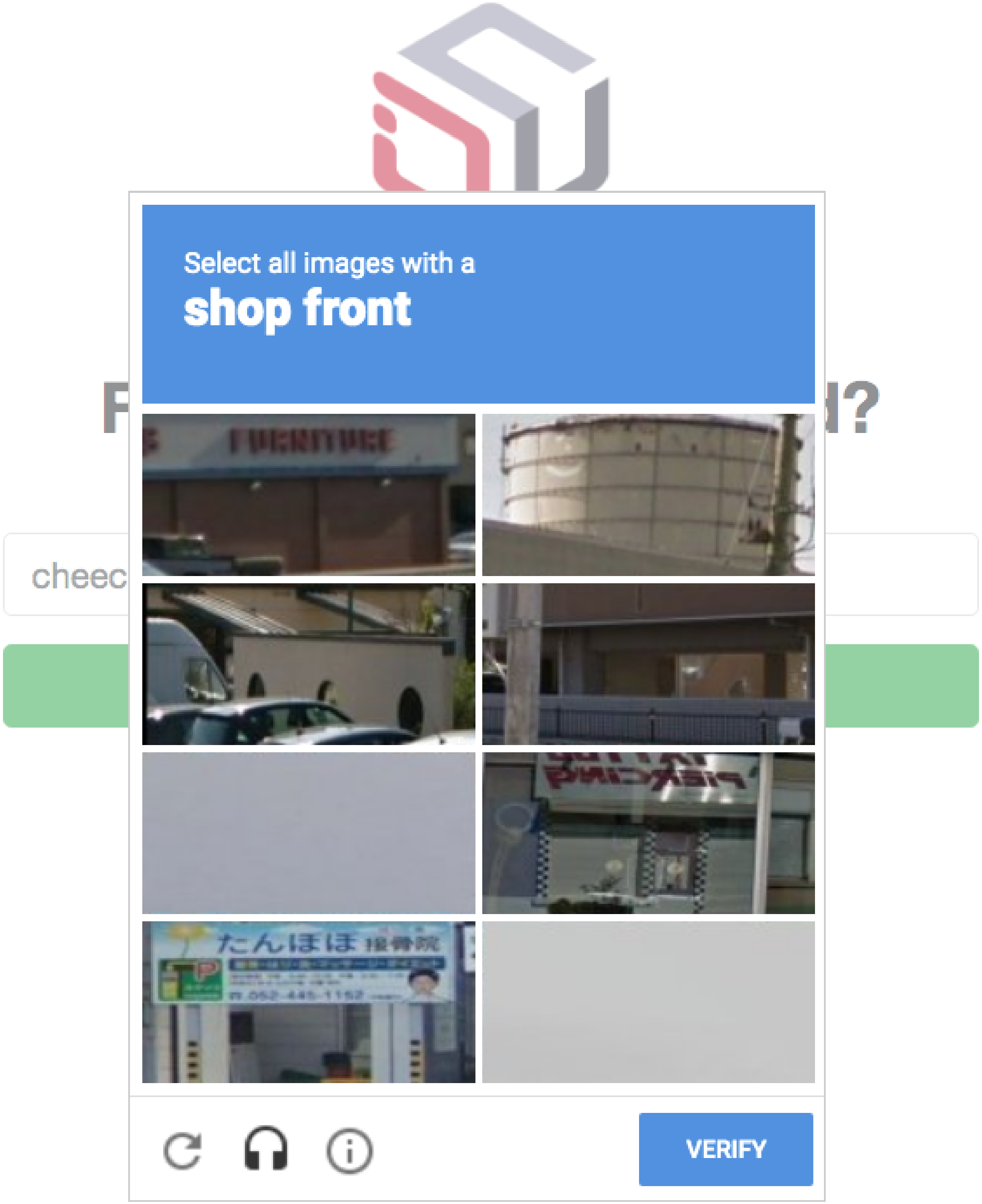
CHAPTER 3

Features

Some of the most notable features in User Self-Service are discussed in this section.

3.1 Google reCaptcha

To avoid automated form submissions and spam, reCAPTCHA from Google, is implemented to attest users if they are human, and not a robot. The Google reCAPTCHA takes-away most of challenges enterprises face in customer on-boarding and provides the right balance between usability and security.



Select all images with a

shop front

CHAPTER 4

Customizations

The purpose of this section is to provide administrators with documentation to customize the IC.SG CIAM User Self-Service (USS).

4.1 Branding

It is possible to change the default logo in USS.

Steps:

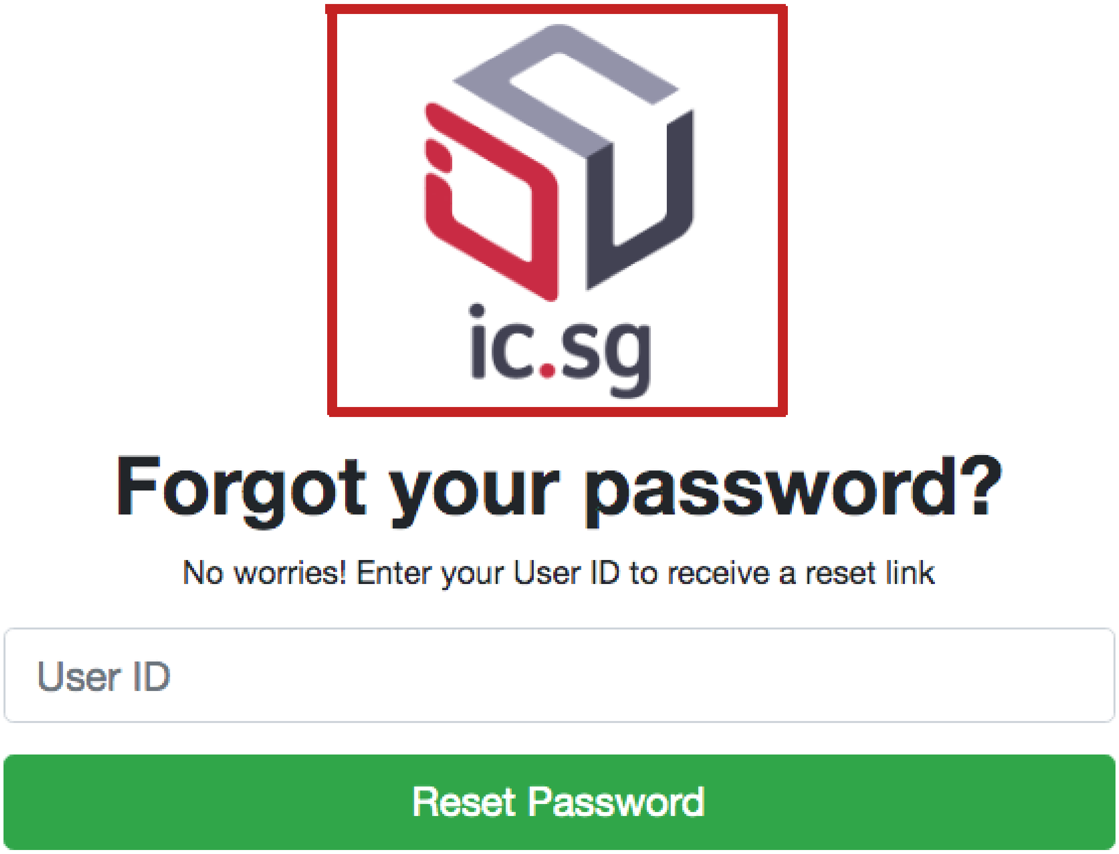
- Prepare a logo file.
- The file name must be **icon-full.png**, no more than 50kB, with dimensions 380px x 480px exactly.
- Upload logo file to webapp/ciam/assets

4.2 Favicon

A favicon (short for favorite icon), also known as a shortcut icon, website icon, tab icon, URL icon, or bookmark icon, is a file containing one or more small icons, associated with a particular website or web page. It is possible to change the favicon in USS.

Steps:

- Prepare a favicon file.
- The file name must be **favicon.ico**, no more than 50kB, with dimensions 64px x 64px exactly.
- Upload favicon file to webapp/ciam/assets



Forgot your password?

No worries! Enter your User ID to receive a reset link

CHAPTER 5

Authors

- JD
- TSO
- FED

CHAPTER 6

Support & License

6.1 Support

If you are having issues, please let us know. We have a mailing list located at: jd@ic.sg

6.2 License

Attribution-NoDerivs CC BY-ND

This documentation is released under a CC BY-ND license.

The documentation is written by experts from IC.SG who work very hard for the successful implementation of Customer Identity and Access Management (CIAM) platform and User Self-Service (USS).

This license lets you reuse the documentation for any purpose, including commercially; however, it cannot be shared with others in adapted form, and credit must be provided to us.