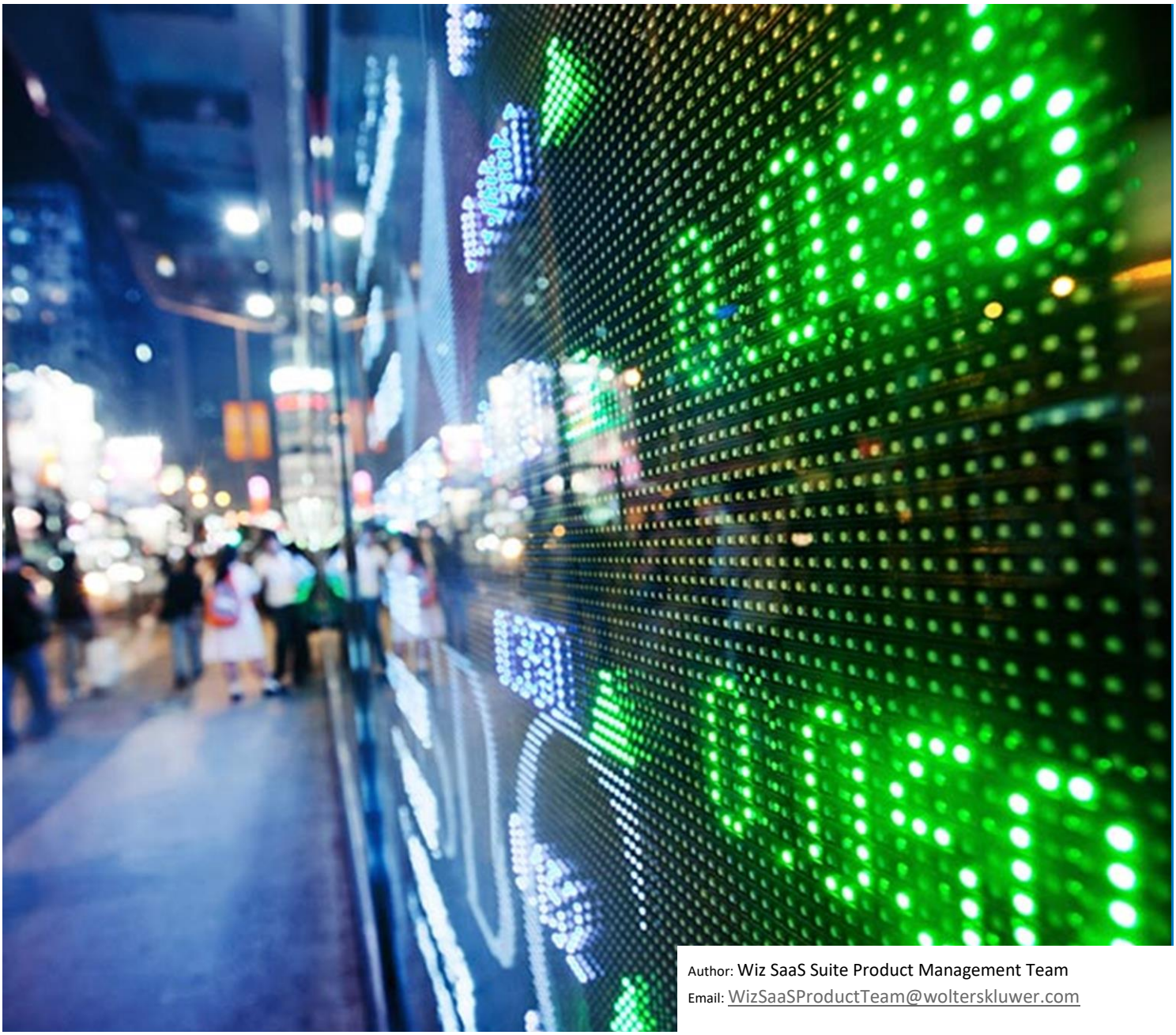
Wolters Kluwer



Author: Wiz SaaS Suite Product Management Team
Email: WizSaaSProductTeam@wolterskluwer.com

August 2024

Financial & Corporate Compliance

Wiz SaaS Suite

Technical Discussion Guide

August 23, 2024
Version 1.12
Wiz SaaS Suite Technical Discussion Guide.pdf

Version	Date	Author/reviewer	Explanation
1.0	4/15/2020	Mindy Marchetti	Initial Creation
1.1	5/27/2020	Mindy Marchetti	Multi-factor Authentication Add
1.2	9/9/2020	Mindy Marchetti	Supported Browsers – Chromium Edge
1.3	12/22/2020	Mindy Marchetti	User Acceptance Testing
1.4	4/1/2021	Mindy Marchetti	Updated browser network & diagram support
1.5	07/21/2021	Mindy Marchetti	Added additional information for Products, Roles, and Permissions
1.6	10/6/2021	Paul Bradt	Added client PC requirements
1.7	2/18/2022	Paul Bradt	Added information on IP Whitelisting
1.8	10/14/2022	Paul Bradt	Added information for FL Lite
1.9	6/13/2023	Paul Bradt	Added information for Fair Lending *Wiz*, updated Security Architecture for new Identity Server version, added data storage model. Updated to refer to all products as *Wiz* SaaS Suite.
1.10	11/18/2023	Paul Bradt	Updated roles and permissions for Small Biz Wiz product and other updates.
1.11	4/19/2024	Paul Bradt	Updated roles and permissions for new functionality.
1.12	8/23/2024	Kevon Paynter	Updated applications and roles to reflect our new Authentication system (OneID)

Disclaimer

Distributed Subject to Terms of a License or other Agreement

The contents of this publication, including its appendices, exhibits, and other attachments, as updated or revised, are highly confidential and proprietary to Wolters Kluwer Financial Services, Inc. or its subsidiaries or affiliates ("Wolters Kluwer Financial Services"). This publication is distributed pursuant to a Non-Disclosure Agreement, Evaluation Agreement, License Agreement and/or other similar agreement(s) with Wolters Kluwer Financial Services, Inc. or its subsidiary or affiliate. Unless otherwise specifically provided in such agreement(s), the reproduction of this publication is strictly prohibited. Use and distribution of this publication are also subject to the responsibilities and obligations of such agreement(s), which require confidential treatment of this publication and its contents. Information in this guide is subject to change without notice and does not represent a commitment on the part of Wolters Kluwer Financial Services.

Do Not Reproduce or Transmit

Unless otherwise specifically authorized in the agreement or license under which this publication has been provided, no part of this publication may be posted, played, transmitted, distributed, copied or reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or retaining on any information storage and retrieval system, without prior written permission from Wolters Kluwer Financial Services.
Requests for permission to reproduce content should be directed to Wolters Kluwer Financial Services, Inc., Corporate Legal
Department, by telephone at 1-800-397-2341.

Not a Substitute for Legal Advice

This publication is intended to provide accurate and authoritative information about the subject matter covered based upon information available at the time of publication. Examples given in this publication are for illustrative purposes only.
Development of this publication and the software (including forms, disclosures, reports, and other documents generated by the software) or other products that it describes was based on Wolters Kluwer Financial Services' understanding of various laws, regulations, and commentaries. Wolters Kluwer Financial Services cannot and does not guarantee that its understanding is correct.
This publication is not intended, and should not be used, as a substitute for legal, accounting, or other professional advice.
Wolters Kluwer Financial Services is not engaged in providing legal, accounting, or other professional services. If legal or other professional assistance is required, you should seek the services of a competent professional. We encourage you to seek the advice of your own attorney concerning all legal issues involving the use of this publication and any products described in this publication. If your interpretations or your counsel's interpretations are contrary to those expressed in this publication, you should of course, follow your/your counsel's interpretations.
The following notice is required by law:

Wolters Kluwer Financial Services' PRODUCTS AND SERVICES ARE NOT A SUBSTITUTE FOR THE ADVICE OF AN ATTORNEY.

Warranty Disclaimer

Except only for the warranties (if any) expressly set forth in the agreement(s) under which this publication is provided (i.e., your agreement or license for the described product), this publication is provided "as is", and Wolters Kluwer Financial Services makes no warranty, express, implied, by description, by sample or otherwise, and in particular and without limitation, makes no implied warranties of merchantability or fitness for purpose. No modifications to this Warranty Disclaimer are authorized unless in writing and signed by the President or a Vice President of the Wolters Kluwer Financial Services entity licensing the product described in this publication.

Table of Contents

1 Overview

The intent of this document is to provide customers and prospective *Wiz* SaaS Suite customers with a technical overview of the system.

1.1 Definition of Terms

The following terms are used throughout this document.

Term	Definition	
WK	Wolters Kluwer, NA	
CRA	Community Reinvestment Act	
HMDA	Home Mortgage Disclosure Act	
Wiz SaaS Suite	The group of products from Compliance Solutions that this document covers, including: • CRA *Wiz* SaaS • HMDA *Wiz* • Small Biz *Wiz* • Wiz Geocoder • Fair Lending *Wiz* (FL) Lite • Fair Lending (FL) *Wiz*	

2 Client Requirements and Recommendations

Users accessing the *Wiz* SaaS Suite will need to meet the minimum system requirements and should also review the recommendations below depending on the work that they are performing.

2.1 Requirements and Recommendations

- **Operating System:** Any that support the officially supported browsers listed below
- **Browser:** Google Chrome, Microsoft Edge
    - See Supported Browsers section for more details.
- **RAM:** Requires 4GB. 8GB or more is recommended for users that will be generating and reviewing reports.
- **Processor:** 2 cores, 2.4 GHz processor or faster
- **Resolution:** Minimum supported is 1440x900.

2.2 Screen Resolution Support

The *Wiz* SaaS Suite is designed to be responsive to different screen resolutions and browser sizing and zoom level. Our minimum supported screen resolution is 1440 x 900. While lower resolutions may work fine in most cases, visual issues that occur below the minimum resolution will not be addressed.

3 Supported Browsers

Users access the *Wiz* SaaS Suite via an internet browser session. The following internet browsers are officially supported:

- Google Chrome (Recommended browser)
- Microsoft Edge (Chromium versions only)

As of May 2021, Internet Explorer is no longer a supported browser.

Due to the frequency of browser updates, we have implemented a grading system to identify how we will respond to support issues relating to different browser and version usages. The browser versions used for testing of each release will be stated in the release notes.

Grading	Support Level	Description
A	Fully Supported	Applies to the current versions and 2 prior versions of the supported browsers that were used in testing of the latest release. All functional and visual items should work as expected and any reported issues will be addressed.
B	Partially Supported	Applies to earlier versions (up to 12 months prior) and newer versions of the supported browser versions indicated in the latest release notes. All functional items should work as expected, but visual appearance may differ slightly. Reported functionality or usability issues will be addressed. Visual issues will be evaluated and fixed if they will cause issues in future releases.
C	Not Supported	Any browser not in the supported list (i.e. Firefox, Internet Explorer) and any browser version that is more than 12 months older than the version stated in the latest release notes.

While the application may work with unsupported browsers, Wolters Kluwer cannot guarantee compatibility with them.

4 Accessing the Application

When the *Wiz* SaaS Suite products are provisioned for a new account, WK creates one initial administrator account. Administrators are considered User group managers and are responsible for creating individual user accounts for their institution.

4.1 Password Requirements

- Must be eight characters long.
- Must contain three of the four-character groups below:
    - At least one uppercase character (A-Z)
    - At least one lowercase character (a-z)
    - At least one numeric character (0-9)
      At least one special character, consisting of the following: ! " # $ % ' ( ) * + , - . / : ; = ? @ [\ ] _ ` { | } ~

      Note: "<" and ">" are not considered valid characters.

Additional Password Requirements:

- Passwords can only be changed once every 48 hours.
- Passwords must change every 90 days.
- When resetting your password, the previous 6 passwords cannot be used. There is no specific time frame required before using the oldest of the 6 passwords other than: "Password cannot be changed prior to 2 days after the last password change".
- If you fail to log in successfully 5 times, your user id will be locked. You will need to contact your system administrator or SupportLine to have it unlocked.

4.2 API Credentials

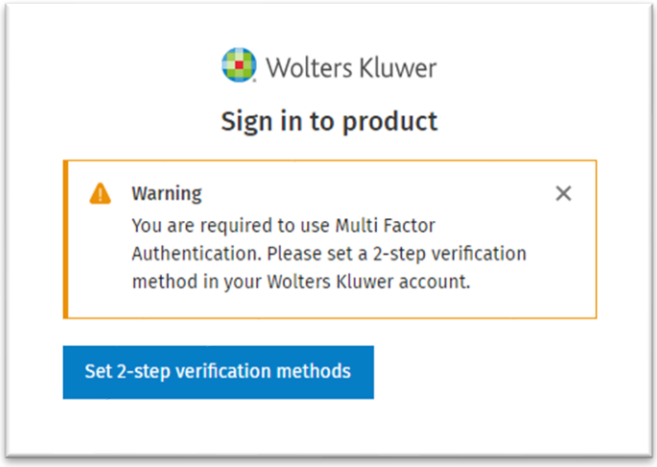
In addition to the functionality available at www.wizenterprise.com, the *Wiz* SaaS Suite offers APIs that integrate into core systems and loan origination systems. Institutions that connect to the applications via APIs are required to use a separate set of API credentials. Administrators can create API Credentials by logging into the application and going to Admin > API Credentials. When the Administrator creates these credentials, they will be prompted to specify between 2-730 days for when the password will expire and are responsible for creating a new password after the specified number of days has passed.

4.3 Multifactor Authentication (MFA)

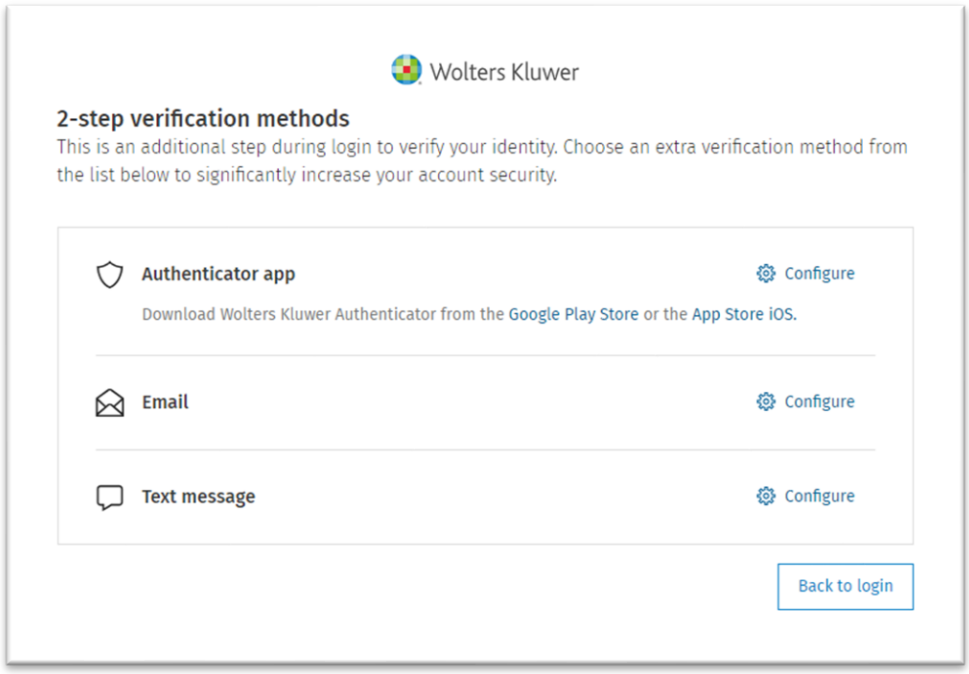
Multifactor Authentication (TOTP) is supported and offers additional security for users logging into an application. A *Wiz* SaaS Suite customer may request that multifactor authentication be utilized for users accessing the application at their institution. WK's default provisioning procedures do *not enable this setting by default,* but it can be enabled either by our customer support team (customersupportwizsentri@wolterskluwer.com) or product management team (WizSaaSProductTeam@wolterskluwer.com) if desired.

The multifactor authentication utilized in the *Wiz SaaS* Suite uses a time-based, one-time password generated by an algorithm that uses the current time of day as one of its authentication factors. After multifactor authentication is enabled, users must either download a TOTP authenticator application, use their email address, or text message to proceed with logging in.

The first time a user attempts to login after MFA has been enabled, they will be prompted to set a 2-step verification method for their account then select from Authenticator app, Email, or Text message.



After configuring the desired verification method, the user will be prompted for the verification code using the configured method whenever they attempt to log into the application moving forward.



Note: Once multifactor authentication has been enabled, all users from that institution must use multi-factor authentication to access the application.

4.4 IP Filtering/Whitelisting

IP Whitelisting is supported and allows for the limiting of access to the system from specific IP addresses or a range of them. IP filtering is done at the account level and applies to all logins.

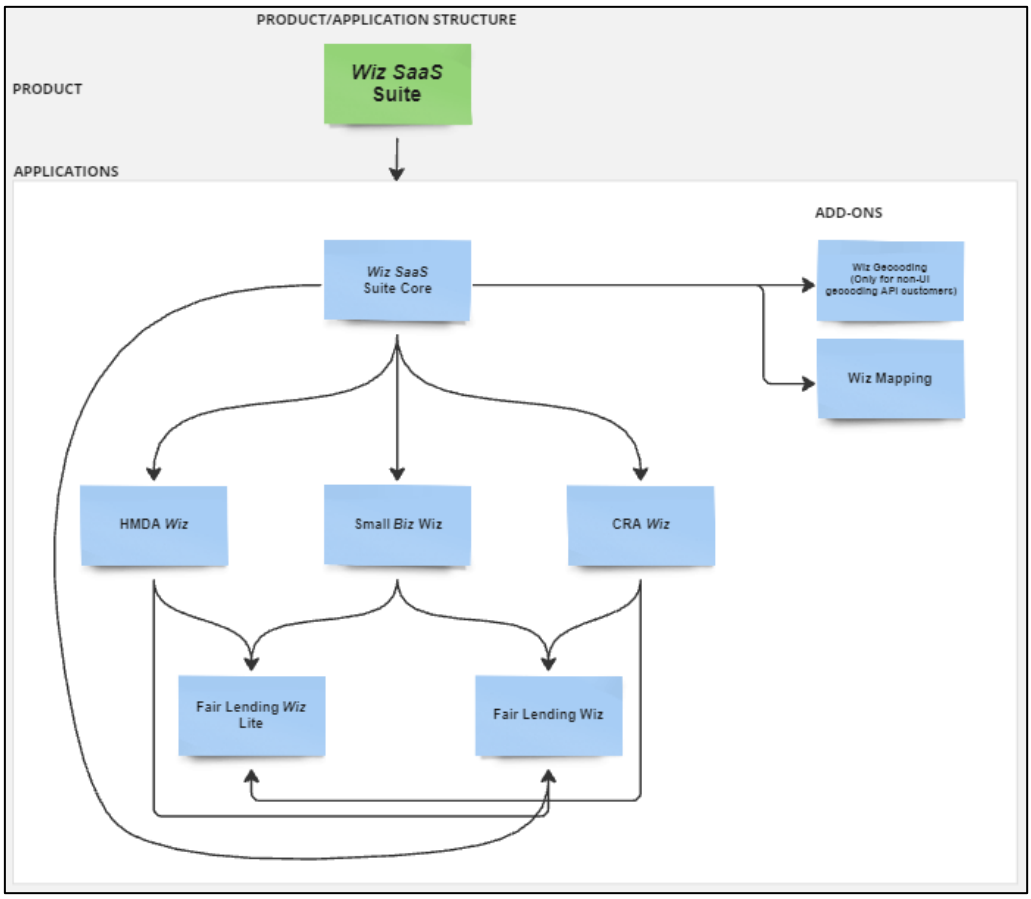
The IP Filtering feature uses the public IP address which may be different than an individual computer's private IP address. Each location that accesses the Internet has a unique 'Public' IP address. The public IP address identifies where an Internet request is coming from and where the response is returned.
A *Wiz* SaaS Suite customer may request that IP Whitelisting be enabled for users accessing the application at their institution. WK's default provisioning procedures does *not enable this by default,* but it can be enabled by our *Wiz* SaaS Suite customer support team @ customersupportwizsentri@wolterskluwer.com or our product management team @ WizSaaSProductTeam@wolterskluwer.com> if desired.

Note: If this feature is configured incorrectly, all users in the account may be blocked from accessing the software. It is important to have someone with network configuration knowledge involved in the implementation of this feature. It is **not** recommended to modify the IP Address Whitelist during regular business hours as users may be negatively affected if changes are made to IP Filtering while using the software.

5 Products, Roles, and Application Structure

5.1 Product/Application Structure

The Wiz SaaS Suite consists of several applications that can be combined in many ways to meet your needs.



5.2 Wiz SaaS Suite Core

The Wiz SaaS Suite Core is the base application that contains most of the common functional areas of the application and is always included. It also contains most of the roles that can be assigned to users.

5.3 HMDA Wiz, Small Biz Wiz, and CRA Wiz

These applications are regulatory compliance products that give users access to different data file types, peer data, and demographics as well as analytics, edit checks, and the ability to submit their data to the regulators.

5.4 Fair Lending Wiz Lite and Fair Lending Wiz

These applications can be used in conjunction with the regulatory compliance products to add enhanced analytics around underwriting, pricing, marketing, and other fair lending analysis.

5.5 Add-ons

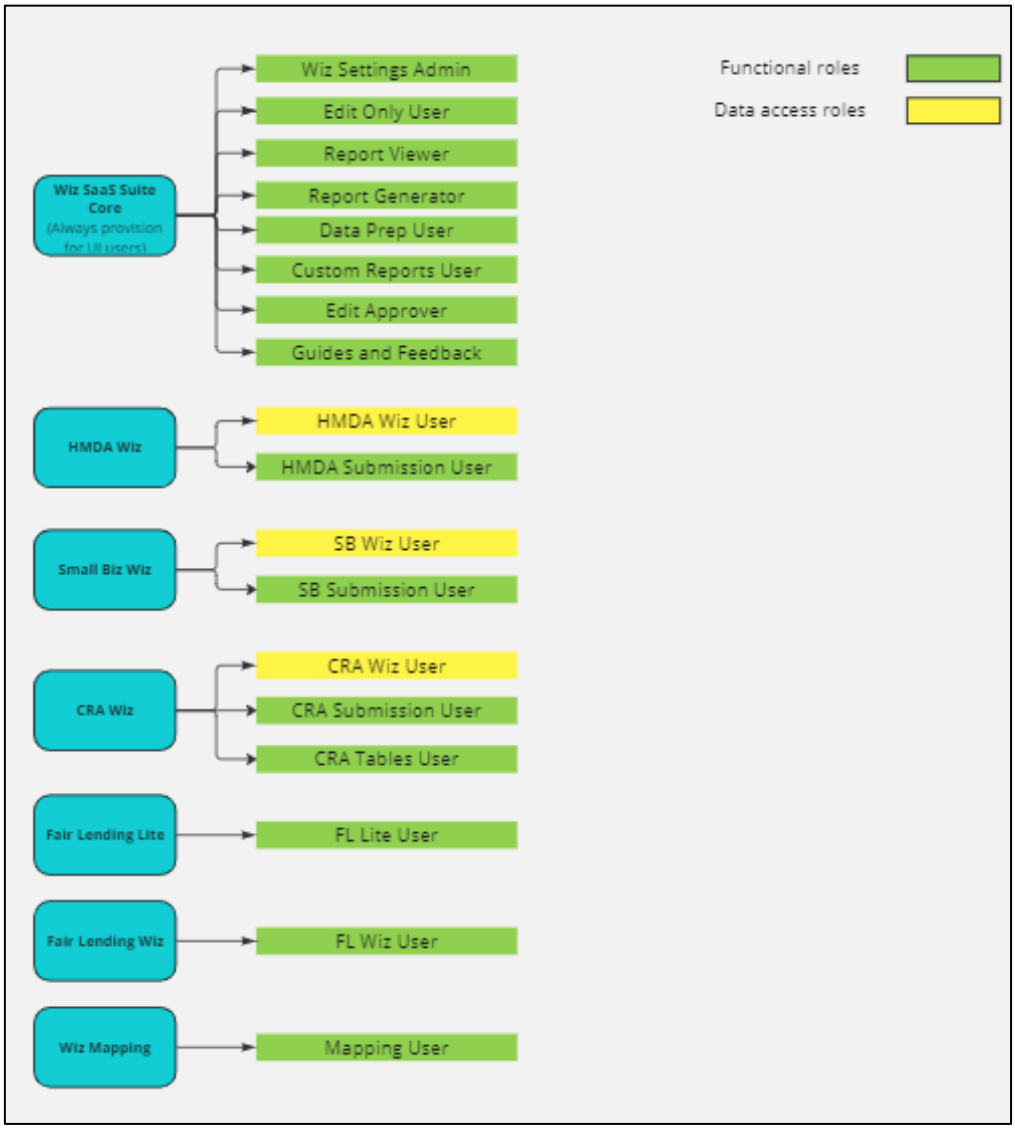
Wiz Mapping can be added to allow users to plot assessment areas and loans on a map for analysis. The Wiz Geocoder is an integration service for providing geocoding and demographic information to other applications.

6 Roles

Roles are assigned to users and control what they can do in the Wiz SaaS Suite. There are two types of roles, functional roles and access roles. Functional roles control use of different components of the system, while data access roles control what types of data that user would have access to within those components. Multiple roles can be assigned to a user to give the permissions they need.

Example: A user that has both the Data Prep User and HMDA Wiz User roles would be able to import data to HMDA DF type files, but they would not be able to import to Small Business DF files if they do not also have the SB Wiz User role.

6.1 Available Roles by Application



6.2 Role Definitions

Role Name	Description
Wiz Settings Admin	Allows the user to access Institution Settings for exemptions, self-identification, and other application settings. When combined with the FL Wiz User, it also gives access to control groups and proxy settings. When combined with the Edit Approver role, it allows users to disable quality edits and warnings that for the file types they have data access roles for.
Edit Only User	Allows the user to select a current file, filter, and use all functionality within the Edit module for file type that the user has data access roles for.
Report Viewer	Allows the user to access Generated Reports and view reports that were generated by other users in the organization, but no ability to generate the reports themselves.
Report Generator	Allows the user to access and generate reports for any areas that they have access to based on the data access roles they have. Also grants the user access to Generated reports so that they can view reports that they have generated or that other users in the organization have generated.
Data Prep User	Allows the user access to File management, Import, Create areas, and User defined edits.
Custom Reports User	Allows the user to access and generate Custom reports (columnar reports and custom tables) and access to the OData links page.
Edit Approver	Allows the user to approve quality edits and warnings at the record level or at the file level.
Guides and Feedback	Enables the feedback button and FAQs, guides, etc.
HMDA Submission User	Allows the user to access Submission and Submission Packages for HMDA DF files.
SB Submission User	Allows the user to access Submission and Submission Packages for Small Business DF files.
CRA Submission User	Allows the user to access Submission and Submission Packages for Small Business and Farm files.
CRA Tables User	Allows the user to access and generate CRA Tables.
FL Lite User	Allows the user to access the Redlining scoping tool as well as the Risk scorecard.
FL Wiz User	Allows the user to access the Redlining scoping tool, all Fair Lending analytics reports, and the Regression and Comparative File Review.
Mapping User	Allows user to access the Mapping tool and the Synchronized map items page.

7 File, Peer, and Demographics Availability by Application

The types of files and data available is dependent on the applications that the organization and/or the user is licensed for.

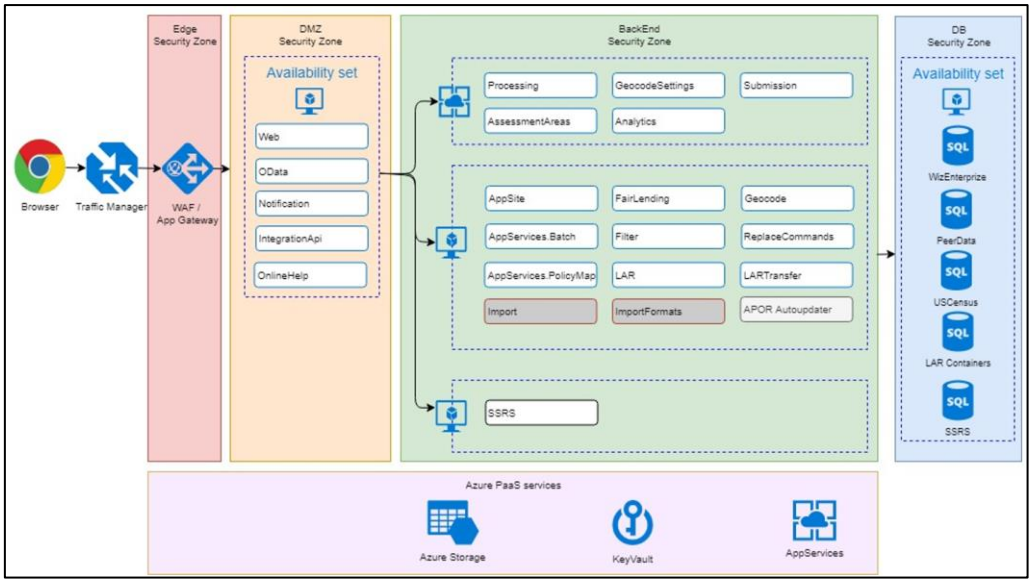
All Applications	
Consumer	File type
Branch and ATM	File type
Other	File type

HMDA Wiz	
HMDA DF	File type
HMDA	File type
Peer Mortgage	Peer
Geodemographics	Demographics

Small Biz Wiz	
Small Business DF	File type
Peer Small Business DF (Once released)	Peer
GeoDemographics	Demographics
Business Demographics	Demographics

CRA Wiz	
HMDA DF	File type
HMDA	File type
Small Business and Farm	File type
Small Business DF (Once CRA Mod goes live)	File type
Community Development	File type
Peer Mortgage	Peer
Peer Small Business	Peer
Peer Small Business DF (Once released)	Peer
Peer Branch and Deposit	Peer
GeoDemographics	Demographics
Business Demographics	Demographics

8 High Level Network / Application Architecture

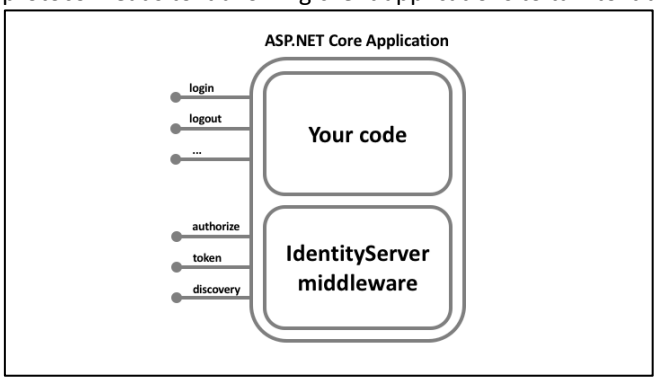


Infrastructure is divided into four different security zones.

- Edge Security Zone is responsible for handling all communications from/to the system secured behind App Gateway with WAF.
- DMZ Security Zone is responsible for handling all communications from/to Web Servers secured with VNET and Firewall. Communications with other security zones are controlled via VNET pairing and IP filtering.
- Backend Security Zone is responsible for handling all App layer components, including App Servers, SSRS Servers, and App Service Environments. All communications are controlled using VNET pairing and Load Balancer configurations.
- Core Security Zone is responsible for managing the data layer. All communications to data layer are controlled with VNET pairing and Load balancer configuration communicating to SQL Server AOAG Listener. Also, SQL Server AOAG is configured to have 2:1 replication with sync commit to secondary replica in primary region and async commit to Tertiary replica in DR zone.
- Internal (WK) Access to all these zones is managed with Express Route Gateway from the WK Backbone. Access is controlled using WK Active directory which is quarterly reviewed.

9 Security Architecture

The *Wiz* SaaS Suite uses OneID for its Authentication and Authorization framework. Identity Server is middleware that adds specification compliant OpenID Connect and OAuth 2.0 endpoints to ASP.NET Core applications. Identity Server middleware adds the necessary protocol heads to it allowing client applications to talk to it using standard protocols.



For authorization the *Wiz* SaaS Suite provides extensive user roles management. Each request is authorized against a token provided by the Identity Server for roles and data access before granting access. Each token has expiration configuration that is used to manage sessions for logged in application use and is maintained in application cookies.

The application automatically logs users out of the application after 30 minutes of inactivity and users are redirected to the application's logout page. New requests are automatically redirected to the login page.

For clients and integrated partners accessing the *Wiz* SaaS Suite via webservices each request is RESTful, meaning no cookie is used, rather each request is authenticated and authorized individually.

10 Internal Security Controls

10.1 Code Security

WK utilizes peer review for Code Security. Peer Reviews are completed on every pull request.

Architectural Review is done for the major features before closing the feature.

10.2 Static Code Analysis Tools

The following static code analysis tools are integrated into the build process:

- BlackDuck identifies and tracks open-source components within applications' source code. It is utilized to minimize security, compliance, and code quality risks.
- Coverity Scan is utilized to find security defects in the application's C#, Angular and JavaScript codebase. It tests every line of code and potential execution path. When an exception is found, the root cause of each defect is clearly explained facilitating efficient remediation.
- CheckMarx SAST (CxSAST) is an enterprise-grade static analysis solution used to identify security vulnerabilities in custom code. This solution is utilized by Wolters Kluwer's Development, Development Operations (DevOps), and security teams to scan source code early in Software Development Lifecycle (SDLC) to identify vulnerabilities and provide actionable insights for remediation.

10.3 Dynamic Scan Tools

Dynamic scan tools are utilized by WK during each development sprint.

- IBM® Security AppScan® automates application security testing by scanning applications, identifying vulnerabilities, and generating reports with intelligent fix recommendations. This solution provides Wolters Kluwer both static and dynamic application security testing throughout development of the applications.

10.4 Manual and Automated QA Testing

WK's Quality Assurance team completes functional testing, load testing, performance testing, and regression testing on each iterative development sprint.

10.5 Penetration Testing

WK employs a third-party vendor for Penetration Testing on the *Wiz* SaaS Suite. Penetration Tests are conducted annually.

10.6 Environment Accessibility

Access to production environments and other Azure objects is controlled and maintained using Active Directory groups and policies defined under WK's Networking Backbone. Membership to Active Directory groups is reviewed on a quarterly basis. Members of the Development, Quality Assurance or DevOps teams do not have membership to these Active Directory groups.

10.7 Patching and Security Updates

Patching and Security updates for the application and its environment are tracked and maintained by WK's GBS-IT Operations Team.

10.8 Anti-Virus Scans

All virtual machines in the *Wiz* SaaS Suite environment are configured with McAfee anti-virus agents. Azure Storage Accounts and Azure App Services are protected using Microsoft Antimalware.

10.9 Additional Security Tools

In addition to the above-mentioned security scans, the following security tools are installed on all the virtual machines in the *Wiz* SaaS Suite environment:

- CrowdStrike Falcon stops breaches via a unified set of cloud-delivered technologies that prevent all types of attacks — including malware.
- OpsRamp centralizes infrastructure monitoring across hybrid workloads with one system of record that gives a unified view of system availability and performance.
- Snow Inventory Agent discovers all assets including hardware configuration, software deployments and usage.

11 Data Storage Model

The *Wiz* SaaS Suite stores data in SQL Server where data is encrypted using SQL Server Transparent Data Encryption (TDE). It is configured with SQL Server Always on Availability Group (AOAG) for High Availability and Disaster Recovery. All temporary files that are either uploaded to or generated by the *Wiz* SaaS Suite are stored in Azure Storage Account which encrypts the data using Microsoft Managed Keys. It is also configured as RA-GRS for High Availability and Disaster Recovery.

11.1 *Wiz* SaaS Multi-Tenant Data Storage

The *Wiz* SaaS Suite is a multi-tenant platform where the customer data is logically segregated in different data stores and the user access to this data is enforced in the application through access control. Each Customer is mapped to a unique Account ID and all the customer data is stored under this unique account ID. Users are configured under this unique Account ID and access control is enforced using the combination of Role and Account ID access levels.

All the data stored in SQL server and Blob storage is encrypted at Rest and Transit. Data is encrypted using AES 256 algorithm and traffic is encrypted using TLS 1.2 protocol.

11.2 Loan Data

Loan records are stored in Loan record containers, The *Wiz* SaaS Suite platform has multiple containers, and the system creates and maintains a mapping between the containers and the Accounts. System creates account specific Schema's and Tables to store customer supplied Loan Data inside the container assigned to the account. The system can support a mapping between a single customer to a single container.

11.3 Fair Lending Reports

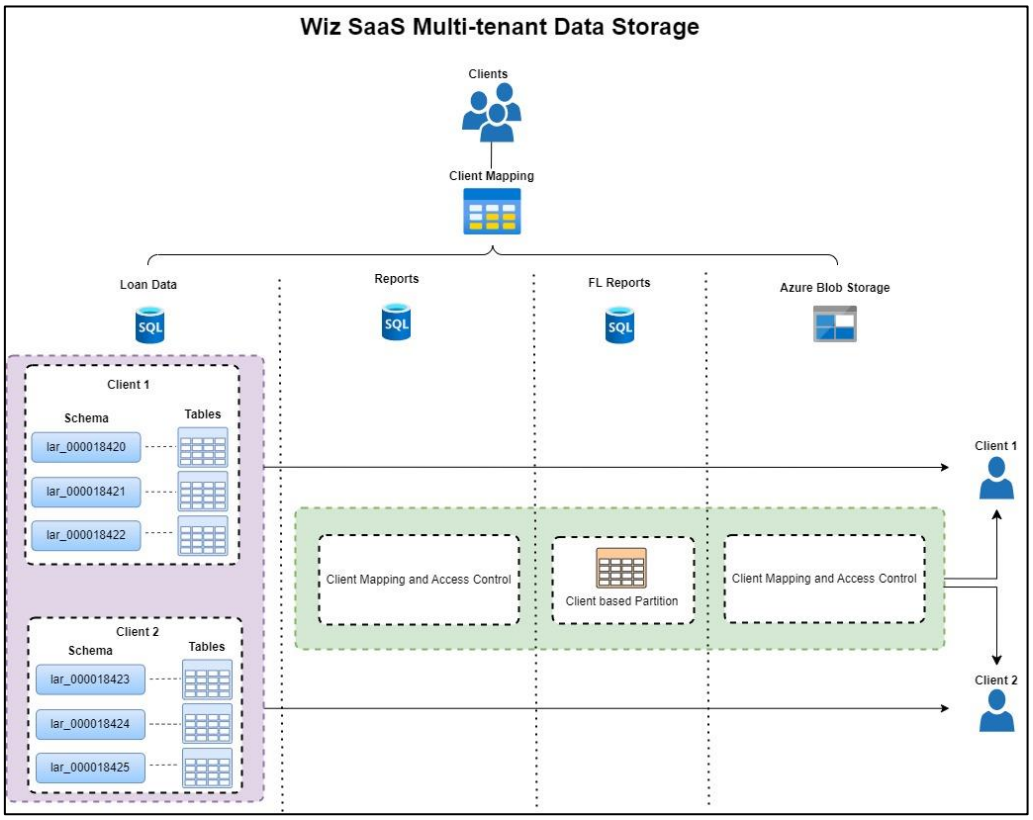
The system is designed to cache the Fair Lending reports for a period of 7 days. The data is segregated using SQL partitions. All cached reports are stored under Account and User level mapping. The system enforces access control based on the user Account and Role. The reports cache can be cleared only by the requesting user on demand prior to system auto purging it.

11.4 Reports

The system is designed to cache the reports for a period of 7 days. All cached reports are stored under Account and User level mapping. The system enforces access control based on the user Account and Role. The reports cache can be cleared only by the requesting user on demand prior to system auto purging it.

11.5 Blob Storage

Customer supplied Loan record files are uploaded in the Blob storage and stored for a period of 48 hours. These files are purged automatically by the system after 48 hours.
Every file uploaded is assigned a unique file name (internal) and account level mapping.
Blob storage can only be accessed by the system services and the system applies role and account level access control.


Wiz SaaS Multi-tenant Data Storage
Clients
Client Mapping
Loan Data
Reports
FL Reports
Azure Blob Storage
SQL
SQL
SQL
Client 1
Schema
Tables
lar_000018420
lar_000018421
lar_000018422
Client 2
Schema
Tables
lar_000018423
lar_000018424
lar_000018425
Client Mapping and Access Control
Client based Partition
Client Mapping and Access Control
Client 1
Client 2

12 Data Privacy & Encryption

Data at rest are encrypted using TDE, Vormetric, and Azure Storage encryption. Data in motion are encrypted using HTTPS over TLS 1.2 and higher, along with Web Application Firewall (WAF) from Azure Application Gateway.

- SQL Data Encryption – Transparent Data Encryption (TDE) is enabled in the SQL database. TDE performs real-time I/O encryption and decryption of the data and log files.
- Local file encryption – Physical files in the Virtual Machines are encrypted with Vormetric using SHA 256 keys. Vormetric provides transparent and continuous file-level encryption and protects against unauthorized access by users and processes in physical, virtual, and cloud environments.
- Azure Storage Encryption - Storage accounts are encrypted using Microsoft Managed Keys. Storage service encryption protects data at rest. Azure Storage encrypts data as it's written in Wolters Kluwer's data center and automatically decrypts it as it is being accessed.
- Data in motion encryption - HTTPS communication is enforced to ensure security for data in motion. SSL certificates with SHA256-RSA encryption along with WAF from App Gateway makes sure any communication to/from the Wiz SaaS Suite is secured, encrypted, and filtered. The SSL certificate encrypts the information that users supply to the site. HTTPS is also secured via Transport Layer Security (TLS) protocol. TLS helps provide data integrity, which helps prevent the transfer of data from being modified or corrupted, and authentication, which proves to users that they are communicating with the intended website.

Note: Only TLS 1.2 or higher protocols are enabled for communication to The *Wiz* SaaS Suite.

13 Data Center

WK uses Microsoft Azure to host its *Wiz* SaaS Suite applications. These applications are hosted in Azure US South Region paired with Azure US North Central Region for disaster recovery.

Microsoft Azure Data Center maintains more than 90 compliance certifications, including over 50 certifications specific to global regions and countries, such as the US, the European Union, Germany, Japan, the United Kingdom, India, and China.

The Microsoft Azure Data Center maintains compliance for SOC I, II and III, ISO 9001/27001, NIST 800-171, FedRAMP and the FFIEC.

For more details on compliance please visit the following link: https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/

13.1 Data management & Accessibility

Data at rest are encrypted and access are controlled using WK's Active Directory which is quarterly reviewed. Any updates or changes to the environments are managed using WK Change Management System (CMS). SQL Server activity logs and Azure activity logs are also reviewed on a quarterly basis.

13.2 Compliance Certifications

The *Wiz* SaaS Suite is SOC II certified. SOC II audits are completed annually.

WK is also in the process certifying the applications for NIST 800-171 compliance.

For a copy of the application's SOC II report please contact your Wolters Kluwer Account Representative.

13.3 Application Availability

Please refer to Software Support Services documentation for details around application availability.

14 User Acceptance Testing

The *Wiz* SaaS Suite (CT) environment is available to clients who want to test program and data updates in advance of production deployments.

For additional information on accessing the CT environment please refer to the following document; *Wiz* SaaS Suite Client Test Procedures.pdf.