Last Updated: 5/19/23

Workiva Sync Technical Details

This document will provide IT teams the information needed to get the Workiva Sync app for Microsoft Excel installed. Workiva Sync allows Workiva users to synchronize information from an Excel spreadsheet on your computer to your Workiva account, allowing you to create new spreadsheets or update existing sheets with data on your computer in just a few simple clicks.

Versions

There may be situations where we have security improvements or breaking changes where you will be notified in advance of the upcoming release. However, since Workiva Sync's functionality is web-based, Workiva can update Workiva Sync without requiring a new app version be installed.

Release Notes

We publish our release notes so that users can see what's included in each version. The release notes can be found at:

https://support.workiva.com/hc/en-us/sections/4404206165268-Release-Notes

Installation Method

Workiva Sync is an Office Add-in installed via Microsoft AppSource which does not involve code that runs on the user's device or in the Office client. Microsoft Excel reads Workiva Sync's manifest file to populate ribbon buttons and menu commands, and Excel loads Workiva Sync's provided HTML code to render the Workiva Sync panel experience inside of Excel. Requests made from this client experience execute in the context of Excel's default browser in a sandbox.

Because of Workiva Sync's modernized Add-in architecture and installation method, there is no offline installer for Workiva Sync. Updates to Workiva Sync occur automatically. The installed version of Workiva Sync will typically only be updated when a change to the manifest file is needed. Workiva will provide access to the Workiva Sync manifest file if it cannot be added via the Microsft Appsource.

More background can be found at:
https://learn.microsoft.com/en-us/office/dev/add-ins/overview/office-add-ins#how-are-office-add-ins-different-from-com-and-vsto-add-ins

Installation Requirements

User Permissions

The user account performing the installation must be an administrator on the PC in question.

Prerequisites

- Excel on iPad
- Excel on Mac (Microsoft 365)
- Excel 2016 or later on Mac
- Excel 2019 or later on Mac
- Excel 2016 or later on Windows
- Excel 2019 or later on Windows
- Excel on Windows (Microsoft 365)
- Excel on the web

Certain versions of Excel 2016 and Excel 2019 use IE11 as the integrated browser with no method of adjusting which browser is used. For more information, see the following article from Microsoft:
https://learn.microsoft.com/en-us/office/dev/add-ins/concepts/browsers-used-by-office-web-add-ins

External communication

Ports and Protocols

Workiva Sync uses HTTPS and port 443 for all communications with Workiva in order to ensure a secure connection to the region used. If the appropriate proxy configuration option is not available we recommend whitelisting all traffic to the region (domain). We do not recommend whitelisting based on the IP address currently associated with the
domain, because the IP for either domain could change to another IP address frequently.

Domains for Regions:

- United States - app.wdesk.com
- European Union - eu.wdesk.com
- Asia-Pacific – apac.wdesk.com

Network (Proxy) Configuration

Workiva Sync executes actions in the context of the default browser used by Microsoft Excel. Workiva Sync provides a manifest file to Excel to facilitate loading the Workiva Sync panel in the Excel experience via HTML (viewable in app). Workiva Sync relies on the default browser's proxy configuration.

Workiva Login

The Workiva Sync login and authentication process uses the existing login in the user's default web browser. The login is launched from the Excel add-in to the default browser to create a shared login session from Wdesk. All login features such as Single Sign-On (SAML) or Browser Validation are supported as a direct result of utilizing the browser-based login

Note: this is not true in the beta version of Workiva Sync, which uses a client ID/secret generated from an OAuth2 Grant for authentication.

Assemblies Included with Workiva Sync

These assemblies are included with the Workiva Sync installation. Workiva may disclose additonal libraries in the future as necessary.

Microsoft Libraries

-Office JavaScript API library

Third Party Libraries

https://github.com/Workiva/workiva_sync/blob/master/package.json#L31

Local Error Log

Not available at this time.

Frequently Asked Questions

Information on data storage, encryption, etc. is available for download via the Workiva Security and Compliance Document Request Portal.

Data Management:

How is the data stored?

- Workiva Sync syncs to Spreadsheets, which uses AWS RDS.
- Workiva Sync does not store any data of its own as it merely facilitates communication to sync data between a given local Excel sheet and the Workiva

platform using Workiva's Platform Open API (https://developers.workiva.com/workiva-platform/reference/platform-spreadsheets)

Additional data storage details:

- app.wdesk.com primarily used by companies based in North America, stores data in data centers in the United States of America.
- The primary Google Data Center for Workiva in the United States, is Council Bluffs, IA and the backup is Mayes County, OK and South Carolina (nam 5).
    - http://www.google.com/about/datacenters/inside/locations/index.html
- The primary Amazon Data Centers and Availability Zones for Workiva in the United States are Northern Virginia with us-east-1a, 1b, 1c, 1d, 1e, 1f
    - https://aws.amazon.com/about-aws/global-infrastructure/
- Cloudflare - Processed at cloud node closest to the user accessing (Web traffic data: Global (see Cloudflare Global Network: https://www.cloudflare.com/network/)
    - No storage of data with Cloudflare.

How is data encrypted?

- Workiva Sync data is encrypted and logically segregated at rest.
- Workiva Sync uses database encryption and application-level encryption. Additionally, BYOK customers benefit from field-level encryption.
- Workiva Sync uses AES 256 encryption algorithm to encrypt data at rest.

Connection between Workiva Sync and the Workiva Platform:

Workiva Sync communicates with the Workiva Platform via REST calls initiated from the customer's environment.

- TLS 1.2 is used for end-to-end encryption.
- API calls use the following whitelisted HTTP methods:
    - GET
    - PUT
    - POST
    - DELETE

Authentication

Workiva Integration Users with an Oauth2 grant can initiate REST API requests in accordance with the user's permissions, configurable by a Workiva Administrator. When the Oauth2 grant is created and assigned to a user by a Workiva Administrator, a Client ID and a Client Secret are created.

This Client ID and Client Secret are included in a POST request to the Oauth2/token endpoint to obtain a bearer token. When accessing the API, authentication is done using the bearer token.

- The Client ID is not classified as a secret and is stored in a Google Data Store

- The Client Secret is confidential and is stored in a Google Data Store and encrypted at rest via AES-256.
- The generated, signed bearer token has a max age of 10 minutes and is validated server-side via Public Key Infrastructure (PKI) service.

All of this is encrypted in transit using TLS 1.2+ over HTTPS/443. Additional security controls include Oauth2 grant expiration (required) and IP restrictions. The Client Secret can also be reset at any time by an authorized Workiva Administrator. Additional information on Workiva's API can be found at https://developers.workiva.com/

Multi-factor Authentication is supported, based in email with a configurable length of time. Additionally, access may be restricted by an IP allow list configured per organization.

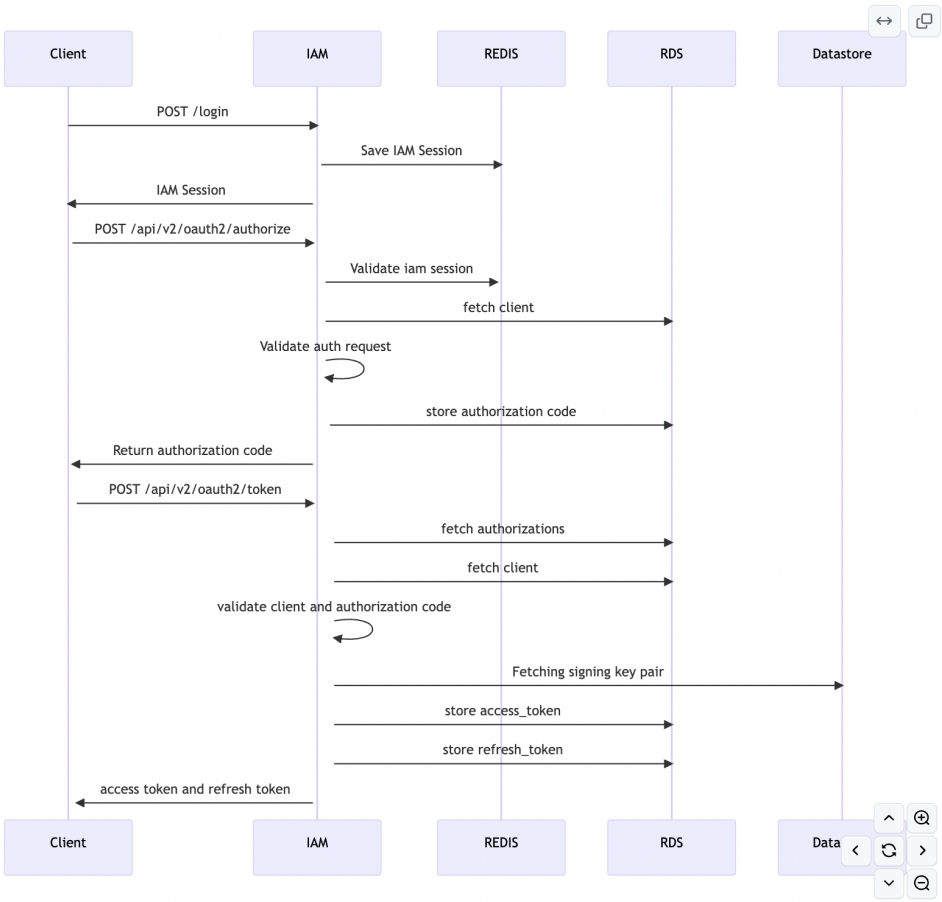
When authenticating via username and password, Workiva follows OWASP Standards for password requirements.

- Min of 16 characters
- No requirement on complexity or password rotation.

Authentication to Workiva Sync uses tokens as follows:

- 3 token types:
  - access token: jwt of variable length
  - id_token: jwt of variable length
  - refresh_token: 96 characters
- Use expiration dates and unique IDs.
- Tokens are typically rotated before the expiration time of the token, however this varies per client.
  - client_credentials: 60 minutes
  - public_api: 60 minutes,
  - implicit_grant: 10 min,
  - acf_token: 10 min,
  - refresh_token: 30min

API sessions are managed via spring session in redis.



Data Transfer

Pertinent requests go through an AWS API gateway for header validation using JSON schema.

Workiva Sync is a web app designed with data security in mind. Only data pertinent to making the request to Workiva's public API is transferred when making a request to Workiva. This may include authentication headers, query parameters, and the post body. Workiva's response to Workiva Sync only includes data pertinent to servicing the request such as status, error codes, or specific content such as sheet names.

Logging

Usage of Workiva Sync and Workiva public APIs generates data which is logged for support and security purposes. The following activities are logged:

- Authentication
    - Login
    - Logout
    - Failed login

- Authorization attempts
    - A policy evaluator checks to ensure user is correctly authorized. When records do not match, the following fields are logged (IDs only):
        - User ID
        - Resource IDs
        - Result of access request (bol)
- Changes to authentication configuration
- Password changes

IP Validation
With regard to IP validation, the behavior exhibited by the Workiva Sync application is no different from existing controls as it leverages all of Workiva platform's standard APIs to facilitate communication (https://support.workiva.com/hc/en-us/articles/360035646452-Set-access-restrictions).

Controls against XSS attacks
Workiva relies on standard libraries to handle output sanitization. The application leverages the React library which will escape special characters that have significance to web content parsers while also considering context. As an additional defense-in-depth measure, a CSP has been defined for the corresponding service.

Controls against clickjacking attacks
In addition to the mitigations provided by office.js (contained within L76 of https://appsforoffice.microsoft.com/lib/1.1/hosted/office.js),

Workiva has also taken additional precautions as recommended by Microsoft in the following documentation: https://github.com/OfficeDev/office-js-docs-pr/blob/7333f011896b73a25c8eb34227ddd19ceb224f5e/docs/concepts/privacy-and-security.md#tips-to-prevent-clickjacking.

Effectively, Workiva Sync leverages the dialog api and requires users to authenticate as a form of confirmation in order to proceed with Add-in use.