Workstation Integrations Security

Brief Overview

Workstation uses two types of secured standards when connecting an integration:

1. API Key – same permissions level for all users to the application. Integration will be connected automatically on default after the admin enables it on Console.
2. OAuth2.0 – permissions level according to the user's permission in the actual application connected. Integration requires user's consent (connect the app manually) after the admin enables it on Console.

What is OAuth2.0

OAuth 2.0 is a secured data sharing standard. This authentication and authorization standard protects user data by providing access to the data without revealing the user's identity or credentials. That is for Workstation to make requests for data to appear in the Enterprise Search and home screen widgets, without accessing passwords and other sensitive information.

OAuth 2.0 enables applications to access each other's data without revealing the user's credentials. This is done through the use of tokens, which are issued by the authorization server and can be used to access the protected resources on the resource server.

Sensitive data such as credit card numbers, medical records, bank statements, or passwords are stored remotely and given a token ID so that merchants and 3rd parties (in this case, Workstation) will not have access to them.

Advantages of OAuth 2.0

Other than the fact that the user's password is not revealed by the 3rd party integration (in this case, Workstation), one of the main advantages of OAuth 2.0 is that it allows users to revoke access to their resources at any time. If users no longer need this 3rd-party integration, they can simply revoke the application's access to their resources. This is not possible with traditional username and password authentication, where the user would have to remember to change their password to revoke access.

In addition, OAuth 2.0 supports different grant types, which allows the authorization server to issue tokens in different ways. This flexibility allows the authorization server to choose the most secure grant type based on the specific requirements of the client and the user, and share only the most relevant data according to predefined scopes.

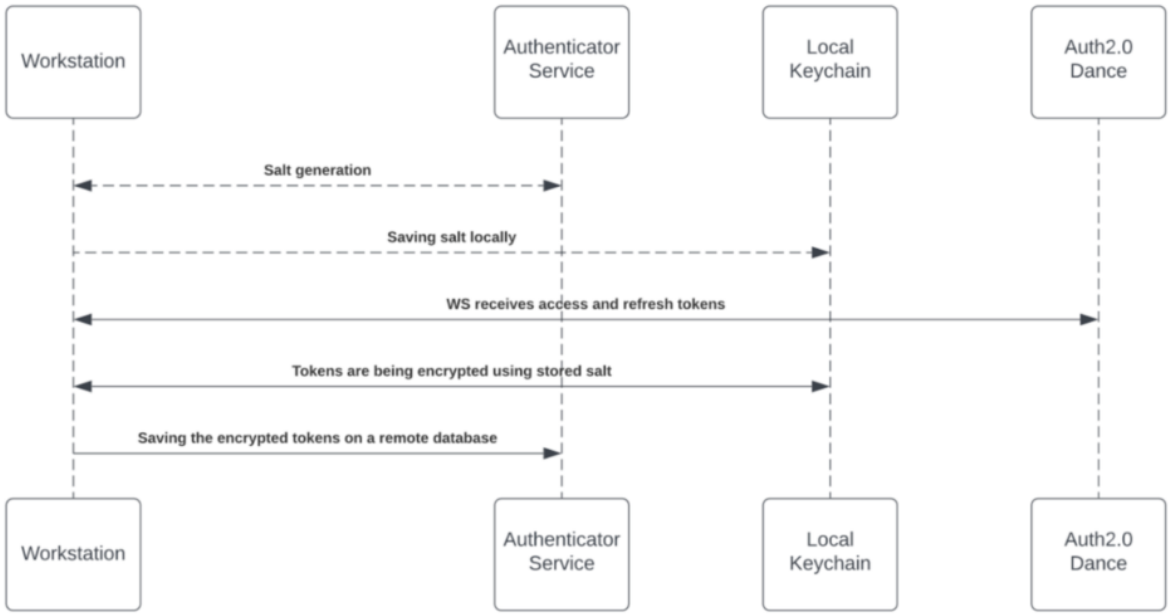
OAuth 2.0 has a flexible protocol that relies on SSL (Secure Sockets Layer) to ensure that data between the web server and browsers remain private. SSL uses cryptography industry protocols to keep data safe.

Refresh Tokens Encryption

Each time a new access token is granted to the Workstation, the application will encrypt the access and refresh tokens and store it in a remote database.

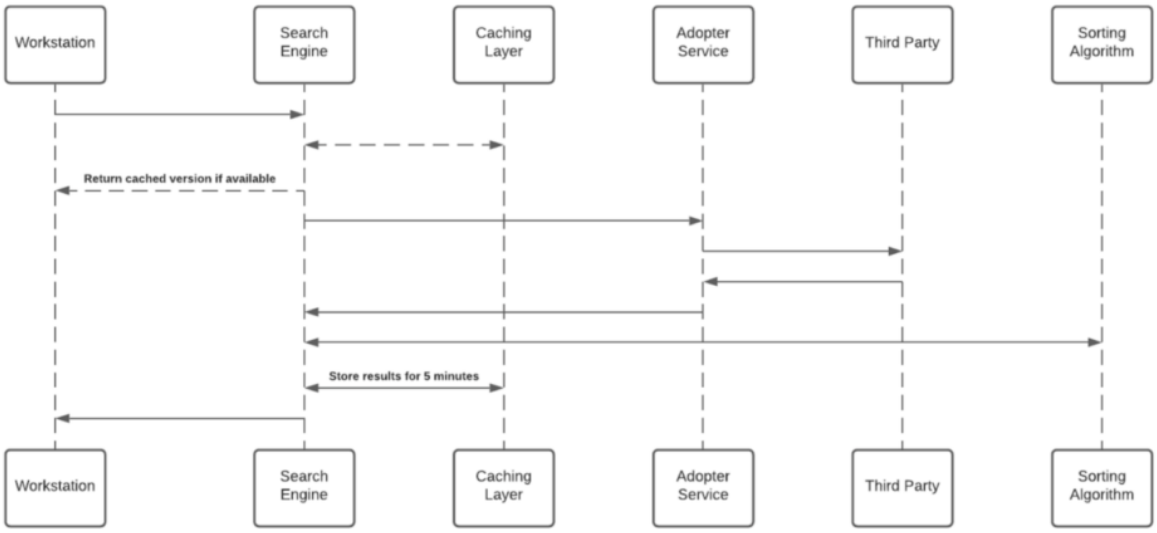
The encryption process includes a unique private key (**salt**) that is generated for each individual at the very first bootstrap and stored in the local machine Keychain. The salt is irreplaceable and not restorable – losing it causes the access tokens to be voided. This security measure is being taken to eliminate identity spoofing when accessing high-sensitive data.

See the diagram below to review the salt generation and storage flow.



Enterprise Search Security

Workstation Enterprise Search doesn't index 3rd-party data on an independently searchable database. See below sequence diagram describes the searching algorithm:



Cache layer saves results for a period of five minutes.

Each Adopter Service creates a unique identifier for the results which is meaningless without access to the 3rd-party and stores it in the graph database.

Read more about the Enterprise Search security in this article:
https://support.walkme.com/knowledge-base/workstation-enterprise-search/