

Sécurité des intégrations de Workstation

Aperçu général

Workstation utilise deux types de normes sécurisées lors de la connexion d'une intégration :

1. Clé API - le même niveau d'autorisation pour tous les utilisateurs de l'application. L'intégration sera automatiquement connectée par défaut après l'activation de l'administrateur sur la console.
2. OAuth2.0 - niveau d'autorisation en fonction de la permission de l'utilisateur dans l'application réelle connectée. L'intégration nécessite le consentement de l'utilisateur (connecter l'application manuellement) après l'activation de l'administrateur sur la console.

Qu'est-ce qu'OAuth2.0

OAuth 2.0 est une norme de partage de données sécurisée. Cette norme d'authentification et d'autorisation protège les données d'utilisateur en fournissant l'accès aux données sans révéler l'identité ou les informations d'identification de l'utilisateur. Cela permet à Workstation de faire des demandes de données qui apparaissent dans les widgets de recherche d'entreprise et d'écran d'accueil, sans accéder à des mots de passe et d'autres informations sensibles.

OAuth 2.0 permet aux applications d'accéder aux données les unes des autres sans révéler les informations d'identification de l'utilisateur. Cela se fait grâce à l'utilisation de jetons qui sont émis par le serveur d'autorisation et peuvent être utilisés pour accéder aux ressources protégées sur le serveur de ressources.

Les données sensibles telles que les numéros de carte de crédit, les dossiers médicaux, les relevés bancaires ou les mots de passe sont stockées à distance et reçoivent un identifiant de jeton de sorte que les commerçants et les tiers (dans ce cas, Workstation) n'y auront pas accès.

Avantages d'OAuth 2.0

Outre le fait que le mot de passe de l'utilisateur ne soit pas révélé par les intégrations tierces (dans ce cas, Workstation), l'un des principaux avantages d'OAuth 2.0 est qu'il permet aux utilisateurs de révoquer l'accès à leurs ressources à tout moment. Si les utilisateurs n'ont plus besoin de cette intégration tierce, ils peuvent simplement révoquer l'accès de l'application à leurs ressources. Cela n'est pas possible avec l'authentification traditionnelle par nom d'utilisateur et par mot de passe, où l'utilisateur devra se souvenir de modifier son mot de passe pour révoquer l'accès.

En outre, OAuth 2.0 prend en charge différents types de subvention, ce qui permet au serveur

d'autorisation d'émettre des jetons de différentes façons. Cette flexibilité permet au serveur d'autorisation de choisir le type de subvention le plus sécurisé en fonction des exigences spécifiques du client et de l'utilisateur, et de partager uniquement les données les plus pertinentes en fonction des plages prédéfinies.

OAuth 2.0 a un protocole flexible qui repose sur un SSL (Secure Sockets Layer) pour garantir que les données entre le serveur Web et les navigateurs restent privées. Le SSL utilise des protocoles du secteur de la cryptographie pour protéger les données.

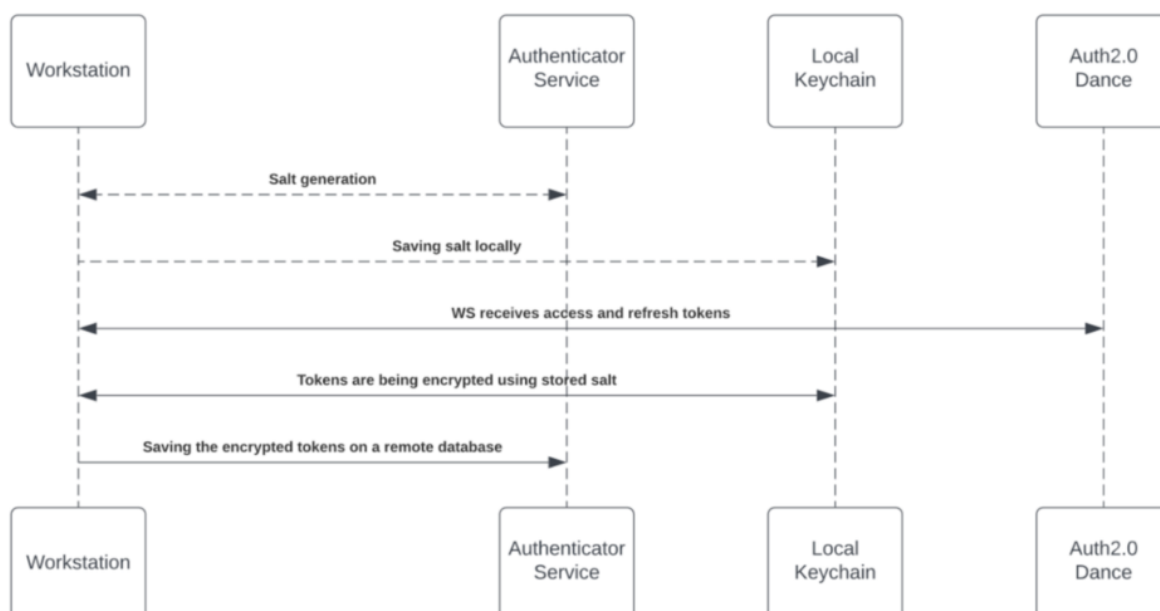
Rafraîchir le chiffrement des jetons

Chaque fois qu'un nouveau jeton d'accès est accordé à Workstation, l'application chiffre l'accès, actualise les jetons et le stocke dans une base de données distante.

Le processus de chiffrement comprend une clé privée unique (« salt ») qui est générée pour chaque individu au premier amorçage et stockée dans le trousseau de machine locale.

La clé salt est irremplaçable et ne peut pas être restaurée. Sa **perte entraîne l'annulation** de l'accès. Cette mesure de sécurité est prise pour éliminer la dépréciation de l'identité lorsque vous accédez à des données très sensibles.

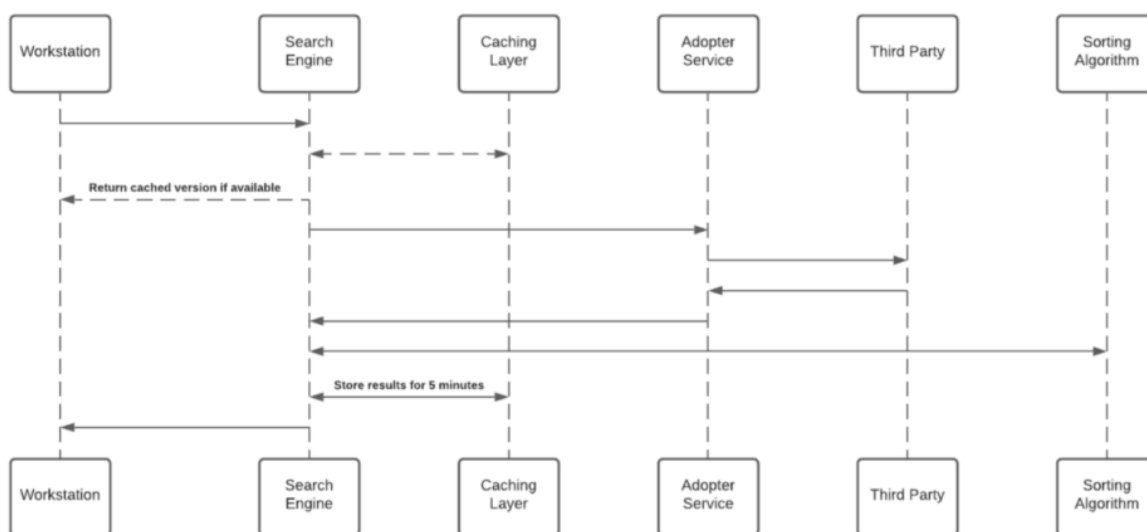
Voir la Figure ci-dessous pour examiner le flux de génération et de stockage salt :



Sécurité de recherche d'entreprise

La recherche d'entreprise utilise des intégrations tierces pour mettre en œuvre une « recherche fédérale ». Les recherches sur Workstation sont prises en charge par un moteur NLP et une base de données des graphiques qui prend en charge une excellente expérience utilisateur.

La recherche d'entreprise de Workstation ne répertorie pas de données tierces sur une base de données indépendante consultable. Consultez le diagramme de séquence ci-dessous qui décrit l'algorithme de recherche :



La couche cache enregistre les résultats pendant une période de cinq minutes

Chaque service d'adoption crée un identificateur unique pour les résultats qui n'ont pas d'importance sans accéder à la partie tierce et le stocke dans la base de données des graphiques.

[En savoir plus sur la sécurité de la recherche d'entreprise.](#)