À propos des appareils de confiance

À propos des appareils de confiance

La SSO avec des appareils de confiance permet aux utilisateurs de s'authentifier en utilisant la SSO et de décrypter leur coffre en utilisant une clé de chiffrement stockée sur l'appareil, éliminant ainsi le besoin d'entrer un mot de passe principal. Les appareils de confiance doivent soit être enregistrés à l'avance de la tentative d'identifiant, soit approuvés par quelques méthodes différentes.

La SSO avec des appareils de confiance offre aux utilisateurs finaux d'entreprise une expérience sans mot de passe qui est également à connaissance zéro et cryptée de bout en bout. Cela empêche les utilisateurs d'être verrouillés en raison de mots de passe principaux oubliés et leur permet de profiter d'une expérience d'identifiant simplifiée.

Commencez à utiliser des appareils de confiance

Pour commencer à utiliser SSO avec des appareils de confiance :

1. Configurez le SSO avec des appareils de confiance pour votre organisation.
2. Fournir aux administrateurs des informations sur comment approuver les demandes d'appareil.
3. Fournir aux utilisateurs finaux des informations sur comment ajouter des appareils de confiance.

Comment ça marche

Les onglets suivants décrivent les processus de cryptage et les échanges de clés qui se produisent lors de différentes procédures d'appareils de confiance :

⇒Intégration

Lorsqu'un nouvel utilisateur rejoint une organisation, une **Clé de Récupération de Compte** (en savoir plus) est créée en chiffrant leur clé de chiffrement de compte avec la clé publique de l'organisation. La récupération de compte est nécessaire pour activer le SSO avec des appareils de confiance.

L'utilisateur est ensuite invité à se demander s'il veut se souvenir, ou faire confiance, à l'appareil. Quand ils choisissent de le faire :

1. Une nouvelle **Clé d'Appareil** est générée par le client. Cette clé ne quitte jamais le client.
2. Une nouvelle paire de clés RSA, **Clé Privée de l'Appareil** et **Clé Publique de l'Appareil**, est générée par le client.
3. La clé de chiffrement du compte de l'utilisateur est chiffrée avec la clé publique non chiffrée de l'appareil et la valeur résultante est envoyée au serveur en tant que **Clé d'utilisateur chiffrée par clé publique**.
4. La **Clé Publique de l'Appareil** est cryptée avec la clé de cryptage du compte de l'utilisateur et la valeur résultante est envoyée au serveur en tant que **Clé Publique Cryptée de l'Utilisateur**.
5. La **Clé Privée de l'Appareil** est cryptée avec la première **Clé de l'Appareil** et la valeur résultante est envoyée au serveur en tant que **Clé Privée Cryptée de l'Appareil**.

La **Clé Utilisateur Cryptée par Clé Publique** et la **Clé Privée Cryptée par Clé d'Appareil** seront, de manière cruciale, envoyées du serveur au client lorsqu'un identifiant est initié.

La **Clé Publique Cryptée par la Clé de l'Utilisateur** sera utilisée si l'utilisateur a besoin de régénérer la clé de cryptage de son compte.

⇒Se connecter

Lorsqu'un utilisateur s'authentifie avec SSO sur un appareil déjà considéré comme fiable :

1. La **Clé d'utilisateur chiffrée avec la clé publique** de l'utilisateur, qui est une version chiffrée de la clé de chiffrement du compte utilisée pour déchiffrer les données du coffre, est envoyée du serveur au client.

2. La **Clé Privée Cryptée par Clé d'Appareil** de l'utilisateur, dont la version non cryptée est nécessaire pour décrypter la **Clé d'Utilisateur Cryptée par Clé Publique**, est envoyée du serveur au client.

3. Le client déchiffre la **Clé Privée Chiffrée par la Clé de l'Appareil** en utilisant la **Clé de l'Appareil**, qui ne quitte jamais le client.

4. La **Clé Privée de l'Appareil** maintenant non cryptée est utilisée pour décrypter la **Clé Utilisateur Cryptée par Clé Publique**, ce qui donne la clé de cryptage du compte de l'utilisateur.

5. La clé de chiffrement du compte de l'utilisateur déchiffre les données du coffre.

⇒Approuvant

Lorsqu'un utilisateur s'authentifie avec SSO et choisit de déchiffrer son coffre avec un appareil non fiable (c'est-à-dire qu'une **Clé Symétrique de l'Appareil** n'existe pas sur cet appareil), il est nécessaire de choisir une méthode pour approuver l'appareil et éventuellement le considérer comme fiable pour une utilisation future sans autre approbation. Ce qui se passe ensuite dépend de l'option sélectionnée :

- **Approuver à partir d'un autre appareil** :

    1. Le processus documenté ici est déclenché, ce qui a pour résultat que le client a obtenu et déchiffré la clé de chiffrement du compte.

    2. L'utilisateur peut maintenant déchiffrer les données de son coffre avec la clé de chiffrement de compte déchiffrée. S'ils ont choisi de faire confiance à l'appareil, la confiance est établie avec le client comme décrit dans l'onglet **Intégration**.

- **Demande d'approbation admin**:

    1. Le client initiateur envoie une requête POST, qui comprend l'adresse de courriel du compte, une clé publique unique de **demande d'authentification**[α], et un code d'accès, à une table de Demande d'Authentification dans la base de données Bitwarden.

    2. Les administrateurs peuvent approuver ou refuser la demande sur la page d'approbations d'appareil.

    3. Lorsque la demande est approuvée par un administrateur, le client approbateur crypte la clé de cryptage du compte de l'utilisateur en utilisant la **clé publique de demande d'authentification** incluse dans la demande.

    4. Le client approbateur met ensuite la clé de chiffrement du compte cryptée dans l'enregistrement de la demande d'authentification et marque la demande comme accomplie.

    5. Le client initiateur GETs la clé de chiffrement de compte cryptée et la déchiffre **localement** en utilisant la **clé privée de demande d'authentification**.

    6. En utilisant la clé de chiffrement de compte déchiffrée, la confiance est établie avec le client comme décrit dans l'**onglet d'intégration**.

[α] - **Auth-request clés publiques** et **clés privées** sont générées de manière unique pour chaque demande d'identifiant sans mot de passe et n'existent que tant que la demande existe. Les demandes non approuvées expireront après 1 semaine.

- **Approuver avec le mot de passe principal** :

    1. La clé de chiffrement du compte de l'utilisateur est récupérée et déchiffrée comme documenté dans la section Identifiant de l'utilisateur du Livre Blanc sur la Sécurité.

2. En utilisant la clé de chiffrement de compte déchiffrée, la confiance est établie avec le client comme décrit dans l'**onglet d'intégration**.

⇒Régénération de clé

> **Note**
> Seuls les utilisateurs qui ont un mot de passe principal peuvent régénérer leur clé de chiffrement de compte. En savoir plus.

Lorsqu'un utilisateur régénère sa clé de chiffrement de compte, pendant le processus de rotation normal :

1. La **Clé Publique Cryptée par la Clé Utilisateur** est envoyée du serveur au client, et ensuite déchiffrée avec l'ancienne clé de cryptage du compte (aussi connue sous le nom de. **Clé de l'Utilisateur**), aboutissant à la **Clé Publique de l'Appareil**.

2. La nouvelle clé de chiffrement du compte de l'utilisateur est chiffrée avec la clé publique non chiffrée de l'appareil et la valeur résultante est envoyée au serveur en tant que nouvelle **Clé d'utilisateur chiffrée par clé publique**.

3. La **Clé Publique de l'Appareil** est cryptée avec la nouvelle clé de cryptage du compte de l'utilisateur et la valeur résultante est envoyée au serveur comme la nouvelle **Clé Publique Cryptée de l'Utilisateur**.

4. Les clés de chiffrement d'appareil de confiance pour tous les autres appareils qui sont conservées dans le stockage du serveur sont effacées pour l'utilisateur. Cela ne laisse que les trois clés requises (**Clé d'utilisateur chiffrée par clé publique**, **Clé publique chiffrée par clé d'utilisateur**, et **Clé privée chiffrée par clé d'appareil** qui n'a pas été modifiée par ce processus) pour ce seul appareil persisté sur le serveur.

Tout client désormais non fiable devra rétablir la confiance par l'une des méthodes décrites dans l'**onglet Approbation**.

Clés utilisées pour des appareils de confiance

Ce tableau fournit plus d'informations sur chaque clé utilisée dans les procédures décrites ci-dessus :

Clé	Détails
Clé de l'appareil	AES-256 CBC HMAC SHA-256, 512 bits de longueur (256 bits pour la clé, 256 bits pour HMAC)
Clé privée de l'appareil & Clé publique de l'appareil	RSA-2048 OAEP SHA1, 2048 bits de longueur
Clé d'Utilisateur Chiffrée avec Clé Publique	RSA-2048 OAEP SHA1
Clé Utilisateur-Cryptée Clé Publique	AES-256 CBC HMAC SHA-256
Clé de l'appareil - Clé privée cryptée	AES-256 CBC HMAC SHA-256

Impact sur les mots de passe principaux

Bien que le SSO avec des appareils de confiance élimine le besoin d'un mot de passe principal, il n'élimine pas dans tous les cas le mot de passe principal lui-même :

- Si un utilisateur est intégré **avant** que SSO avec des appareils de confiance ne soit activé, ou s'ils sélectionnent **Créer un compte** à partir de l'invitation de l'organisation, leur compte conservera son mot de passe principal.
- Si un utilisateur est intégré **après** l'activation de SSO avec des appareils de confiance et qu'ils sélectionnent **Se connecter** → **SSO d'Entreprise** à partir de l'invitation de l'organisation pour la provision JIT, leur compte n'aura pas de mot de passe principal.

> ⚠ **Warning**
>
> Pour ces comptes qui n'ont pas de mot de passe principal à la suite de SSO avec des appareils de confiance, les retirer de votre organisation ou révoquer leur accès coupera tout accès à leur compte Bitwarden à moins que :
>
> 1. Vous leur attribuez un mot de passe principal en utilisant la récupération de compte au préalable.
> 2. L'utilisateur se connecte au moins une fois après la récupération du compte afin de terminer complètement le processus de récupération du compte.

Impact sur d'autres fonctionnalités

Selon qu'un hachage de mot de passe principal est disponible en mémoire pour votre client, ce qui est dicté par la manière dont votre application client est initialement accédée, elle peut présenter les modifications de comportement suivantes :

Fonctionnalité	Impact
Vérification	Il existe un certain nombre de fonctionnalités dans les applications client Bitwarden qui nécessitent normalement la saisie d'un mot de passe principal pour être utilisées, y compris l'exportation des données du coffre, la modification des paramètres de l'identifiant en deux étapes, la récupération des clés API, et plus encore. Si l'utilisateur n'utilise pas un mot de passe principal pour accéder au client, **toutes ces fonctionnalités** remplaceront la confirmation du mot de passe principal par une vérification TOTP basée sur le courriel.
Verrouillage/déverrouillage du coffre	Dans des circonstances ordinaires, un coffre verrouillé peut être déverrouillé à l'aide d'un mot de passe principal. Si l'utilisateur n'utilise pas un mot de passe principal pour accéder au client, les applications client verrouillées ne peuvent être déverrouillées qu'avec un PIN ou avec la biométrie. Si ni le code PIN ni la biométrie ne sont activés pour une application client, le coffre se déconnectera toujours au lieu de verrouiller. Déverrouiller et se connecter nécessiteront **toujours** une connexion internet.

Fonctionnalité	Impact
Ressaisir le mot de passe principal	Si l'utilisateur ne déverrouille pas son coffre avec un mot de passe principal, la relance du mot de passe principal sera désactivée.
CLI	Les utilisateurs qui n'ont pas de mot de passe principal **ne pourront pas** accéder au gestionnaire de mots de passe CLI.