bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > DEPLOY CLIENT APPS

Déployer les Clients Centralement

Afficher dans le centre d'aide:
https://bitwarden.com/help/configure-clients-selfhost/

Déployer les Clients Centralement

Lors de l'exploitation d'un serveur Bitwarden auto-hébergé dans un environnement professionnel, les administrateurs peuvent vouloir configurer centralement les paramètres de l'application client (en particulier, l'URL du serveur) avant de les déployer auprès des utilisateurs avec une plateforme de gestion des points de terminaison. Les paramètres sont appliqués lors de l'installation de l'application client.

Le processus pour ce faire sera différent pour chaque application client :

Extensions de navigateur

Chrome et Chromium

Les étapes suivantes supposent que les utilisateurs n'ont pas encore installé l'extension Bitwarden pour navigateur sur leurs machines. S'ils le font, ils devront réinitialiser aux paramètres pré-configurés, ce qui leur sera demandé de faire en suivant ce flux de travail :

⇒Linux

Pour pré-configurer les URLs d'environnement pour Linux :

1. Créez l'une des structures de répertoires suivantes si elles n'existent pas déjà sur votre système :
   - Pour Chrome, `/etc/opt/chrome/politiques de sécurité/gérées/`
   - Pour Chromium, `/etc/opt/chromium/politiques de sécurité/gérées/`
2. Dans le dossier `géré`, créez un fichier `bitwarden.json` avec le contenu suivant:

```Bash
{
  "3rdparty": {
  "extensions": {
  "nngceckbapebfimnlniiiahkandclblb": {
      "environment": {
        "base": "https://my.bitwarden.server.com"
        }
      }
    }
  }
}
```

L'ID de l'extension (`nngceckbapebfimnlniiiahkandclblb`) variera en fonction de votre méthode d'installation. Vous pouvez trouver votre ID d'extension en naviguant vers le menu d'extension de votre navigateur (par exemple, `chrome://extensions`).

La plupart des installations nécessiteront uniquement l'URL `"de base"` : cependant, certaines configurations uniques peuvent vous demander de saisir des URL pour chaque service indépendamment :

```Bash
{
  "3rdparty": {
  "extensions": {
  "nngceckbapebfimnlniiiahkandclblb": {
      "environment": {
        "base": "https://my.bitwarden.server.com",
        "webVault": "https://my.bitwarden.server.com",
        "api": "https://my.bitwarden.server.com",
        "identity": "https://my.bitwarden.server.com",
        "icons": "https://my.bitwarden.server.com",
        "notifications": "https://my.bitwarden.server.com",
        "events": "https://my.bitwarden.server.com"
        }
      }
    }
  }
}
```

> **Note**
> Si vous utilisez la version du Chrome ou Chromium Web Store de Bitwarden, vous pouvez suivre ces instructions pour forcer l'installation de Bitwarden sur les machines des utilisateurs finaux lorsque vous distribuez des politiques de sécurité gérées. Vous pouvez sauter les étapes qui se chevauchent, comme la création de répertoires requis.

3. Comme vous devrez déployer ces fichiers sur les machines des utilisateurs, nous vous recommandons de vous assurer que seuls les admins peuvent écrire des fichiers dans le répertoire `/politiques de sécurité`.

4. En utilisant votre logiciel de distribution préféré ou votre outil MDM, déployez ce qui suit sur les machines des utilisateurs :

   - Le navigateur basé sur Chrome ou Chromium
   - `/etc/opt/{chrome or chromium}/politiques de sécurité/gérées/bitwarden.json`

> **Tip**
> Pour plus d'aide, consultez le guide Démarrage rapide du navigateur Chrome de Google pour Linux.

⇒Fenêtres

Pour pré-configurer les URLs d'environnement pour Windows :

1. Ouvrez le Gestionnaire de politiques de sécurité de groupe Windows et créez un nouvel objet de politique de groupe (GPO) ou utilisez un GPO existant conçu pour vos utilisateurs finaux.

2. Éditez le GPO et naviguez vers **Configuration de l'utilisateur -> Préférences -> Paramètres Windows -> Registre.**

3. Cliquez avec le bouton droit de la souris sur **Registre** dans l'arborescence des fichiers et sélectionnez **Nouveau > Élément de Registre.**

4. Créez un nouvel élément de Registre avec les propriétés suivantes:

   - **Action** : Mettre à jour
   - **Ruche**: `HKEY_LOCAL_MACHINE`
   - **Chemin Clé**: `HKEY_LOCAL_MACHINE\LOGICIEL\Politiques de sécurité\Google\Chrome\3rdparty\extensions\\politique\environnement`

     Le variera en fonction de votre méthode d'installation. Vous pouvez trouver votre ID d'extension en naviguant vers le menu d'extension de votre navigateur (par exemple, `chrome://extensions`).

     > **Note**
     > Bien que Microsoft Edge soit un navigateur basé sur Chromium, l'emplacement du **Chemin Clé** est différent de l'entrée pour Google Chrome. Pour Microsoft Edge, utilisez le chemin de clé suivant :
     >
     > - `HKEY_LOCAL_MACHINE\LOGICIEL\Politiques de sécurité\Microsoft\Edge\3rdparty\Extensions\\politique\environnement`

   - **Nom de la valeur**: `base`
   - **Type de valeur**: `REG_SZ`
   - **Donnée de valeur**: Le domaine configuré de votre serveur

5. Sélectionnez **OK** une fois que l'élément est configuré.

   La plupart des installations nécessiteront uniquement l'URL `de base`, cependant, certaines configurations uniques peuvent vous demander de saisir des URL pour chaque service indépendamment. Si votre configuration l'exige, répétez **l'Étape 4** pour créer un nouvel élément de Registre pour chacun des éléments suivants :

   - Nom de la valeur : `webVault`
   - Nom de la valeur : `api`
   - Nom de la valeur : `identité`
   - Nom de la valeur : `icônes`
   - Nom de la valeur : `notifications`
   - Nom de la valeur : `événements`

> **Note**
> Vous pouvez également utiliser un GPO pour forcer l'installation de l'extension du navigateur. En savoir plus.

⇒macOS

Pour pré-configurer les URLs d'environnement pour macOS :

1. Créez un nouveau fichier `com.google.chrome.extensions..plist`.

   Le variera en fonction de votre méthode d'installation. Vous pouvez trouver votre ID d'extension en naviguant vers le menu d'extension de votre navigateur (par exemple, `chrome://extensions`).

2. Dans le fichier `.plist` créé, ajoutez le contenu suivant :

   ```
   Bash
   ```

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.
   0.dtd">
   <plist version="1.0">
       <dict>
           <key>environment</key>
           <dict>
               <key>base</key>
               <string>https://my.bitwarden.server.com</string>
           </dict>
       </dict>
   </plist>
   ```

   La plupart des installations nécessiteront uniquement la paire `base` et , cependant, certaines configurations uniques peuvent vous demander d'entrer des URL pour chaque service indépendamment :

```
Bash
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.
0.dtd">
<plist version="1.0">
    <dict>
        <key>environment</key>
        <dict>
            <key>base</key>
            <string>https://my.bitwarden.server.com</string>
                        <key>webVault</key>
                    <string>https://my.bitwarden.server.com</string>
                    <key>api</key>
                    <string>https://my.bitwarden.server.com></string>
                    <key>identity</key>
                    <string>https://my.bitwarden.server.com</string>
                    <key>icons</key>
                    <string>https://my.bitwarden.server.com</string>
                    <key>notifications</key>
                    <string>https://my.bitwarden.server.com</string>
                    <key>events</key>
                    <string>https://my.bitwarden.server.com</string>
        </dict>
    </dict>
</plist>
```

3. Convertissez le fichier `.plist` en un profil de configuration `.mobileconfig`.

> **Note**
> Si vous allez utiliser la version de Bitwarden du Chrome ou Chromium Web Store, vous pouvez suivre ces instructions pour forcer l'installation de Bitwarden sur les machines des utilisateurs finaux en créant un autre profil de configuration qui peut être distribué à l'étape suivante.

4. En utilisant votre logiciel de distribution préféré ou votre outil MDM, installez ce qui suit sur les machines des utilisateurs :
   - Le navigateur basé sur Chrome ou Chromium
   - Le profil de configuration `.mobileconfig`

Firefox

⇒Linux

Pour pré-configurer les URLs d'environnement pour Linux :

1. Créez un répertoire `/etc/firefox/politiques de sécurité`:

```Bash
mkdir -p /etc/firefox/policies
```

2. Comme vous devrez déployer ce répertoire et les fichiers qu'il contient sur les machines des utilisateurs, nous vous recommandons de vous assurer que les anciens admins peuvent écrire des fichiers dans le répertoire `/politiques de sécurité` :

```Bash
chmod -R 755 /etc/firefox/policies
```

3. Créez un fichier `politiques.json` dans `/etc/firefox/politiques` et ajoutez le contenu suivant:

```Bash
{
 "policies": {
    "3rdparty": {
      "Extensions": {
        "{446900e4-71c2-419f-a6a7-df9c091e268b}": {
          "environment": {
            "base": "https://my.bitwarden.server.com"
          }
        }
      }
    }
  }
}
```

La plupart des installations nécessiteront uniquement l'URL `"de base"` : cependant, certaines configurations uniques peuvent vous demander de saisir des URL pour chaque service indépendamment :

```Bash
{
 "policies": {
    "3rdparty": {
      "Extensions": {
        "{446900e4-71c2-419f-a6a7-df9c091e268b}": {
          "environment": {
            "base": "https://my.bitwarden.server.com",
            "webVault": "https://my.bitwarden.server.com",
            "api": "https://my.bitwarden.server.com",
            "identity": "https://my.bitwarden.server.com",
            "icons": "https://my.bitwarden.server.com",
            "notifications": "https://my.bitwarden.server.com",
            "events": "https://my.bitwarden.server.com"
          }
        }
      }
    }
  }
}
```

4. En utilisant votre logiciel de distribution préféré ou votre outil MDM, déployez `/etc/firefox/politiques de sécurité/politiques.json` sur les machines des utilisateurs.

⇒Fenêtres

Pour pré-configurer les URLs d'environnement pour Windows :

1. Ouvrez le Gestionnaire de politiques de sécurité de groupe Windows et créez un nouvel objet de politique de sécurité de groupe (GPO) ou utilisez un GPO existant conçu pour vos utilisateurs finaux.

2. Éditez le GPO et naviguez vers **Configuration de l'utilisateur > Préférences > Paramètres Windows > Registre**.

3. Cliquez avec le bouton droit sur **Registre** dans l'arborescence des fichiers et sélectionnez **Nouveau > Élément de Registre**.

4. Créez un nouvel élément de Registre avec les propriétés suivantes:

   - **Action** : Mettre à jour
   - **Ruche**: `HKEY_LOCAL_MACHINE`
   - **Chemin Clé**: `HKEY_LOCAL_MACHINE\LOGICIEL\Politiques de sécurité\Mozilla\Firefox\3rdparty\Extensions\{446900e4-71c2-419f-a6a7-df9c091e268b}\environnement`

- **Nom de la valeur**: `base`
- **Type de valeur**: `REG_SZ`
- **Donnée de valeur**: Le domaine configuré de votre serveur

5. Sélectionnez **OK** une fois que l'élément est configuré.

   La plupart des installations nécessiteront uniquement l'URL de base, cependant, certaines configurations uniques peuvent vous obliger à entrer des URL pour chaque service indépendamment. Si votre configuration l'exige, répétez **l'étape 4** pour créer un nouvel élément de registre pour chacun des éléments suivants :

   - Nom de la valeur : `webVault`
   - Nom de la valeur : `api`
   - Nom de la valeur : `identité`
   - Nom de la valeur : `icônes`
   - Nom de la valeur : `notifications`
   - Nom de la valeur : `événements`

⇒macOS

Pour pré-configurer les URLs d'environnement pour macOS :

1. Supprimez l'attribut de mise en quarantaine appliqué automatiquement à Firefox en exécutant la commande suivante :

   ```bash
   xattr -r -d com.apple.quarantine /Applications/Firefox.app
   ```

2. Créez un répertoire `/Applications/Firefox.app/Contents/Resources/distribution`.

3. Créez un fichier `policies.json` dans le `dossier de distribution` et ajoutez le contenu suivant:

```Bash
{
 "policies": {
    "3rdparty": {
      "Extensions": {
        "{446900e4-71c2-419f-a6a7-df9c091e268b}": {
          "environment": {
            "base": "https://my.bitwarden.server.com"
          }
        }
      }
    }
  }
}
```

La plupart des installations nécessiteront uniquement l'URL `"de base"` : cependant, certaines configurations uniques peuvent vous demander de saisir des URL pour chaque service indépendamment :

```Bash
{
 "policies": {
    "3rdparty": {
      "Extensions": {
        "{446900e4-71c2-419f-a6a7-df9c091e268b}": {
          "environment": {
            "base": "https://my.bitwarden.server.com",
            "webVault": "https://my.bitwarden.server.com",
            "api": "https://my.bitwarden.server.com",
            "identity": "https://my.bitwarden.server.com",
            "icons": "https://my.bitwarden.server.com",
            "notifications": "https://my.bitwarden.server.com",
            "events": "https://my.bitwarden.server.com"
          }
        }
      }
    }
  }
}
```

4. En utilisant votre logiciel de distribution préféré ou votre outil MDM, déployez `/etc/firefox/politiques de sécurité/politiques.json` sur les machines des utilisateurs.

Applications de bureau

Pour configurer centralement l'application de bureau pour le déploiement, commencez par effectuer les étapes suivantes sur une seule station de travail :

1. Installez l'application de bureau. Si vous utilisez Windows, installez silencieusement Bitwarden en tant qu'administrateur en utilisant `installer.exe /allusers /S` (voir la documentation NSIS).

2. Naviguez vers les paramètres stockés localement de l'application de bureau. Ce répertoire est différent en fonction de votre système d'exploitation (par exemple, `%AppData%\Bitwarden` sur Windows, `~/Library/Application Support/Bitwarden` sur macOS). Trouvez votre répertoire.

3. Dans l'annuaire, ouvrez le fichier `data.json`.

4. Éditer `data.json` pour configurer l'application de bureau comme souhaité. En particulier, créez l'objet suivant pour configurer l'application avec l'URL de votre serveur auto-hébergé :

```Bash
"global_environment_environment": {
   "region": "Self-hosted",
   "urls": {
      "base": "self-host.com"
    }
 }
```

5. Définissez la valeur de `"région"` sur `"Auto-hébergé"`:

```Bash
"region": "Self-hosted"
```

6. Une fois configuré comme vous le souhaitez, utilisez votre solution de gestion de points de terminaison de choix (comme Jamf) pour déployer l'application de bureau pré-configurée en tant que modèle.

> **Note**
> Comme alternative à la configuration manuelle du fichier `data.json`, vous pouvez attribuer des `environmentUrls` en utilisant l'application de bureau Bitwarden. Sélectionnez la région souhaitée à l'aide de l'interface graphique de l'application de bureau, puis fermez l'application et localisez votre fichier data.json afin de copier les informations de la variable d'environnement.

Applications mobiles

La plupart des solutions de gestion des appareils mobiles (MDM) ou de gestion de la mobilité en entreprise (EMM) permettent aux administrateurs de pré-configurer les applications avant le déploiement de manière standard. Pour pré-configurer les applications mobiles Bitwarden pour utiliser l'URL de votre serveur auto-hébergé, construisez la configuration d'application suivante :

Clé de Configuration	Type de Valeur	Valeur de Configuration
`urlEnvironnementDeBase`	corde	Votre URL de serveur auto-hébergé, par exemple `https://my.bitwarden.server.com`.