

ADMIN CONSOLE > DEPLOY CLIENT APPS

Configure Clients for Your Server

View in the help center:
<https://bitwarden.com/help/configure-clients-selfhost/>

Configure Clients for Your Server

When operating a self-hosted Bitwarden server in a business setting, administrators may want to centrally configure client application settings (particularly, Server URL) before deploying to users with an endpoint management platform. Settings are applied upon installation of the client application. These processes may also be helpful if you're using a [Bitwarden Cloud EU server](#).

The process for doing so will be different for each client application:

Browser extensions

Chrome and Chromium

The following steps assume that users do not yet have the Bitwarden browser extension installed on their machines. If they do, they will need to reset to pre-configured settings, which they will be prompted to do when following [this workflow](#):

⇒Linux

To pre-configure environment URLs for Linux:

1. Create one of the following directory structures if they do not already exist on your system:

- For Chrome, `/etc/opt/chrome/policies/managed/`
- For Chromium, `/etc/opt/chromium/policies/managed/`

2. In the `managed` folder, create a `bitwarden.json` file with the following contents:

Bash

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

The extension ID (`nngceckbapebfimlniiahkandclblb`) will vary depending on your installation method. You can find your extension ID by navigating to your browser's extension menu (for example, `chrome://extensions`).

Most installations will only require the `"base":` URL, however some unique setups may require you to enter URLs for each service independently:

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

If you'll be using the Chrome or Chromium Web Store version of Bitwarden, you can follow [these instructions](#) to force install Bitwarden on end-user machines when you distribute managed policies. You can skip overlapping steps, like creating required directories.

- As you will need to deploy these files to users' machines, we recommend making sure only admins can write files in the `/policies` directory.
- Using your preferred software distribution or MDM tool, deploy the following to users' machines:
 - The Chrome or Chromium-based browser
 - `/etc/opt/{chrome or chromium}/policies/managed/bitwarden.json`

Tip

For more help, refer to Google's [Chrome Browser Quick Start for Linux](#) guide.

⇒ Windows

To pre-configure environment URLs for Windows:

1. Open the Windows Group Policy Manager and create a new Group Policy Object (GPO) or use an existing GPO scoped for your end-users.
2. Edit the GPO and navigate to **User Configuration -> Preferences -> Windows Settings -> Registry**.
3. Right-click **Registry** in the file tree and select **New > Registry Item**.
4. Create a new Registry Item with the following properties:

- **Action:** Update
- **Hive:** `HKEY_LOCAL_MACHINE`
- **Key Path:** `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\3rdparty\extensions\\policy\environment`

The `<extension_id>` will vary depending on your installation method. You can find your extension ID by navigating to your browser's extension menu (for example, `chrome://extensions`).

Note

While Microsoft edge is a Chromium based browser, the **Key Path** location is different than the input for Google Chrome. For Microsoft Edge, use the following key path:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\3rdparty\extensions\\policy\environment`

- **Value name:** `base`
- **Value type:** `REG_SZ`
- **Value data:** Your server's configured domain

Note

Registry key management systems may omit `HKEY_LOCAL_MACHINE\` from the Full Key Path. `HKEY_LOCAL_MACHINE` is a Hive and is omitted from the Key Path if the system has a separate Hive setting.

5. Select **OK** once the item is configured.

Most installations will only require the `base` URL, however some unique setups may require you to enter URLs for each service independently. If your setup requires this, repeat **Step 4** to create a new Registry Item for each of the following:

- Value name: `webVault`
- Value name: `api`
- Value name: `identity`
- Value name: `icons`

- Value name: `notifications`
- Value name: `events`

Note

You can also use a GPO to force-install the browser extension. [Learn more.](#)

⇒ macOS

To pre-configure environment URLs for macOS:

1. Create a new file `com.google.chrome.extensions.<extension_id>.plist`.

The `<extension_id>` will vary depending on your installation method. You can find your extension ID by navigating to your browser's extension menu (for example, `chrome://extensions`).

2. In the created `.plist` file, add the following contents:

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>
```

Most installations will only require the `base <key>` and `<string>` pair, however some unique setups may require you to enter URLs for each service independently:

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. Convert the `.plist` file to a `.mobileconfig` configuration profile.

Note

If you'll be using the Chrome or Chromium Web Store version of Bitwarden, you can follow [these instructions](#) to force install Bitwarden on end-user machines by creating another configuration profile that can be distributed in the next step.

4. Using your preferred software distribution or MDM tool, install the following on users' machines:

- The Chrome or Chromium-based browser
- The `.mobileconfig` configuration profile

Firefox

⇒Linux

To pre-configure environment URLs for Linux:

1. Create a directory `/etc/firefox/policies`:

Bash

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

2. As you will need to deploy this directory and the files in it to users' machines, we recommend making sure old admins can write files in the `/policies` directory:

Bash

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

3. Create a `policies.json` file in `/etc/firefox/policies` and add the following contents:

Bash

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

Most installations will only require the `"base"`: URL, however some unique setups may require you to enter URLs for each service independently:

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. Using your preferred software distribution or MDM tool, deploy `/etc/firefox/policies/policies.json` to users' machines.

⇒ Windows

To pre-configure environment URLs for Windows:

1. Open the Windows Group Policy Manager and create a new Group Policy Object (GPO) or use an existing GPO scoped for your end-users.
2. Edit the GPO and navigate to **User Configuration > Preferences > Windows Settings > Registry**.
3. Right-click **Registry** in the file tree and select **New > Registry Item**.
4. Create a new Registry item with the following properties:
 - **Action:** Update
 - **Hive:** `HKEY_LOCAL_MACHINE`
 - **Key Path:** `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Mozilla\Firefox\3rdparty\Extensions\{446900e4-71c2-419f-a6a7-df9c091e268b}\environment`

- **Value name:** `base`
- **Value type:** `REG_SZ`
- **Value data:** Your server's configured domain

Note

Registry key management systems may omit `HKEY_LOCAL_MACHINE\` from the Full Key Path. `HKEY_LOCAL_MACHINE` is a Hive and is omitted from the Key Path if the system has a separate Hive setting.

5. Select **OK** once the item is configured.

Most installations will only require the base URL, however some unique setups may require you to enter URLs for each service independently. If your setup requires this, repeat **Step 4** to create a new Registry item for each of the following:

- Value name: `webVault`
- Value name: `api`
- Value name: `identity`
- Value name: `icons`
- Value name: `notifications`
- Value name: `events`

⇒ macOS

To pre-configure environment URLs for macOS:

1. Remove the quarantining attribute automatically applied to Firefox by running the following command:

Bash

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

2. Create a directory `/Applications/Firefox.app/Contents/Resources/distribution`.

3. Create a file `policies.json` in the `distribution` folder and add the following contents:

Bash

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

Most installations will only require the **"base"**: URL, however some unique setups may require you to enter URLs for each service independently:

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. Using your preferred software distribution or MDM tool, deploy `/etc/firefox/policies/policies.json` to users' machines.

Note

In order to centrally deploy the Bitwarden browser extension to EU servers, `base` and `notifications` must be set to the EU cloud. For example:

Plain Text

```
"base": "https://vault.bitwarden.eu"
"notifications": "https://notifications.bitwarden.eu"
```

If enabled correctly, user's browser extensions will display **Logging in on: self-hosted** but will still connect to bitwarden.eu.

Desktop apps

To centrally configure the Desktop app for deployment, first complete the following steps on a single workstation:

1. Install the Desktop app. If you're using Windows, silently install Bitwarden as an administrator using `installer.exe /allusers /S` (see [NSIS documentation](#)).
2. Navigate to the Desktop app's locally stored settings. This directory is different depending on your OS (e.g. `%AppData%\Bitwarden` on Windows, `~/Library/Application Support/Bitwarden` on macOS). [Find your directory](#).
3. In the directory, open the `data.json` file.
4. Edit `data.json` to configure the Desktop app as desired. In particular, create the following object to configure the app with your self-hosted Server URL:

Bash

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

💡 Tip

Customers using Bitwarden cloud servers may instead set `"region": "US"` or `"EU"` to connect to those servers.

5. Once configured the way you want it, use your endpoint management solution of choice (like [Jamf](#)) to deploy the pre-configured Desktop app as a template.

📌 Note

As an alternative to manually configuring the `data.json` file, you can assign `environmentUrls` using the Bitwarden desktop app. Select your desired region using the desktop app GUI, then close the app and [locate your data.json file](#) in order to copy the environment variable information.

If users are experiencing graphics or performance issues, Bitwarden includes settings that can be adjusted to improve performance. See [Password Manager FAQs](#).

Mobile apps

Most Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solutions allow administrators to pre-configure applications before deployment in a standard fashion. To pre-configure Bitwarden Mobile apps to use your self-hosted Server URL, construct the following Application Configuration:

Configuration Key	Value Type	Configuration Value
<code>baseEnvironmentUrl</code>	string	Your self-hosted Server URL, for example <code>https://my.bitwarden.server.com</code> .

Web app

For users of the web app, Bitwarden recommends using your endpoint, group policy, or mobile device management tool to setup a bookmark or desktop shortcut pointing to the appropriate web app URL (for example, <https://vault.bitwarden.eu> or your self-hosted server).

Learn how to [deploy managed bookmarks using Google Admin Console](#).