bitwarden | Artikel Helpcentrum

SELF-HOSTING

Certificaatopties

Weergeven in het Helpcentrum:
https://bitwarden.com/help/certificates/

Certificaatopties

Dit artikel beschrijft de certificaatopties die beschikbaar zijn voor zelf gehoste instanties van Bitwarden. U selecteert uw certificaatoptie tijdens de installatie.

> **Note**
> De informatie in dit artikel is mogelijk niet van toepassing op zelf gehoste implementaties van Bitwarden Unified.

Een certificaat genereren met Let's Encrypt

Let's Encrypt is een certificaatautoriteit (CA) die gratis vertrouwde SSL-certificaten uitgeeft voor elk domein. Het installatiescript van Bitwarden biedt de optie om een vertrouwd SSL-certificaat te genereren voor uw domein met behulp van Let's Encrypt en Certbot.

Certificaatvernieuwing wordt elke keer gecontroleerd als Bitwarden opnieuw wordt opgestart. Als je Let's Encrypt gebruikt, moet je een e-mailadres opgeven voor herinneringen voor het verlopen van certificaten.

Als je Let's Encrypt gebruikt, moeten de poorten 80 en 443 open zijn op je machine.

Een Let's Encrypt-certificaat handmatig bijwerken

Als u de domeinnaam van uw Bitwarden-server wijzigt, moet u het gegenereerde certificaat handmatig bijwerken. Voer de volgende opdrachten uit om een back-up te maken, uw certificaat bij te werken en Bitwarden opnieuw op te bouwen:

Bash

```bash
./bitwarden.sh stop

mv ./bwdata/letsencrypt ./bwdata/letsencrypt_backup

mkdir ./bwdata/letsencrypt

chown -R bitwarden:bitwarden ./bwdata/letsencrypt

chmod -R 740 ./bwdata/letsencrypt

docker pull certbot/certbot

docker run -i --rm --name certbot -p 443:443 -p 80:80 -v <Full Path from / >/bwdata/letsencrypt:/et
c/letsencrypt/ certbot/certbot certonly --email <user@email.com> --logs-dir /etc/letsencrypt/logs
```

Selecteer 1 en volg de instructies:

```Bash
openssl dhparam -out ./bwdata/letsencrypt/live/<your.domain.com>/dhparam.pem 2048
./bitwarden.sh rebuild
./bitwarden.sh start
```

PowerShell

> **Tip**
> Je moet een build van OpenSSL voor Windows installeren.

```Bash
.\bitwarden.ps1 -stop
mv .\bwdata\letsencrypt .\bwdata\letsencrypt_backup
mkdir .\bwdata\letsencrypt
docker pull certbot/certbot
docker run -i --rm --name certbot -p 443:443 -p 80:80 -v <Full Path from \ >\bwdata\letsencrypt\:/e
tc/letsencrypt/ certbot/certbot certonly --email <user@email.com> --logs-dir /etc/letsencrypt/logs
Select 1, then follow instructions
<path/to/openssl.exe> dhparam -out .\bwdata\letsencrypt\live\<your.domain.com>\dhparam.pem 2048
.\bitwarden.ps1 -rebuild
.\bitwarden.ps1 -start
```

Een bestaand SSL-certificaat gebruiken

U kunt er ook voor kiezen om een bestaand SSL-certificaat te gebruiken. Hiervoor hebt u de volgende bestanden nodig:

- Een servercertificaat (`certificate.crt`)
- Een privésleutel (`private.key`)
- Een CA-certificaat (`ca.crt`)

Mogelijk moet u uw primaire certificaat bundelen met tussenliggende CA-certificaten om SSL vertrouwensfouten te voorkomen. Alle certificaten moeten worden opgenomen in het certificaatbestand van de server als er een CA-certificaat wordt gebruikt. Het eerste certificaat in het bestand moet uw servercertificaat zijn, gevolgd door eventuele tussenliggende CA-certificaten, gevolgd door de root-CA.

In de standaardconfiguratie plaatst u uw bestanden in `./bwdata/ssl/uw.domein`. U kunt een andere locatie opgeven voor uw certificaatbestanden door de volgende waarden aan te passen in `./bwdata/config.yml`:

```
Bash

ssl_certificate_path: <path>
ssl_key_path: <path>
ssl_ca_path: <path>
```

Note

De waarden gedefinieerd in `config.yml` vertegenwoordigen locaties binnen de NGINX container. Directories op de host worden gekoppeld aan directories in de NGINX container. In de standaardconfiguratie zien de toewijzingen er als volgt uit:

De volgende waarden in `config.yml`:

```
Bash

ssl_certificate_path: /etc/ssl/your.domain/certificate.crt
ssl_key_path: /etc/ssl/your.domain/private.key
ssl_ca_path: /etc/ssl/your.domain/ca.crt
```

Map naar de volgende bestanden op de host:

```
Bash

./bwdata/ssl/your.domain/certificate.crt
./bwdata/ssl/your.domain/private.key
./bwdata/ssl/your.domain/ca.crt
```

Je zou alleen moeten werken met bestanden in `./bwdata/ssl/`. Werken met bestanden direct in de NGINX container wordt niet aangeraden.

Diffie-Hellman sleuteluitwisseling gebruiken

Optioneel, als Diffie-Hellman sleuteluitwisseling wordt gebruikt om efemere parameters te genereren:

- Neem een `dhparam.pem` bestand op in dezelfde map.
- Stel de waarde `ssl_diffie_hellman_path:` in `config.yml` in.

Note

Je kunt je eigen `dhparam.pem` bestand maken met OpenSSL met `openssl dhparam -out ./dhparam.pem 2048`.

Een zelfondertekend certificaat gebruiken

U kunt er ook voor kiezen om een zelfondertekend certificaat te gebruiken, maar dit wordt alleen aanbevolen om te testen.

Zelfondertekende certificaten worden standaard niet vertrouwd door Bitwarden-clienttoepassingen. U moet dit certificaat handmatig installeren in de vertrouwde winkel van elk apparaat waarmee u Bitwarden wilt gebruiken.

Genereer een zelfondertekend certificaat:

```bash
mkdir ./bwdata/ssl/bitwarden.example.com
openssl req -x509 -newkey rsa:4096 -sha256 -nodes -days 365 \
  -keyout ./bwdata/ssl/bitwarden.example.com/private.key \
  -out ./bwdata/ssl/bitwarden.example.com/certificate.crt \
  -reqexts SAN -extensions SAN \
  -config <(cat /usr/lib/ssl/openssl.cnf <(printf '[SAN]\nsubjectAltName=DNS:bitwarden.example.com
\nbasicConstraints=CA:true')) \
  -subj "/C=US/ST=New York/L=New York/O=Company Name/OU=Bitwarden/CN=bitwarden.example.com"
```

Uw zelfondertekende certificaat (`.crt`) en privésleutel (`private.key`) kunnen in de map `./bwdata/ssl/self/your.domain` worden geplaatst en in de map `./bwdata/config.yml` worden geconfigureerd:

```bash
 ssl_certificate_path: /etc/ssl/bitwarden.example.com/certificate.crt
 ssl_key_path: /etc/ssl/bitwarden.example.com/private.key
```

Een zelfondertekend certificaat vertrouwen

Windows

Om een zelfondertekend certificaat onder Windows te vertrouwen, voer je `certmgr.msc` uit en importeer je het certificaat in de Trusted Root Certification Authorities.

Linux

Om een zelfondertekend certificaat op Linux te vertrouwen, voeg je je certificaat toe aan de volgende mappen:

```bash
/usr/local/share/ca-certificates/
/usr/share/ca-certificates/
```

En voer de volgende commando's uit:

```bash
sudo dpkg-reconfigure ca-certificates
sudo update-ca-certificates
```

Voor onze Linux desktop app, toegang tot de web kluis met Chromium-gebaseerde browsers, en de Directory Connector desktop app, moet je ook deze Linux cert management procedure voltooien.

Voor de Bitwarden CLI en Directory Connector CLI moet je zelfondertekende certificaat worden opgeslagen in een lokaal bestand en moet er bijvoorbeeld verwezen worden naar een `NODE_EXTRA_CA_CERTS=` omgevingsvariabele:

```bash
export NODE_EXTRA_CA_CERTS=~/.config/Bitwarden/certificate.crt
```

Android

Raadpleeg de documentatie over het toevoegen en verwijderen van certificaten van Google om een zelfondertekend certificaat op een Android-apparaat te vertrouwen.

Note

Als je **niet zelf host** en de volgende certificaatfout tegenkomt op je Android-apparaat:

```bash
Exception message: java.security.cert.CertPathValidatorException: Trust anchor for certificati
on path not found.
```

U moet de Bitwarden-certificaten uploaden naar uw apparaat. Raadpleeg deze community thread voor hulp bij het vinden van de certificaten.

Gebruik geen certificaat

Warning

Als u ervoor kiest om geen certificaat te gebruiken, moet u **uw installatie afschermen met een proxy die Bitwarden via SSL serveert**. Dit komt omdat Bitwarden HTTPS vereist; als u Bitwarden probeert te gebruiken zonder het HTTPS-protocol, treden er fouten op.