

# Az Apache2 HTTP telepítése az ön aláírt SSL/TLS tanúsítványokkal a Debian 11.05 szerverekenél

<https://websiteforstudents.com/setup-apache2-http-with-self-signed-ssl-tls-certificates-on-ubuntu-16-04-lts-servers/>  
<https://vitux.com/how-to-install-and-configure-apache-web-server-on-ubuntu/>

## ELŐFELTÉTEL!

**Mielőtt nekikezdenénk a szolgáltatás telepítésének, konfigurálásának előtte ellenőrizzük, hogy a DNS szolgáltatás telepítve és konfigurálva van-e. Ha nincs, akkor ezt tegyük meg előtte!**

Amikor belső tesztelést hajt végre fejlesztői környezetben, akkor valószínűleg nincs szüksége nyilvános aláírással ellátott SSL/TLS tanúsítványokra. Annak ellenére, hogy megmutattuk, hogyan lehet ingyenesen titkosítani a tanúsítványokat, ha webhelye nincs nyilvánosan hozzáférhető, vagy ha nyilvános domainhez van hozzárendelve, az Encryptr nem fog működni az Ön számára.

Az egyetlen lehetőség az ön aláírt tanúsítványok használata.

Az SSL / TLS tanúsítvány olyan mechanizmus, amely lehetővé teszi a privát kommunikációt két hálózati eszköz között. Ez egy protokoll, amely lehetővé teszi a biztonságos kommunikációt a webkiszolgálók és a webes ügyfelek, és még sok más hálózati szolgáltatás között.

Az SSL / TLS implementációkkal kapcsolatban alapvetően kétféle tanúsítvány létezik: Nyilvános és magán tanúsítványok. Nyilvános tanúsítványok azok, amelyeket a weboldalakon és más nyilvános erőforrásokon használnak és a magán vagy ön aláírt tanúsítványokat generálnak belsőleg, főleg tesztelési célokra. Ha készen áll az Apache2 telepítésére saját aláírási tanúsítványokkal, folytassa az alábbiakkal:

## Telepítse az Apache2 HTTP webszervert

Ha még nincs telepítve az Apache2 HTTP Server, az alábbi parancsok segítségével telepítheti azt az Ubuntu 16.04 LTS-re. Csak másolja és illessze be az összes sort, és futtassa.

```
sudo apt-get update
```

```
sudo apt-get install apache2
```

```
sudo a2enmod ssl
```

```
sudo service apache2 restart
```

```
sudo service apache2 status
```

```
tanulo@debian:~$ sudo service apache2 restart
tanulo@debian:~$ sudo service apache2 status
• apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2023-01-15 16:55:54 CET; 5s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 1920 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1924 (apache2)
    Tasks: 55 (limit: 1131)
   Memory: 9.4M
      CPU: 18ms
   CGroup: /system.slice/apache2.service
           └─1924 /usr/sbin/apache2 -k start
             └─1925 /usr/sbin/apache2 -k start
               └─1926 /usr/sbin/apache2 -k start
```

```
jan 15 16:55:54 debian systemd[1]: Starting The Apache HTTP Server...
```

```
jan 15 16:55:54 debian apachectl[1923]: AH00558: apache2: Could not reliably determine the server's s
```

```
jan 15 16:55:54 debian systemd[1]: Started The Apache HTTP Server.
```

```
lines 1-17/17 (END)
```

## Ellenőrizze az Apache telepítését

A telepítés befejezése után ellenőrizheti a verziószámot, és így ellenőrizheti, hogy az Apache2 valóban telepítve van-e a rendszerén, a következő parancs beírásával:

```
sudo apache2 -version
```

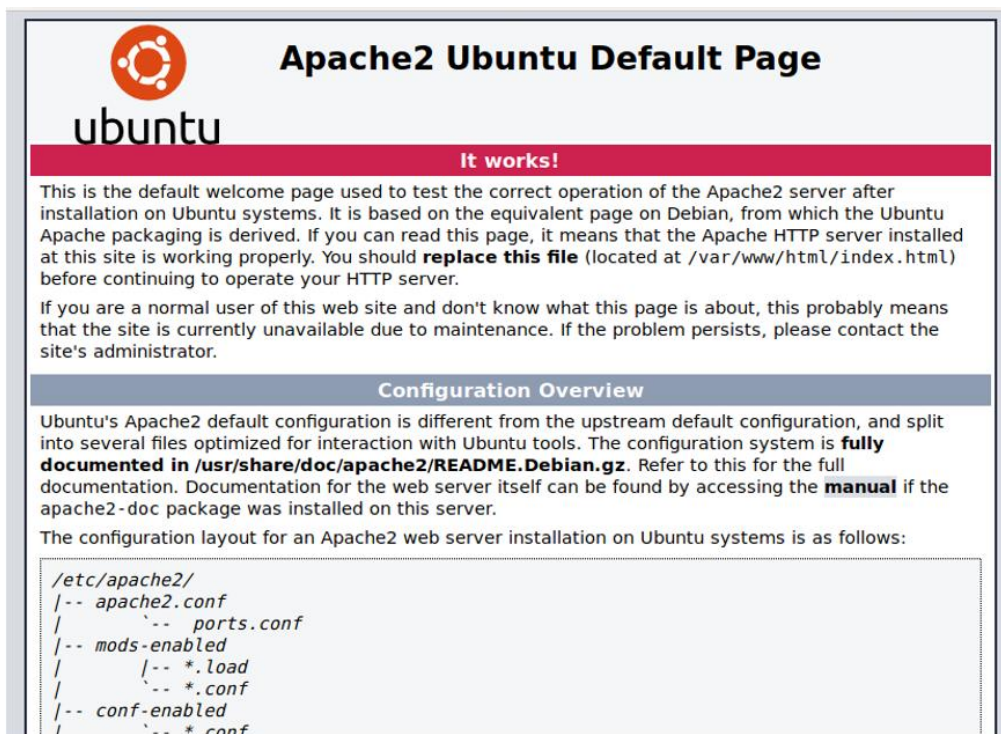
```
tanulo@SERVER:~$ apache2 -version
Server version: Apache/2.4.18 (Ubuntu)
Server built:   2018-06-07T19:43:03
```

## Apache megfelelő működésének ellenőrzése

Az Apache futtatásának ellenőrzéséhez indítsa el a kliensbe virtuálisgépet, majd a böngészőben adja ki a szerver IP címével az alábbi URL-t ([http://server\\_IP](http://server_IP)), ami az esetünkben a következő lesz:

<http://192.168.0.1>

Ezzel az Ubuntu következő Apache weboldalát jeleníti meg, ellenőrizve, hogy az Apache szerver megfelelően működik.



## Állítsa be a virtuális gazdagépeket az Apache-ban

Bemutatunk egy példát arra, hogyan lehet virtuális gazdagépet beállítani az Apache kiszolgálón keresztül. A mintázott [suli.local](http://suli.local) nevű webhelyet az Ubuntu Apache alapértelmezés szerint engedélyezett szerverblokkjának használatával állítottuk be.

# 1. lépés: Állítsa be a domain nevet

**Figyelem! A domain nevet egyeztessük a DNS szolgáltatással megadott névvel!**

**Pl.: sulis.local**

Az alapértelmezés szerint engedélyezett szerverblokk képes a `/var/www/html` mappából származó dokumentumok kiszolgálására. Létrehozunk egy könyvtárat a `/var/www/` könyvtárban, az alapértelmezett könyvtárat érintetlenül hagyva.

Hozza létre ezt a könyvtárat a következő paranccsal, helyettesítve a megfelelő domain nevet:

```
sudo mkdir -p /var/www/sulis.local/html
```

Ezután a következő parancsokkal rendelje hozzá a könyvtár tulajdonjogát:

```
sudo chown -R $USER:$USER /var/www/sulis.local/html
sudo chmod -R 755 /var/www/sulis.local
```

Hozzunk létre egy index oldalt, amelyhez később hozzáférhetünk, és tesztelhetjük, hogy az Apache futtatja-e a domain nevet. Hozzon létre egy HTML fájlt:

```
sudo nano /var/www/sulis.local/html/index.html
```

Írja be a következő HTML-kódot:

```
<html>
<head>
  <title> Welcome! </title>
</head>
<body>
  <h1> Hello World! </h1>
</body>
</html>
```

Mentéssel lépünk ki, ha készen vagyunk.

Az Apache-nak virtuális gazdafájltra van szüksége a szerver tartalmának kiszolgálásához. Az alapértelmezett konfigurációs fájl erre a célra már létrehozva, de új fájlt készítünk az egyedi konfigurációinkhoz.

```
sudo nano /etc/apache2/sites-available/sulis.local.conf
```

Adja meg a domain név következő testreszabott konfigurációs adatait:

```
<VirtualHost *:80>
    ServerAdmin tanulo@SERVER.hu
    ServerName sul1.local
    ServerAlias www.sul1.local
    DocumentRoot /var/www/sul1.local/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

**FIGYELEM!** A 2. sorban a **tanulo@SERVER.hu** helyett írja be azt a felhasználónevet és gépnevet ami aktuális éppen a rendszerében. pl.: **tanulo@debian**

Mentéssel lépünk ki, ha készen vagyunk.

## 2. lépés: Engedélyezze a domain konfigurációs fájlt

Engedélyezze az a2ensite eszközzel létrehozott konfigurációs fájlt:

```
sudo a2ensite sul1.local.conf
```

```
Enabling site sul1.hu.
To activate the new configuration, you need to run:
service apache2 reload
```

(FIGYELEM! A képen látható **sul1.hu** helyett **sul1.local** a helyes!)

Az új konfiguráció aktiválása előtt futtassuk a következő parancsot, amely letiltja az eredeti konfigurációs fájlt:

```
sudo a2dissite 000-default.conf
```

```
Site 000-default disabled.
To activate the new configuration, you need to run:
service apache2 reload
```

Indítsa újra az Apache szolgáltatást:

```
sudo systemctl restart apache2
```

## 3. lépés: Tesztelje a konfigurációt

Végül ellenőrizzük, hogy vannak-e konfigurációs hibák a következő parancs segítségével:

```
sudo apache2ctl configtest
```

Ha nem kap hibát, akkor a következő kimenetet látja majd:

```
tanulo@server:~$ sudo apache2ctl configtest
Syntax OK
```

### HIBAJAVÍTÁS

A következő hiba azonban gyakori az Ubuntu-ban:

```
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 192.168.100.5. Set the 'ServerName' directive globally to suppress this message
Syntax OK
```

Oldja meg a hibát a következőképpen:

- Írja be a következő parancsot a fent említett hiba elhárításához:

```
echo "ServerName suli.local" | sudo tee /etc/apache2/conf-available/servername.conf
```

```
tanulo@server:~$ echo "ServerName suli.local" | sudo tee /etc/apache2/conf-available/servername.conf
tee: /etc/apache2/conf-available/servername.conf: No such file or directory
ServerName suli.local
```

- Majd a következő parancsot is adja ki:

```
sudo a2enconf servername
```

```
sudo a2enconf servername
Enabling conf servername.
To activate the new configuration, you need to run:
systemctl reload apache2
```

- Most ismét ellenőrizze, hogy van-e hiba, és láthatja, hogy a fentiekkel megoldódott a probléma:

```
tanulo@server:~$ sudo apache2ctl configtest
Syntax OK
```

## 4. lépés: Vizsgálja meg, hogy az Apache szolgálja-e a domain nevet

Az Apache kiszolgáló úgy van beállítva, hogy kiszolgálja a domain nevet. Ez ellenőrizhető a kiszolgáló nevének az alábbiak szerint történő megadásával a rendszeren futó bármely böngészőben:

**<http://www.suli.local>**

Az indexoldalnak a következőképpen kell megjelennie, jelezve, hogy az Apache készen áll a kiszolgálóblokk kiszolgálására!

 **www.suli.local**

**Hello World!**

## 5. lépés: Saját aláírt tanúsítványok létrehozása

Ha nem tudja telepíteni vagy engedéllyel nem rendelkezik megbízható igazolásokkal egy igazolási hatóságtól, akkor ön aláírt tanúsítvánnyal léphet fel. Mind a megbízható, mind az ön aláírt tanúsítványok azonosak és ugyanazokat a protokollokat használják. Az egyetlen különbség az, hogy az egyiket harmadik fél bíz meg, a másikat pedig nem.

**Ellenőrizze, hogy az alábbi mappák léteznek-e:**

```
sudo ls -l /etc/ssl/private/
```

```
sudo ls -l /etc/ssl/certs/
```

## Majd adja ki az alábbi parancssort:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/suli.local.key -out /etc/ssl/certs/suli.local.crt
```

(Figyelem! A fenti openssl parancs egy sorba írandó!)

pl.:

```
vizsgazo@Company:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/company.local.key -out /etc/ssl/certs/company.local.crt
Generating a 2048 bit RSA private key
.....+++
writing new private key to '/etc/ssl/private/company.local.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
vizsgazo@Company:~$
```

**FIGYELEM! A company.local helyett suli.local írjon!**

**Az adatok kitöltése helyett most nyomhat üres ENTER-eket is.**

- **openssl** : Ez az alapvető parancssori eszköz az OpenSSL tanúsítványok, kulcsok és más fájlok létrehozásához és kezeléséhez.
- **req** : Ez az alparancs meghatározza, hogy használni akarjuk az X.509 tanúsítvány aláírási kérés (CSR) kezelését. Az „X.509” egy nyilvános kulcsú infrastruktúra-szabvány, amelyet az SSL és a TLS betart a kulcs és a tanúsítványkezelés során. Új X.509 tanúsítványt akarunk létrehozni, tehát ezt az alparancsot használjuk.
- **-x509** : Ez tovább módosítja az előző alparancsot azáltal, hogy azt mondja a segédprogramnak, hogy önáláírt tanúsítványt szeretnénk készíteni, ahelyett, hogy tanúsítvány aláírási kérelmet generálnánk, ahogy ez általában megtörténik.
- **-nodes (csomópontok)** : Ez azt mondja az OpenSSL-nek, hogy hagyja ki a tanúsítvány jelszóval történő titkosításának lehetőségét. Szükségünk van az Apache-re, hogy a fájl beolvasása felhasználói beavatkozás nélkül, a szerver indulásakor. Egy jelmondat megakadályozná ezt, mert minden újraindítás után be kell írunk.
- **-days 365** : Ez az opció határozza meg azt az időtartamot, amely alatt a tanúsítvány érvényesnek tekinthető. Itt határoztuk meg egy évre.
- **-newkey rsa: 2048** : Ez meghatározza, hogy új tanúsítványt és új kulcsot akarunk generálni egyszerre. Az előző lépésben nem hoztunk létre olyan kulcsot, amely a tanúsítvány aláírásához szükséges, ezért létre kell hoznunk azt a tanúsítvánnyal együtt. Ez a `rsa:2048` rész azt mondja, hogy készítsen egy 2048 bit hosszú RSA kulcsot.
- **-keyout** : Ez a sor megmutatja az OpenSSL-nek, hogy hová kell helyezni az általunk létrehozott privát kulcsfájlt.
- **-out** : Ez megmondja az OpenSSL-nek, hogy hová kell helyezni az általunk létrehozott tanúsítványt.

A fenti parancsok futtatása után a rendszer felkéri, hogy válaszoljon néhány kérdésre a létrehozott tanúsítvánnyal kapcsolatban.

Ha elkészült a fenti lépésekkel, akkor a privát kulcsfájl az **/etc/ssl/private/** mappa mappába kerül, az úgynevezett **example.com.key** fájlba, és a tanúsítványfájl az **/etc/ssl/certs /** mappa nevű **example.com.crt** fájlba kerül a fenti parancssorban meghatározottak szerint.

Mindkét fájlra hivatkozni kell az Apache2 konfigurációs beállításokban.



```
vizsgazo@Company:~$ sudo cat /etc/ssl/private/company.local.key
-----BEGIN PRIVATE KEY-----
MIIEvGIBADANBgqhkkIG9w0BAQEEFAASCBKAgSkAgEAAoIBAQDhcfF31bK+KmKnW
JKQb3qrhfmfmG5UvdgEPLHyKdD08KLPBxHYRANSgidocd3eSwiUetuiP6IjSHD51
JKxGjdxq0/jm6QqaqaSLRM8jgBpBaJCUUSogAb0eua1FU78UP06BTBC6dmIxIj1x
Z9HfFr0VU69q11Ewp3uMK41ASoi0qU8Mizptz013uD1JwiJhC+ONDOND/qRPsVck
aWSG9nppr138DtU32ftmvG0gPKXzAMC88uPFdN7ToDH12A+Xrv1GhYUua3j/1Qq0
n+90mTsqAL0bq+tk5j22AAi1uUuokvG52I1fo7yF7mGsUGLR//IL+2nPIdBoBdoG
DL7172aQMBAAECgEBANBBrUvefsD043FcfphvJ0nKJy4v4As0eJgpxexXx4ye
pbzRsfl3FfU89dh3gC7ozEQzNQhMNaBToFouYdb3qB9H+ISaIExfwodB01zq0dn4
JaAe/9sDIGK0X8EGbNTs19cCKXdoK14ujn7E4JDaeDms1bTeekCA3MupNlOp6NpH
3uJ5PN7sI3uU5CmskSZL2VRVkg1Vm79qxmW/obNSM47QKY4BAjVe4t4+QK6JHx1a
9K4HLYtWYXaetnKuowHxhi54etEXLvgfowaFB7YWJ2NHJLkT3dar619mmhJ7Vmxg
/gnce0PHKq2q2+ibtU52H2NSYxjuQT06bwaZAxrHa2oCgYEAg9Kys9SGQ2SLseruy
vHSvOxFYjQdWDSWzjfrS1LEtYJ1+j/Usu/LZRor/fWSX/z8iRtjpj3NBQMjHJJzn
cQWn+fzi/E4b+NeRwz3eJgX+JV/si46g8KT5T17JGn0917qvIiCbbBFxIkroPHP
gH3YKSjphXR92Wt+5E6r/+TQTREcGyEA6pS5rVtANPnlaaKDeU4sL+uP25JaAnt
7//8mi01hnZe+180uHuk1oKlnNpzyYN52b7f99n0mvtvkfbiUKEAwb+mq2ZAg7fLrsh/dPF
o0C94ceKdG6DPuVdiKoInNpzyYN52b7f99n0mvtvkfbiUKEAwb+mq2ZAg7fLrsh/dPF
QQ22XIaJ8GkGgYBYf+VZBrzh1MGKmPB/2F2cmu3GtYff7N9r9SfAKK4RHYpV0HF
rmM4fBHR8p12yegzoh3Ka4Rc8+Ur/VFH5+f3cLp6vj1hYXJe0Ge5aG0PGYA54WY7
mSAIie67f8bJavHH5jc86/b87vcUq/+f0iUrET1q61iAbUd11ELGS1R0QKbGbw
E0/IEeX1CE5cWjYtXedv51zbrT6w4oIdfpgLOvKa3VnJY2Sv6BbmLPok4vr1I1fR
Lr1PiHaryCaNR0j5dm1PP6u2XoeiMDm9V9z39qiIaiYdsi26NQ1DTSj/7DvX201E
+XN7re3fsftiUif1knG4P04B24tsXQUJq1WceNUBAoGBALwGMegONPN5skok9tIIT
n4U1opeHPG7nowUM9a2SgKu0Wdj0bkrHX6yMh8P6+6eN1NL0z98aL/NURUXeEBm
HXR956HEKG6ZDNgYtbrLWvt/Ms4Y5jVues2qx7/CirGDmZMPoMcRcWBLyvcMzeRu
WQqMMantirsw3Dgyv7y6m/cvk
-----END PRIVATE KEY-----
vizsgazo@Company:~$
```

```

vizsgazo@Company:~$ sudo cat /etc/ssl/certs/company.local.crt
-----BEGIN CERTIFICATE-----
MIIDATCCACWgAwIBAgIJJAODTnEwHsu1MA0GCSqGSIb3DQEBCwUAMEUwCzAJBgNV
BAYTAFVHRMRWAwQVYDQIDApTB21lLVN0YXR1MSEwHwYDQVQQIDBhJbnRlcm5ldCBY
aWRnaXZrIFBoeSBMdGQwHkHNCmJlNUDEwMjM0NDM3hcnMjTWNDUEwJm0NDM3wJBF
MQswCQYDQVYDQGEwJBVTEtMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50
ZXJuZS1lc3Rlcm5ldCBhZG90eSBhZG90eSBhZG90eSBhZG90eSBhZG90eSBhZG90
CgKCAQEA4Xbd9Wvyip11ZEG96q4X5psBuVL3YBDy4cinXQ/CizwCR2EQDUhiA6
HhdxLFosLboqe1I0hw+dSSsRo3catP45ukKmqmk10TP14AaQW1Q1FEqIAG9Hrmp
RVD/FDzqUwQun21MSI5cKfR3ax9FV0vatdRfQd7JCuJQJAE1jg1PDIs6bc6Jd7g5
ScNY4QvtDQzjQ/6qz7FXJG1khvZ6aa4t/A7bt2X7Zr4DoD1yswDAvPLjxXTe06Ax
5WQP167yBoWDrmt4/9UKtJ/vTpK7KgCzm6vrSuY9tgGopblLqJLxudiJX608he5H
rFb1of/yC/tpz4gw6AXaBgy+5e82mQIDAQABo1AwTjAdBgNVHQ4EFgQUUV6kpVpKD
tc78bE0sU09+2+x0EzYwHwYDVROjBBBgwFAUABV6kpVpKDtC78bE0sU09+2+x0EzYw
DAYDVROTBAlUwAwEB/2ANBgkqhkiG9w0BAQsFAAUCAQEAAdGxJNEb0oFeJY
LiYjrY2ZLU138MLmu9W05BjMjpsJT3f0EcD1BYbbh60zG859m5e5+EI15Y0m01K
Lqoup2HNKJW0y2zV2j27grESsT0h+y9IhoqLN/sX6LPys0nsa6a94jSD7DhbHU+c
hkxaBoE1SPm+TLC1m9sjeCxAkVHnHFYyqJgTse1j8SRyV6sf8kT71rBnsrMG0b9N
wkXPxpjgX1vk1iX4+1fmr9/1Zvy2T2h04Hd4q7rQyLUKuBAb4BfEr2ATTQkpUKuy
qLhQ2TuzcnxeCbzgIbqWfe610Px1XBxS+1+cMf9V0JW11U+XU2P/C9y1oVPJQG2Q
6g==
-----END CERTIFICATE-----
vizsgazo@Company:~$ _

```

## 6. lépés: A tanúsítványok telepítése

A tanúsítvány előállítás után a következő lépés az lesz, hogy telepítse azt az Apache2 szerverre. Ehhez nyissa meg az Apache2 SSL/TLS konfigurációs fájlt az Ubuntu-n, és adja hozzá az alábbiakban a kiemelt sorokat.

```
sudo nano /etc/apache2/sites-available/default-ssl.conf
```

Ezután hivatkozzon a tanúsítványfájlokra Apache2 konfigurációban, az alább látható módon:

**FIGYELEM! A pirossal kiemelt részeket kell átírni/begépelni!**

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin tanulo@debian
```

```
ServerName suli.local
ServerAlias www.suli.local
DocumentRoot /var/www/suli.local/html

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

SSLEngine on

SSLCertificateFile /etc/ssl/certs/suli.local.crt
SSLCertificateKeyFile /etc/ssl/private/suli.local.key
```

```
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
    SSLOptions +StdEnvVars
</Directory>

BrowserMatch "MSIE [2-6]" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost>
```

</IfModule>

Mentse el a fájlt, és zárja be.

## sudo a2ensite default-ssl.conf

```
Enabling site default-ssl.
To activate the new configuration, you need to run:
service apache2 reload
```

Végül indítsuk újra a szolgáltatást és ellenőrizzük a státusz és kész is vagyunk.

```
sudo service apache2 restart
```

```
sudo service apache2 status
```

<https://websiteforstudents.com/setup-apache2-http-with-self-signed-ssl-tls-certificates-on-ubuntu-16-04-lts-servers/>

Edge:

## Adatvédelem

Válassza ki a Microsoft Edge adatvédelmi beállításait. [További tudnivalók ezekről a beállításokról](#)

„Követés letiltása” kérelmek küldése



A webhelyek ellenőrizhetik, hogy vannak-e mentett fizetési módjai



Tanúsítványok kezelése

HTTPS/SSL-tanúsítványok és -beállítások kezelése







## Ez a webhely nem biztonságos.

Ez azt is jelentheti, hogy valaki meg akarja Önt téveszteni, vagy el akarja lopni a kiszolgálónak küldött adatokat. Azt ajánljuk, hogy haladéktalanul zárja be a webhelyet.

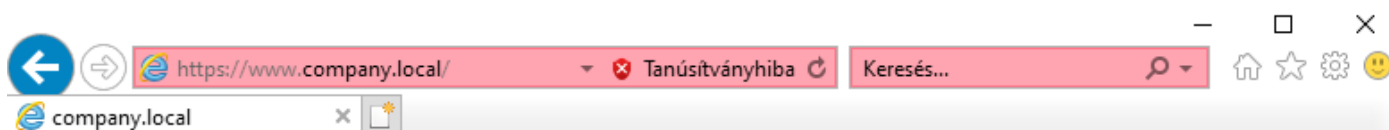
✓ [A lap bezárása](#)

🔍 [További információ](#)

**Az Ön számítógépe nem tekinti megbízhatónak a webhely biztonsági tanúsítványát. A webhely biztonsági tanúsítványában szereplő állomásnév eltér a meglátogatni kívánt webhelytől.**

Hibakód: DLG\_FLAGS\_INVALID\_CA  
DLG\_FLAGS\_SEC\_CERT\_CN\_INVALID

⚠ [Tovább lépés a webhelyre \(nem ajánlott\)](#)



# HELLO!!!