



F5 Big IP Controller 4.X CSR Creation

You can generate a key, a temporary certificate, and a certificate request form with the Configuration utility or from the command line.

Note: We recommend using the Configuration utility for this process. The certification process is generally handled through a web page. Parts of the process require you to cut and paste information from a browser window in the Configuration utility to another browser window on the website.

You must have a separate certificate for each domain name on each BIG-IP Controller or redundant pair of BIG-IP Controllers, regardless of how many non-SSL web servers are load balanced by the BIG-IP Controller.

If you are already running an SSL server, you can use your existing keys to generate temporary certificates and request files. However, you must obtain new certificates if the ones you have are not for the following web server types: Apache + OpenSSL Stronghold

Generating a key and obtaining a certificate using the Configuration utility

To obtain a certificate, you must have a private key. If you do not have a key, you can use the Configuration utility on the BIG-IP Controller to generate a key and a temporary certificate. You can also use the Configuration utility to create a request file that you can submit. You must complete the following tasks in the Configuration utility to create a key and generate a certificate request.

- Generate a certificate request
- Submit the certificate request to a certificate authority and generate a temporary certificate
- Install the SSL certificate from the certificate authority
- Finally, install the intermediate certificate authority certificate.

To create a new certificate request using the Configuration utility

In the navigation pane, click Proxies. The Proxies screen opens.

On Proxies screen, click the Create SSL Certificate Request tab, the New SSL Certificate Request screen opens. In the Key Information section, select a key length and key file name, you can choose either 512 or 1024 bytes. Type in the name of the key file. This should be the fully qualified domain name of the server for which you want to request a certificate. You must add the .key file extension to the name.

In the Certificate Information section, type the information specific to your company.

Country - Type the two letter ISO code for your country

State or Province - Type the full name of your state or province

Locality - Type the city or town name

Organization - Type the name of your organization

Organizational Unit - Type the division name or organizational unit

Domain Name - Type the name of the domain upon which the server is installed

Email Address - Type the email address of a person to be contacted about this



Challenge Password - Type the password you want to use as the challenge password
Retype Password - Retype the password you entered for the challenge password.

Click the Generate Certificate Request button.

After a short pause, the SSL Certificate Request screen opens. Use the SSL Certificate Request screen to start the process of obtaining a certificate from a certificate authority, and then to generate and install a temporary certificate.

Generate and install a temporary certificate

Click the Generate Self-Signed Certificate button to create a self-signed certificate for the server. We recommend that you use the temporary certificate for testing only. You should make your site live only after you receive a properly-signed certificate from a certificate authority. When you click this button, a temporary certificate is created and installed on the BIG-IP Controller. This temporary certificate allows you to set up an SSL gateway for the SSL Accelerator while you wait for a certificate authority to return a permanent certificate.

Generating a key and obtaining a certificate from the command line

To obtain a valid certificate, you must have a private key. If you do not have a key, you can use the `genconf` and `genkey` utilities on the BIG-IP Controller to generate a key and a temporary certificate. The `genkey` and `gencert` utilities automatically generate a request file that you can submit to a certificate authority. If you have a key, you can use the `gencert` utility to generate a temporary certificate and request file.

These utilities are described in the following list:

genconf - This utility creates a key configuration file that contains specific information about your organization. The `genkey` utility uses this information to generate a certificate.

genkey - After you run the `genconf` utility, run this utility to generate a temporary 30 day certificate for testing the SSL Accelerator on the BIG-IP Controller. This utility also creates a request file that you can submit to a certificate authority to obtain a certificate.

gencert - If you already have a key, run this utility to generate a temporary certificate and request file for the SSL Accelerator.

To generate a key configuration file using the genconf utility

If you do not have a key, you can generate a key and certificate with the `genconf` and `genkey` utilities. First, run the `genconf` utility from the root (`/`) with the following commands:

```
cd /  
/usr/local/bin/genconf
```

The utility prompts you for information about the organization for which you are requesting certification. This information includes:

- The fully qualified domain name (FQDN) of the server
- The two-letter ISO code for your country
- The full name of your state or province



The city or town name
The name of your organization
The division name or organizational unit

To generate a key using the genkey utility

After you run the genconf utility, you can generate a key with the genkey utility.

```
cd /user/local/bin/genkey
```

After the utility starts, it prompts you to verify the information created by the genconf utility. After you run this utility, a certificate request form is created in the following directory:

```
/config/bigconfig/fqdn.req
```

In addition to creating a request form that you can submit to a certificate authority this utility also generates a temporary certificate. The temporary certificate is located in:

```
/config/bigconfig/ssl.crt/fqdn.crt
```

The "fqdn" is the fully qualified domain name of the server. Note that you must copy the key and certificate to the other controller in a redundant system, but for an SSL proxy you should have a valid certificate from your certificate authority.

To generate a certificate with an existing key using the gencert utility

To generate a temporary certificate and request file to submit to the certificate authority with the gencert utility, you must first copy an existing key for a server into the following directory on the BIG-IP Controller:

```
/config/bigconfig/ssl.key/
```

After you copy the key into this directory, type the following command at the command line:

```
cd /user/local/bin/gencert
```

After the utility starts, it will prompt you for various information. After you run this utility, a certificate request form is created in the following directory:

```
/config/bigconfig/ssl.crt/fqdn.req
```

The "fqdn" is the fully qualified domain name of the server