How to Request An SSL In 100TB Console

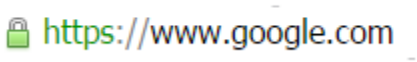
This Knowledgebase article was created to help you with installing a Secure Socket Layer Certificate for an added layer of security to the web traffic on your server.

Also known as an SSL, these certificates are generally required when operating or hosting any sensitive data such as credit cards, social security numbers, bank accounts and private or personal information.

The SSL will add a layer of security by encrypting the internet traffic between a server and a end user. All SSLs have the following attributes:

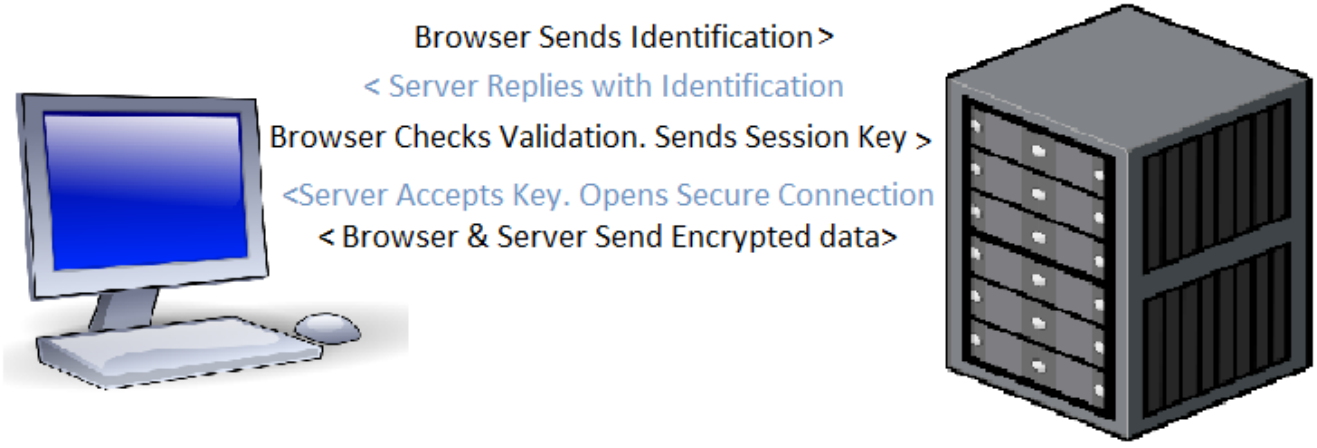
- Private Key: Stored on the server, should never be divulged, copied, sent in an email, text or any other form of communication. This is the unique key that makes the SSL secure, and must remain unique to the server.
- Public Key: Used when verifying the server's Identity.
- CSR: Used to issue an SSL, will contain information such as address, domain and country.
- Certificate: Issued from an authorized certificate authority.

All of this information is stored on the server that the domain/content is hosted on. This will appear in your web browser as a green padlock, which indicates that the server has a properly authenticated and working SSL Certificate. For example:



The most important part of any SSL is the issuer. Although the private key is important, there are several ways to generate self-signed SSLs for use, especially for smaller types of hosting setups or private domains. In order for the green padlock to appear in your URL, your SSL needs to be signed by a trusted CA (Certificate Authority). We have partnered with Comodo® as our SSL issuer to provide trusted certificates from a valid Certificate Authority. We highly recommend working through our partnership to make sure that any SSLs you purchase will properly protect your websites.

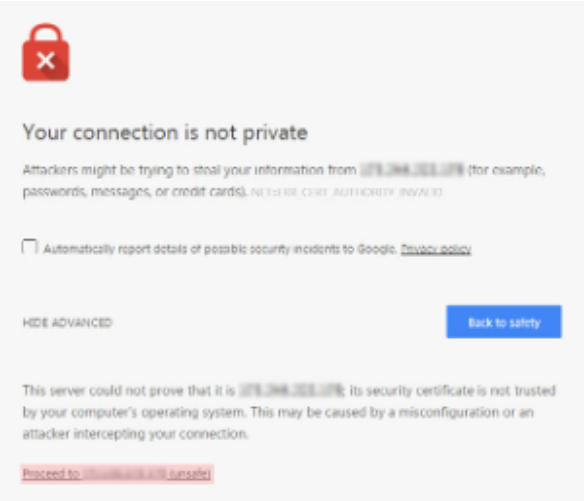
The most important part of any SSL is the issuer. Although the private key is important, there are several ways to generate self-signed SSLs for use, especially for smaller types of hosting setups or private domains. In order for the green padlock to appear in your URL, your SSL needs to be signed by a trusted CA (Certificate Authority). We have partnered with Comodo® as our SSL issuer to provide trusted certificates from a valid Certificate Authority. We highly recommend working through our partnership to make sure that any SSLs you purchase will properly protect your websites.



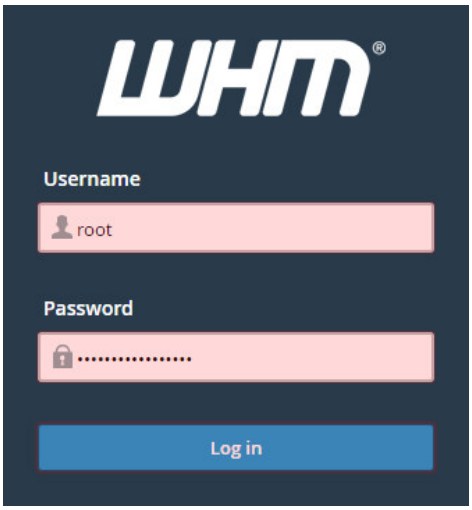
T

Generate a Private Key and CSR in WHM

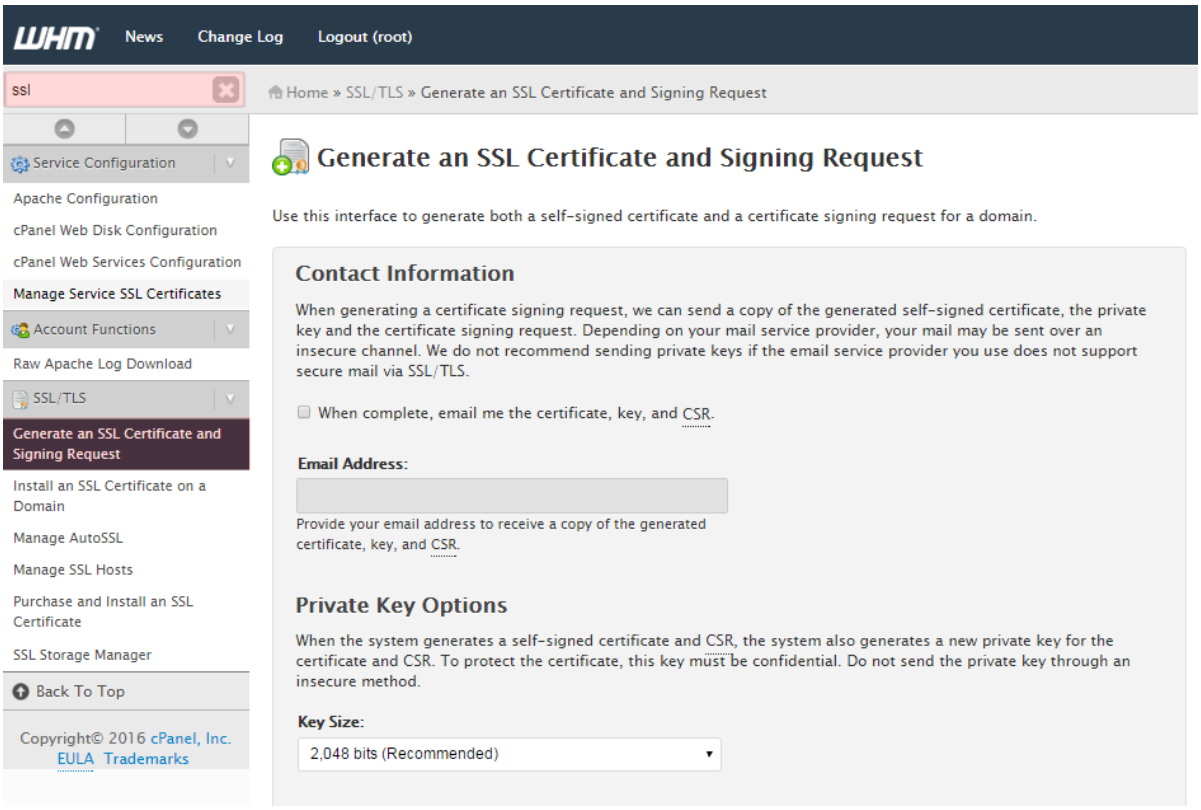
First, log into your WHM manager as ‘root’ at https://yourserversip:2087. If you don’t have an SSL for your server’s hostname, you’ll see a warning that the connection is not private. In this Chrome example, you can continue with the advanced option, and proceed anyway:



For WHM, you will use the root user and the root password provided by us. If you choose to copy and paste these, make sure there is no whitespace before and after the password characters, otherwise the system will not accept your entries.



Once logged in, you can search SSL in the search bar. Then, click “Generate an SSL Certificate and Signing Request”:



Next, complete any of the empty fields with the required information.

****DO NOT PUT IN A PASSPHRASE****. Passphrases stored in CSRs are not encrypted, which means third-party attackers can easily read these passphrases and these are generally not needed.

Enter the empty fields on the form with the following information:

Email Address - If you would like the CSR emailed to you

Domains - You can put one domain/subdomain only

City

State

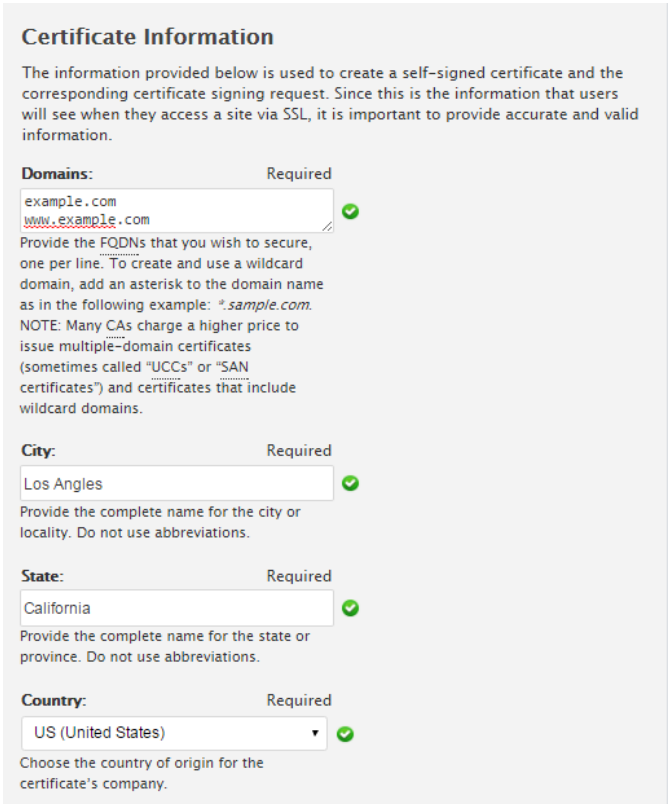
Country

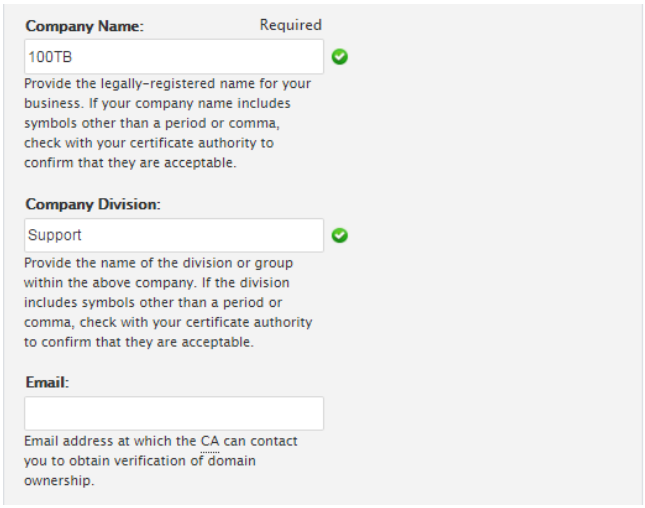
Company Name

Company Division

Email - Enter an email address at which the Certificate Authority can contact you to obtain verification of domain ownership.

100TB example:





Click “Create” once you have entered all of the important information. This process will generate a CSR and matching private key.
You will need to copy the Signing Request (CSR) ONLY:

Generate a Private Key And CSR Via Command Line

If you're not using WHM/CPanel software, you can use command line to generate the private key and CSR necessary to get an SSL on your server.

First, make sure you have openssl installed.

> Note - Openssl is installed in conjunction with an Apache Web Server (HTTPD) installation.

Ubuntu /Debian

```
#> sudo apt-get install openssl
```

CentOS /RedHat

```
#> yum install openssl
```

- Note: This is typically installed on CentOS by default.

1. Create a Private Key to store on the Server

```
#> openssl genrsa -des3 -out (private key name goes here).key 2048
```

```
example@server~]#  openssl genrsa -des3 -out example.com.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.............+++
e is 65537 (0x10001)
Enter pass phrase for example.com.key:
```

2. Enter a passphrase for the .key:

Enter anything you'd like, but note that it needs to be at least 4 characters long.

```
Enter pass phrase for example.com.key:
Verifying - Enter pass phrase for example.com.key:
example@server~]#
```

3. Generate a CSR (Certificate Signing Request)

```
#> openssl req -new -key test_private.key -out  test.csr
```

You will be asked to fill out the following fields:

- Country Name (2 Letter code):
- State or Province (eg, city) []
- Organization Name (eg, company) []:
- Organizational Unit Name (eg, section) []:
- Common Name (e.g. server FQDN or YOUR name) []:(your domain name for the SSL here)
- Email Address []:

Note, a challenge Password or optional company name is not necessary to complete and can be left blank.

```
example@server~]#  openssl req -new -key example.com.key -out example.com.csr
Enter pass phrase for example.com.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) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:LA
Organization Name (eg, company) [Default Company Ltd]:example inc.
Organizational Unit Name (eg, section) []:Development
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:example@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
example@server~]#
```

Once you have completed the required fields, a .csr file will be created. You can use the commands cat or less to view the contents of the file and copy the CSR.

First type "ls" to list out the files in the current directory.

```
example@serverssl]#  ls
example.com.csr  example.com.key
```

Then you can view what's inside by using the command:

```
#> cat example.com.csr
```

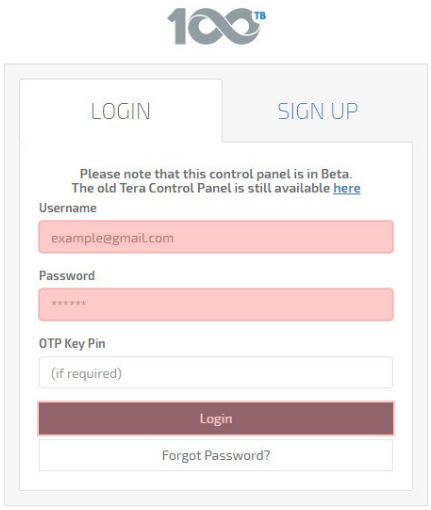
```
example@serverssl]#  cat example.com.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC1DCCAbwCAQAwgY4xCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTELMAkGA1UE
BwwCTEExFTATBgNVBAoMDGV4YW1wbGUgaW5jLjEUMBIGA1UECwwLRGV2ZWxvcG11
bnQxFDASBgNVBAMMC2V4YW1wbGUuY29tMSIwIAYJKoZIhvcNAQkBFhN1eGFtcGxl
QGV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuN58
/wPEFGK2mU2dXON8GL7IWzV19mvR7JIX3YdfRLkrs3aX/ONK+lySyPvwotSIAVW2
coDgG8/kesfSCX1woId6hic+099aQ/dexN3KbuBenEUyqADIr497ebzm3nFRuKxD
FlptakND1VazK4jkKWF12TjlM/PXd9gwqps+LtdpNGSxt/TMk/TK1RMNncm5Ic2n
CdnzJNJa0v+WbLq759CEHztuuoHt03JZ0q342E6HK59vvDXuKh+0SB3lsseQQDU0
6w1kad8YA1+W+umWnBoA1/Mk1RsTDGVK8mM1sRroe5M7X+IsXISnqQnuzsPtRmdH
EfQeQyYZA5cHEPzZFwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAEUu3iSo/FgX
UadmZRjojRWgcwdDpAAPESnboK7ec59GLpTstxUZTHarYD+mWX1BSGIGWmk3LZab
Vpz3SEeIqIuha4Hi7r9xA8y9HJPQ4vcxgWOvdk1KLre/8dullUfDA3rf5fkvOZDT
I3rK6zpFyrwSCu8IkSiYib5KT7q0owoDoM+Q1TB0seVKPKShwhwBoLtHKHk/VZvm
bNF9USJWHRxcrnf6spx5SwowvSibHNmSw/Xe73AmrwufmfiAeb2joxVozmS52OP6
6+E5clrIK9NwXLTdLD5tYsB8J05ShVRzr+PT91Ozfyn19TJrlt/k3/iBVUe2y6Q1
D1ZpeFYPSPM=
-----END CERTIFICATE REQUEST-----
```

With your mouse, highlight the certificate from ---------BEGIN all the way till REQUEST------

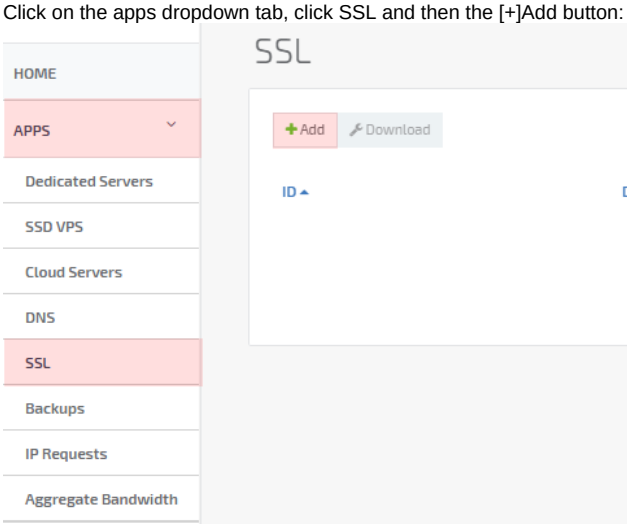
In PuTTY, this will copy to your clipboard.

Request Your SSL in Console

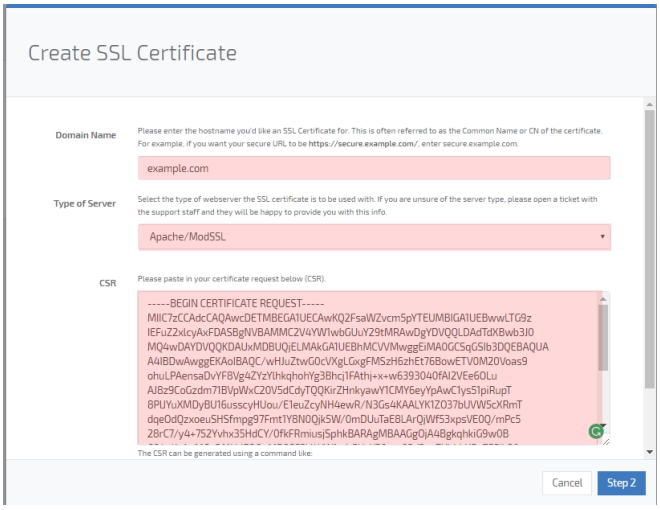
1. Log into https://console.100tb.com



2. Click on the apps dropdown tab, click SSL and then the [+]Add button:

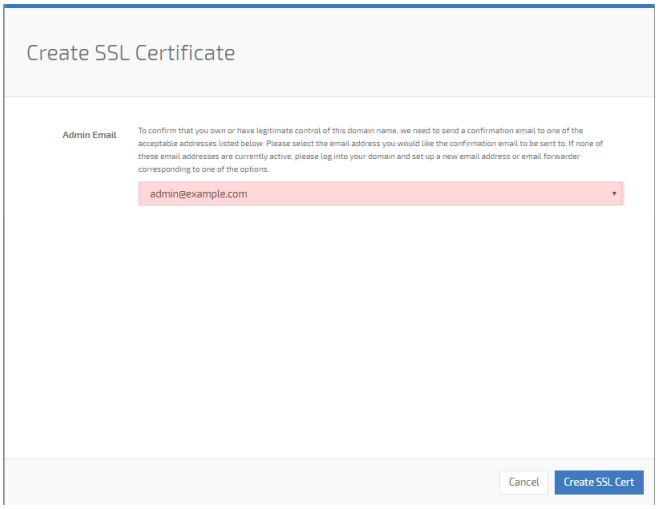


3. Next, enter the hostname (Domain name) you'd like to create an SSL Certificate for. This is often referred to as the Common Name or CN of the certificate. For example, if you want your secure URL to be https://secure.example.com/, enter secure.example.com. Or if you prefer https://www.example.com/, enter www.example .com. Make sure to replace example.com with your own hostname/domain name.
4. Paste the CSR into the space provided:

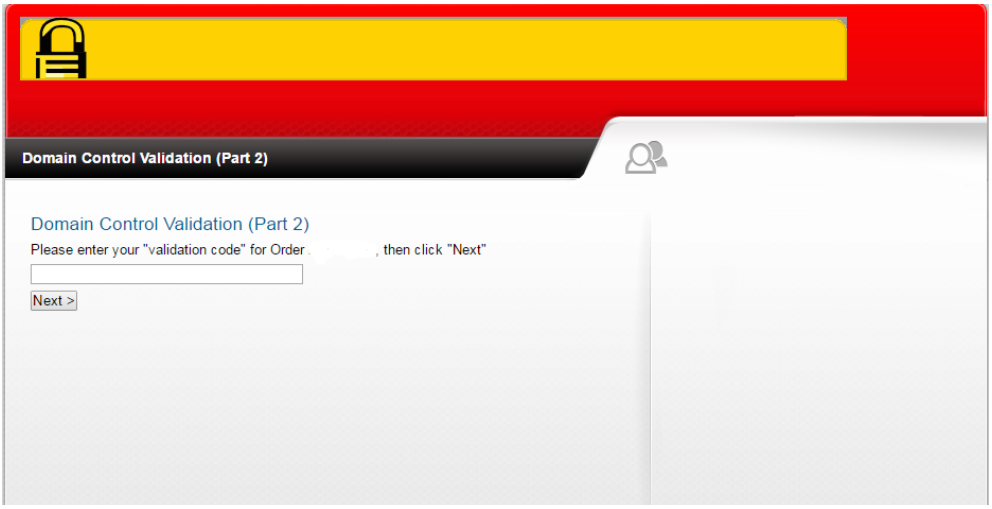


Once you have Entered in the Domain/Hostname and pasted the Signing Request from WHM, click “Step 2”. You will be prompted to select an email address that the SSL can be verified with.

IMPORTANT! Make sure that the email you select is in the dropdown list provided and is able to receive email. Our SSL issuer Comodo requires that you have a working admin email.



Once you click “Create SSL Cert” it may take some time for the SSL issuer to provide it for you in your account. You will need to check your email for a verification email from Comodo.



You will be able to download this once Comodo has issued, it and you’ll be able to view it within your https://console.100tb.com/#/apps/ssl list.

Contact Support

If you have any questions about this process, please contact our technical support team by opening a chat or creating a ticket.