How to configure https and digest

1. MPD/IS file directory

/continuous/content/

1. Sa file directory

/content/sa

1. Turn off  the firewall service

#service iptables stop

#service ip6tables stop

1. Create a RSA private key for apache server

# openssl genrsa -des3 -out server.key 2048

1. Create a Certificate Signing Request (CSR) with the server RSA private key

# openssl req -new -key server.key -out server.csr

Note:

in this step, it requires to input several information about your identity, for the “Common name” you should input the domain name of this server.

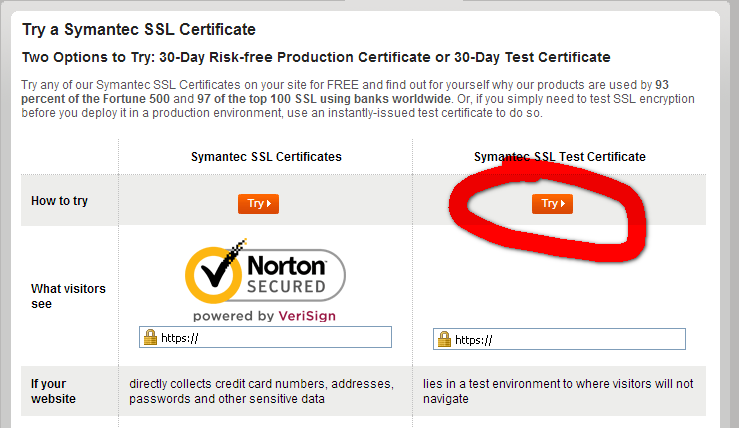
1. Apply the certificate from a CA

now we use Symantec to get the signed certificate. For test, we use the trial certificate provided by Symantec.

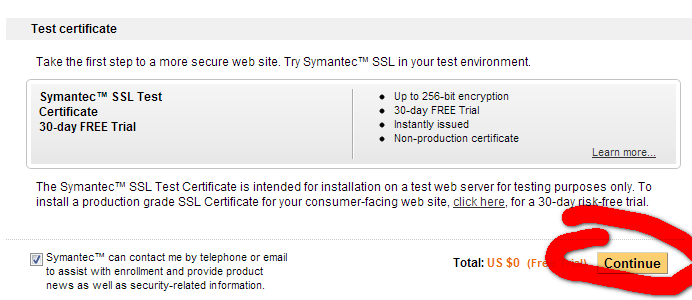
* 1. Login to

<https://www.symantec.com/en/aa/theme.jsp?themeid=verisign-ssl-certificates&tabID=4&inid=vrsn_symc_ssl_Try>

* 1. Choose Symantec SSL Test Certificate

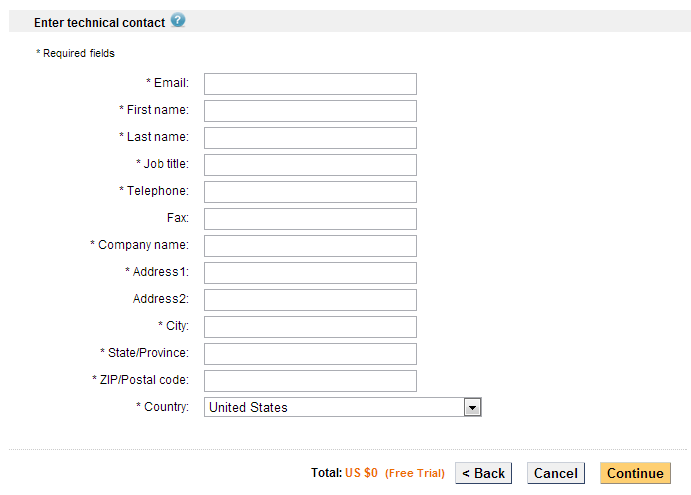


* 1. Accept the policy and continue

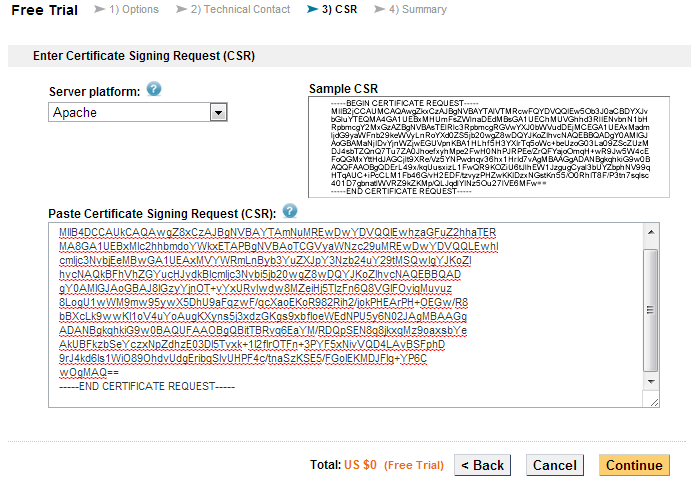


* 1. Fill your personal information for test.

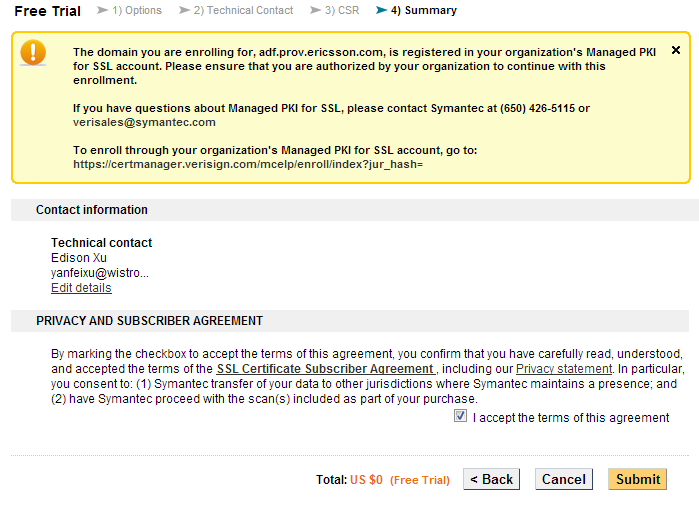
Note: The mailbox must be accessible to receive the certificate published!



* 1. Open csr file and paste the contents into the box. Choose Apache as server platform.



* 1. Accept the Summary and continue



* 1. Check the mailbox you input and receive the certificate

After finishing the steps in that chapter, you will get a mail immediately from Symantec, containing the certificate of the CDN server which is already signed.

* 1. Copy the certificate at the bottom of the mail, and paste as **mpdis.crt** file
  2. Download CA file

In the mail it also provides the links of two CA’s certificates (CA root certificate and CA intermediate certificate), both of which is used to decrypt of the signature of the certificate (here is CDN server) it issues. Please save these two certificates into two files:

ca-intermediate-trialSymantic.crt ca-root-trialSymantic.crt

* 1. put three certificates on the apache server, the path doesn’t matter but you should remember it:

1. at /var/tmp/apache\_https/ca\_certificate/ 🡨 here store the CA’s certificate.

ca-intermediate-trialSymantic.crt ca-root-trialSymantic.crt

1. at /var/tmp/apache\_https/

mpdis.crt

1. Configure Apache https conf files

#vi /etc/httpd/conf/extra/httpd-vhosts.conf

*<VirtualHost \*:443>*

*SSLEngine on*

*SSLOptions +StrictRequire*

*SSLProtocol +all*

*SSLCipherSuite HIGH:MEDIUM:!aNULL:+SHA1:+MD5:+HIGH:+MEDIUM*

*SSLSessionCacheTimeout 600*

*SSLCertificateFile /var/tmp/apache\_https/mpdis.crt*

*SSLCertificateKeyFile /var/tmp/ apache\_https /server.key*

*# authenticate user by user/password*

*DocumentRoot /content/sa/*

*<Directory /content/sa/>*

*Options Indexes MultiViews*

*AllowOverride None*

*Order allow,deny*

*allow from all*

*AuthType Digest*

*AuthName "MPDIS"*

*AuthUserFile /etc/httpd/conf/extra/.passwd*

*AuthDigestProvider file*

*Require valid-user*

*</Directory>*

*</VirtualHost>*

1. Generate .passwd file and add digest username/password

# htdigest -c /etc/httpd/conf/extra/.passwd [realm name] [user name]

The realm name should be same as the value of “AuthName” defined in /etc/httpd/conf/extra/httpd-vhosts.conf file.

1. Start apache server

#apachectl start

The output is as below:

*Apache/2.2.27 mod\_ssl/2.2.27 (Pass Phrase Dialog)*

*Some of your private key files are encrypted for security reasons.*

*In order to read them you have to provide the pass phrases.*

*Server test.test:443 (RSA)*

*Enter pass phrase:*

Please input the password you input when Create a RSA private key

1. Verify http and digest in another machine
   1. prepare ca file

put the two certificates to fold, the path doesn’t matter but you should remember it:

for example: /var/tmp/testca

ca-intermediate-trialSymantic.crt

ca-root-trialSymantic.crt

* 1. combine the two ca file

# cat ca-root-trialSymantic.crt >> ca-bundle-for-cdn.pem

# cat ca-intermediate-trialSymantic.crt >> ca-bundle-for-cdn.pem

* 1. mapping domain name and IP address in /etc/hosts

for example:

#vi /etc/hosts

192.168.12.20 MPDIS

* 1. Configure .curlrc

#cd ~

#vi .curlrc

Add -u username:password

For example:

-u bmsc:embms1234

* 1. get sa file

#curl --cacert /var/tmp/testca/ca-bundle-for-cdn.pem --digest https://<domain>:443/< file path>

for example:

#curl --cacert /var/tmp/testca/ca-bundle-for-cdn.pem --digest https://MPDIS:443/bmsc/test.tx

* 1. upload MPD/IS file

curl -T <file path> http://<domain>:80

for example:

curl -T /var/tmp/my-net.xml http://MPDIS:80

1. Upload file to SFTP
   1. Connect to SFTP:

# sftp bmsc@<domain>

For example:

# sftp bmsc@MPDIS

* 1. input the password

default password is: bmscpass

* 1. go the current user’s fold

sftp> cd /bmsc

* 1. upload file

sftp> put <file name in current fold>

for example:

sftp> put sa

* 1. logout

sftp> bye