

C·O·M·O·D·O
EnterpriseSSL

Using EnterpriseSSL to boost consumer confidence in your web services

For Apache-based servers

www.comodogroup.com

support@comodogroup.com



Tel: (877) COMODO-5



Tel: +44 (0) 161 874 7070

Why you need **security** for your website

The Internet has created many new global business opportunities for enterprises conducting online commerce. However, the many security risks associated with conducting e-commerce have resulted in security becoming a major factor for online success or failure.

Over the past 7 years, consumer magazines, industry bodies and security providers have educated the market on the basics of online security. The majority of consumers now expect security to be integrated into any online service they use, as a result they expect any details they provide via the Internet to remain confidential and integral. For many customers, the only time they will ever consider buying your products or services online is when they are satisfied their details are secure.

This guide explains how you can utilize EnterpriseSSL to activate the core security technology available on your existing webserver. You will also learn how EnterpriseSSL allows you to protect your customer's transactions and provide visitors with proof of your digital identity – essential factors in gaining confidence in your services and identity.

Using EnterpriseSSL Certificates to secure your online transactions tells your customers you take their security seriously. They will visibly see that their online transaction will be secure, confidential and integral and give them the confidence that you have removed the risk associated with trading over the Internet.

Using Security helps you realize the benefits of online commerce:

- Cost effectiveness of online operations and delivery
- Open global markets – gain customers from all over the world
- New and exciting ways of marketing directly to your customers
- Offer new data products and services via the Web

Only if you have visibly secured your site with SSL security technology will your customers have confidence in your online operations. Read on to learn how SSL helps you achieve the confidence essential to successful e-commerce.

What is SSL?

Secure Sockets Layer, SSL, is the standard security technology for creating an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. In order to be able to generate an SSL link, a web server requires an SSL Certificate.

When you choose to activate SSL on your webserver you will be prompted to complete a number of questions about the identity of your website (e.g. your website's URL) and your company (e.g. your company's name and location). Your webserver then creates two cryptographic keys – a Private Key and a Public Key. Your Private Key is so called for a reason – it must remain private and secure. The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) – a data file also containing your details. You should then submit the CSR during the SSL Certificate application process Comodo, the EnterpriseSSL Certification Authority, who will validate your details and issue an SSL Certificate containing your details and allowing you to use SSL.

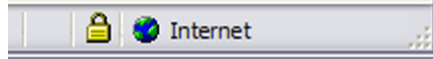
Your webserver will match your issued SSL Certificate to your Private Key. Your webserver will then be able to establish an encrypted link between the website and your customer's web browser.

For detailed application and installation instructions please refer to section "Step by step instructions to set up SSL on your webserver" of this guide.

“SSL is the de facto web transaction security technology. Webservers have been built to support it; web browsers have been built to use it. Secure your customers transactions transparently without your customers having to do a thing!”

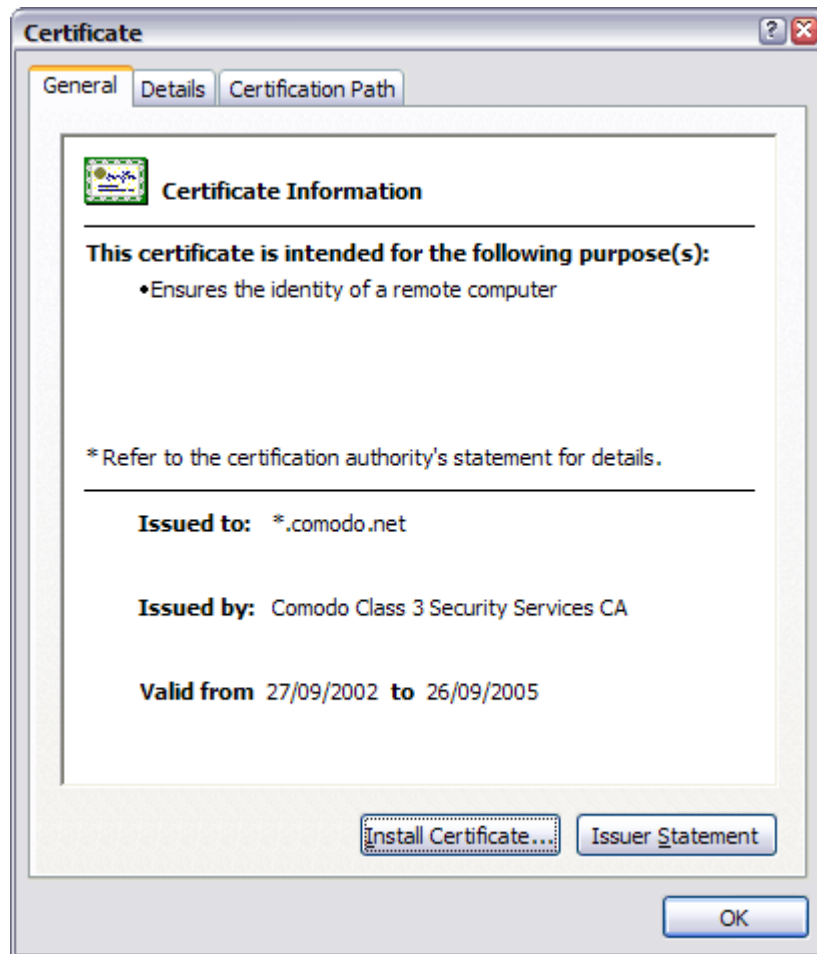
Displaying the SSL secure padlock

The complexities of the SSL protocol remain invisible to your customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session – the Padlock:



As seen by users of Internet Explorer

Clicking on the Padlock displays your SSL Certificate and your details:



As seen by users of Internet Explorer

All SSL Certificates are issued to either companies or legally accountable individuals. Typically an SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiry date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate.

When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user.

“Starting at only \$139 per year per Certificate, with multi-year discounts available, EnterpriseSSL provide the most cost effective fully validated and fully supported Enterprise Certificates available.”

Why should you use an **EnterpriseSSL Certificate**?

Comodo, the Certification Authority behind EnterpriseSSL, is the fastest growing SSL Provider in the world. Unlike other Certification Authorities, Comodo does not just provide SSL Certificates – they are a world-renowned security and cryptography service provider. When you are a customer of Comodo, you can feel safe knowing that your website security is provided by experts.

EnterpriseSSL Certificates are the most cost-effective fully validated and fully supported 128 bit SSL enterprise-specific certificates you can buy today! You can contact the technical support team between 3am - 7pm EST (soon to be 24 hours). You can also feel safe in the knowledge that Comodo will validate your application in accordance with the latest digital signature legislation pertaining to Qualified Certificates. This validation is done effectively and quickly, ensuring you need not wait the traditional 3 working days normally associated with a fully validated SSL Certificate.

EnterpriseSSL boasts industry leading browser ubiquity – comparable to Verisign and Thawte, however without the costs associated with other SSL Providers. EnterpriseSSL Certificates are compatible with over 99.3% of browsers – including Internet Explorer 5.00 and above, Netscape 4.5 and above, AOL 6 and above and Opera 5.00 and above.

EnterpriseSSL benefits summary:

EnterpriseSSL Certificates are the most cost effective SSL Certificates you can buy which include:

- Full validation conducted quickly – in many cases you can expect your SSL Certificate to be issued within minutes
- Multi-channel priority support with dedicated account manager
- Over 99.3% browser compatibility
- 128 bit strong encryption security

EnterpriseSSL Certificates provide you with the key to successfully using SSL on your webserver.

Step by step instructions to set up SSL on your Apache webserver

There are four stages to setting up SSL on your Apache webserver:

1. Create a Certificate Signing Request (CSR)
2. Apply online
3. Installing your Certificate
4. Displaying your Secure Site Seal

1. Generating a Certificate Signing Request (CSR)

A CSR is a file containing your certificate application information, including your Public Key. Generate your CSR and then copy and paste the CSR file into the web form in the enrolment process:

Generate keys and certificate:

To generate a pair of private key and public Certificate Signing Request (CSR) for a webserver, "server", use the following command:

```
openssl req -new -nodes -keyout myserver.key -out server.csr
```

This creates two files. The file myserver.key contains a private key; do not disclose this file to anyone. Carefully protect the private key.

In particular, be sure to backup the private key, as there is no means to recover it should it be lost. The private key is used as input in the command to generate a Certificate Signing Request (CSR).

You will now be asked to enter details to be entered into your CSR

.

What you are about to enter is what is called a Distinguished Name or a DN.

For some fields there will be a default value, If you enter '.', the field will be left blank.

```
-----  
Country Name (2 letter code) [AU]: GB  
State or Province Name (full name) [Some-State]: Yorks  
Locality Name (eg, city) []: York  
Organization Name (eg, company) [Internet Widgits Pty Ltd]: MyCompany  
Ltd  
Organizational Unit Name (eg, section) []: IT  
Common Name (eg, YOUR name) []: mysubdomain.mydomain.com  
Email Address []:
```

Please enter the following 'extra' attributes to be sent with your certificate request

```
A challenge password []:  
An optional company name []:  
-----
```

Use the name of the webserver as Common Name (CN). If the domain name is mydomain.com append the domain to the hostname (use the fully qualified domain name).

The fields email address, optional company name and challenge password can be left blank for a webserver certificate.

Your CSR will now have been created. Open the server.csr in a text editor and copy and paste the contents into the online enrolment form when requested.

2. Applying for your EnterpriseSSL Certificate Online

Visit www.enterprisesssl.com and select your SSL Certificate product type. You will be required to submit the CSR into a web form. When you make your application, make sure you include the CSR in its entirety into the appropriate section of the enrolment form. When you view your CSR it will appear something like:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVjCCAr8CAQAwedMBSGA1UEAxMUD3d3Lm15ZG9tYWlubmFtZS5jb20xDDAK
BgNVBAsTAldlyjEaMBGGA1UEChMRWW91ciBDb21wYW55IE5hbWUxEDA0BgNVBAct
B015IENpdHkxETAPBgNVBAGTCE15IFN0YXRlMQswCQYDVQQGEWJVUzCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAuev9LnSRX/6u5Iz7ckpt0IG4DwnAF/lksJ0
n5r9w1EK9Np5/OJEt72r5es3nie5rTKo304yvSLovkS0vqT+i0lEzvl5B4mXTEPw
fDLjEcwcNb8SCJ4ArUAhHKJWHDKJHDKDA6587568gfhjffjFHGFHPhsgGHJGJjhhj
HFD^TGFrYTrYTrfGHI&DHJKDHkjjwikkAgwCgYIKoZIhvcNHHKIHfrytDETR$456
AwcwEwYDVR01BAwwGjYkAwYABOjEAWBvgfjGCisAQQEGjNagiIve4wgesCAQEE
WgBNAGkAYwByAG8AZwByAGEAcABOAGkAYwAgAFAAcgvBvAHYAaQBkAGUAcgOBiQCq
QwByAHkAcAB0AG8AZwByAGEAcABOAGkAYwAgAFAAcgvBvAHYAaQBkAGUAcgOBiQCq
EH3QppP7Ewuz6oh4EUXMbKdqieAcBQ52iFSXqQ/nlxAtEpVUfjIM3exr42EhyYlr
1V7cpUKbSr/eQ6c/hjiUi17EpvleBBV0BkFwSwzJoShx0BmOKvDnKINNQC3Jya+M
N/t9axyuCdUYJiLglNnJcBLSxL/6hovXNDLuCLgMAAAAAAAAAAAAAAMA0GCSqGSIB3
DQEBBQUAA4GBAEQT6Pwj0BHeOUw+AR0GAT30q+1OYNkr341CouMC6M7Kq1KgVZDV
tRes4uz1Yf8+WRCutVvDByrey+CdgzJzHvHqS61Aj2swx8QadclVWOkZfH//k/KE
1MiOeb6c3Mp1ECorjIm+HRN20Qga+dnDBOowyRyn7Vz+Nkar88mrJwk/
-----END NEW CERTIFICATE REQUEST-----
```

Be sure to copy the CSR text in its entirety into the application form, including the:

```
-----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----
```

3. Installing your EnterpriseSSL Certificate

Step one: Copy your certificate to file

You will receive an email from Comodo Security Services with the certificate in the email (**yourdomainname.crt**). When viewed in a text editor, your certificate will look something like:

```
-----BEGIN CERTIFICATE-----
MIIDVjCCAr8CAQAwedMBSGA1UEAxMUD3d3Lm15ZG9tYWlubmFtZS5jb20xDDAK
BgNVBAsTAldlyjEaMBGGA1UEChMRWW91ciBDb21wYW55IE5hbWUxEDA0BgNVBAct
B015IENpdHkxETAPBgNVBAGTCE15IFN0YXRlMQswCQYDVQQGEWJVUzCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAuev9LnSRX/6u5Iz7ckpt0IG4DwnAF/lksJ0
n5r9w1EK9Np5/OJEt72r5es3nie5rTKo304yvSLovkS0vqT+i0lEzvl5B4mXTEPw
fDLjEcwcNb8SCJ4ArUAhHKJWHDKJHDKDA6587568gfhjffjFHGFHPhsgGHJGJjhhj
HFD^TGFrYTrYTrfGHI&DHJKDHkjjwikkAgwCgYIKoZIhvcNHHKIHfrytDETR$456
AwcwEwYDVR01BAwwGjYkAwYABOjEAWBvgfjGCisAQQEGjNagiIve4wgesCAQEE
WgBNAGkAYwByAG8AZwByAGEAcABOAGkAYwAgAFAAcgvBvAHYAaQBkAGUAcgOBiQCq
QwByAHkAcAB0AG8AZwByAGEAcABOAGkAYwAgAFAAcgvBvAHYAaQBkAGUAcgOBiQCq
EH3QppP7Ewuz6oh4EUXMbKdqieAcBQ52iFSXqQ/nlxAtEpVUfjIM3exr42EhyYlr
1V7cpUKbSr/eQ6c/hjiUi17EpvleBBV0BkFwSwzJoShx0BmOKvDnKINNQC3Jya+M
N/t9axyuCdUYJiLglNnJcBLSxL/6hovXNDLuCLgMAAAAAAAAAAAAAAMA0GCSqGSIB3
DQEBBQUAA4GBAEQT6Pwj0BHeOUw+AR0GAT30q+1OYNkr341CouMC6M7Kq1KgVZDV
tRes4uz1Yf8+WRCutVvDByrey+CdgzJzHvHqS61Aj2swx8QadclVWOkZfH//k/KE
1MiOeb6c3Mp1ECorjIm+HRN20Qga+dnDBOowyRyn7Vz+Nkar88mrJwk/
-----END CERTIFICATE-----
```

Copy your Certificate into the directory that you will be using to hold your certificates. In this example we will use `/etc/ssl/cert/`. Both the public and private key files will already be in this directory. The private key used in the example will be labelled `private.key` and the public key will be `yourdomainname.crt`.

It is recommended that you make a directory that contains the private key file only readable by root.

Step two: Install the Intermediate Certificates

You will need to install the chain certificates (intermediates) in order for browsers to trust your certificate. As well as your SSL certificate (`yourdomainname.crt`) two other certificates, named `GTECyberTrustRootCA.crt` and `ComodoClass3SecurityServicesCA.crt`, are also attached to the email from Comodo Security Services.

Apache users will not require these certificates. Instead you can install the intermediate certificates using the following 'bundle' method. In the Virtual Host settings for your site, in the `httpd.conf` file, you will need to complete the following:

1. Copy the below `ca-bundle` file to the same directory as `httpd.conf` (this contains all of the CA certificates in the chain).

```
-----BEGIN CERTIFICATE-----
MIIB+jCCAWMCAGjMA0GCSqGSIb3DQEBAUAMEUxCzAJBgNVBAYTAlVTMRgwFgYD
VQQKEw9HVEUgQ29ycG9yYXRpb24xHDAaBgNVBAMTE0dURSBDDeWJlclRydXN0IFJv
b3QwHhcNOTYwMjIzMjMwMTAwWhcNMDYwMjIzMjM1OTAwWjBFMQswCQYDVQQGEwJV
UzEYMBYGA1UEChMFR1RFIENvcnBvcnF0aW9uMRwwGgYDVQQDEXNHVEUgQ3liZXJl
cnVzdCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC45k+625h8cXyv
RLfTD0bZZOWTWUK0x7pJjTUtEueLveUFMVnGss8KDPufpz+iCwAEVh43KRuH6X4M
ypqfpX/1FZSjlaJGgthoTNE3FQZor734sLPwKFVWVgkWYXcKLiXUT0Wqx7311t/5
lKiOQswkB6RJ0q1bQaAYznEol44AwIDAQABMA0GCSqGSIb3DQEBAUAA4GBABKz
dcZfHeFhVYAA1IFLezEPI2PnPFMD+fQ2qLvZ46WXTeorKeDwanOB5sCJo9Px4KWl
IjeaY8JIILTbcuPI9t18vrGvU9oUtCG41tWW4/5ODFlitppK+Uldjg+BqXH/9Apy
bW1EDp3zdHSolTRJ6V6e6bR64eVaH4QwnNofpSXY
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEyDCCBDGgAwIBAgIEAgACmzANBgkqhkiG9w0BAQUFADBQMswCQYDVQQGEwJV
UzEYMBYGA1UEChMFR1RFIENvcnBvcnF0aW9uMRwwGgYDVQQDEXNHVEUgQ3liZXJl
cnVzdCBSb290MB4XDTEyMDYwMjIzMjMwMTAwWhcNMDYwMjIzMjM1OTAwWjBFMQsw
CQYDVQQGEwJVUzEYMBYGA1UEChMFR1RFIENvcnBvcnF0aW9uMRwwGgYDVQQDEXNH
VEUgQ3liZXJlcnVzdCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD
BAsTFihjKTIwMDI9Q29tb2RvIEExpbWl0ZWQxLDAgBgNVBAMTl0NvbnV9kbyBDbGFz
cyAzIFNlY3VyaXR5IFNlcnZpY2VzIENBMTIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAsR5gZuDBBp4naC8CmceI34Xr22Xs1Elnei4fzdwVLNYerPKdRjpd
A8A9BSxaGALZJUKjcsCtKNKtPDHiSfw7XpjrQDPwabJanuosSaYmLkzWzKtA0qre
LE6Btbp7uFzQe71H9cAG0sDk10fbYkCvoRrRaxjbuNC71Mc8eeolZK4mGeE8Zkdn
kpl7Vas0wnVu2SeOnYzwhDprnIYEopC16p2Mz/s5Q6jwGC2e9xkQLJwv4dCx/9dZ
xM1AMVnXgdtrHPJBUoFBSYO4yAn+mSJHgE+cy67gKNUcrHBHsCWroTChFC2v6am6N
X3n49ikDMKRurtSFXapAmTh22x4BfeUmpQIDAQABo4IBpzCCAAMrQYDVR0fBD4w
PDA6oDigNoY0aHR0cDovL3d3dy5wdWJsawMtDHJlc3QuY29tL2NnaS1iaW4v1JfM
LzIwMDYvY2RwLmNybdAgBgNVHQ4EFgQU91IiFxUTCANZvxixVn0i0uen++GYwgZIG
AlUdIASBijCBhzBJBgoqhkig+GMBAGEFMDswOQYIKwYBBQUHAGELWlh0dHA6Ly93
d3cuHvibG1jLXRYdXN0LmNvbS9DUFMvT21uaVJvb3QuaHRtbDdA6BgwrBgEABIX
AQIBAwEwKjAobGgrBgEFBQcCARYcaHR0cHM6Ly9zZW51cmUy29tb2RvLm51dC9D
UDBYBgNVHSMEUTBPOUmKRzBFMQswCQYDVQQGEwJVUzEYMBYGA1UEChMFR1RFIEN
vcnBvcnF0aW9uMRwwGgYDVQQDEXNHVEUgQ3liZXJlcnVzdCBSb290ggIBozArBgNV
HRAEJDAiga8yMDAyMDgyNzE5MDczMVqBDzIwMDUwMjIzMjM1OTAwWjA0BGNVHQ8B
Af8EBAMCAEYwDwYDVR0TBAGwBgEB/wIBADANBgkqhkiG9w0BAQUFAAOBGC2p7B6
cYvgurOBHjYyeeOY1vGrTtK1cQZaZ6BLAeUwQG2JtZ4VqrHH9ArGXA7pN96o18fc
zslx+3QCB9xfFSIUwd21LkG6cJ3UB7KybdCROGAAL1EqlzWINlVMr5W1vHqvaDj
vA2AourM+5pX7XilnjlW6tHndMo0w8+uXengDA==
-----END CERTIFICATE-----
```

2. Add the following line to SSL section of the httpd.conf (assuming /etc/httpd/conf is the directory to where you have copied the ca.txt file). if the line already exists amend it to read the following:

```
SSLCACertificateFile /etc/httpd/conf/ca-bundle/ca.txt
```

If you are using a different location and certificate file names you will need to change the path and filename to reflect your server.

The SSL section of the updated httpd config file should now read similar to this example (depending on your naming and directories used):

```
SSLCertificateFile /etc/ssl/crt/yourdomainname.crt
```

```
SSLCertificateKeyFile /etc/ssl/crt/private.key
```

```
SSLCACertificateFile /etc/httpd/conf/ca-bundle/ca_new.txt
```

Save your **httpd.conf** file and restart Apache.

Fast, cost-effective **SSL Security** for your webserver...


The Internet is a revolutionary medium for you to improve your sales and online services for customers. EnterpriseSSL is the perfect solution to securing your webserver with SSL quickly, easily and cost-effectively.

Contact us to discuss your individual security requirements

Contact us between 3am and 7pm EST to discuss how InstantSSL can help you:

support@comodogroup.com

sales@comodogroup.com

Comodo 

Comodo Group Ltd, 3401 E. McDowell Rd,
Suite B, Phoenix AZ 85008.

Tel: (877) COMODO-5

Fax: (720) 863 2140

3am- 7pm EST

Comodo 

Comodo Europe
New Court, Regents Place,
Regent Road, Manchester M5 4HB,
United Kingdom

Tel: +44 (0) 161 874 7070

Fax: +44 (0) 161 877 1767

8am - 12am GMT

www.comodogroup.com