Entrust.Net

Technical Information –
Frequently Asked Questions

Client Confidential

TABLE OF CONTENTS

O'REILLY WEBSITE PROFESSIONAL 2.X

This section provides the answers to the most commonly asked questions about O'Reilly WebSite Professional 2.x. If you have a question that is not answered here please contact Entrust support.

WHY DOES NAVIGATOR 3.X DISPLAY A "SECURITY LIBRARY ERROR" WHEN USERS CONNECT TO MY SERVER?

This sometimes happens after you apply the 2.0b hotfix to WebSite Pro 2.0. For a description of the issue and possible solutions see the O'Reilly Web Site.

WHEN I INSTALL MY CERTIFICATE I SEE THE ERROR "FAILED TO IMPORT CERTIFICATE. CORE: KEY NOT FOUND". WHY?

The root certificate (from Thawte) that was included in your Web server may have expired.

Check the root certificate expiry as follows: open Server Properties, open the Key Ring, and select Trusted Roots. Double-click the entry named "Thawte Server CA" and look under the Certificate heading for the expiry date. If the root certificate has expired, import a new one as described below. If the root certificate has not expired you may be having problems that are not related to your Entrust.net Web server certificate. Please take a look at the O'Reilly Technical Support pages at http://software.oreilly.com/techsupport/ for possible solutions.

Import the new root certificate as follows: open http://www.entrust.net/support/serverbasic.txt in a Web browser. The root certificate will be displayed in the browser window. Copy the root certificate from the browser into a text editor and save the file to your hard drive. Then follow the instructions in your WebSite Pro documentation to import the root certificate. If you are using O'Reilly WebSite Professional 2.0, ensure that you have applied the 2.0b hotfix before attempting to import the new certificate. The hotfix is available from the O'Reilly Technical Support Knowledge Base.

WHY DOES NETSCAPE NAVIGATOR 4.06 AND HIGHER DISPLAY THE ERROR "NETSCAPE HAS ENCOUNTERED BAD DATA FROM THE SERVER" WHEN CONNECTING TO O'REILLY WEBSITE PROFESSIONAL 2.1 - 2.3.7?

This can happen when a 128-bit version of Netscape Navigator 4.06 browser is set up to use RC4 or RC2 encryption with a 40-bit key and an MD5 MAC and attempts to connect to a 128-bit WebSite Professional server that is using a server certificate with a 1024-bit key. This issue affects WebSite Professional 2.1 to 2.3.5. For a description of the problem and possible solutions, see theO'Reilly Technical Support Knowledge Base.

WHY DO NAVIGATOR 3.X USERS SEE A "CERTIFICATE AUTHORITY EXPIRED" MESSAGE WHEN THEY CONNECT TO MY SERVER?

They have not yet updated the root certificate in their browsers. See Managing root certificate expiry for recommendations on how to deal with this issue. You will find detailed instructions on how users can update their root certificates in Importing a root certificate into your Web browser.

I'VE INSTALLED MY ENTRUST.NET WEB SERVER CERTIFICATE. WHY ISN'T IT ACTIVE?

If you are having trouble activating a certificate in your Web server, please see the O'Reilly Technical Support pages.

APACHE (MOD_SSL): APACHE-SSL OR APACHE (MOD_SSL)

This section provides the answers to the most commonly asked questions about Apache-SSL and Apache with mod_ssl. If you have a question that is not answered here please contact Entrust support.

Note: This section assumes that you are using SSLeay with your server. If you are using OpenSSL instead of SSLeay, you will find additional information at http://www.openssl.org.

I'M NOT SURE I'LL BE ABLE TO INSTALL MY ENTRUST.NET WEB SERVER CERTIFICATE. IS THERE A WAY I CAN TRY INSTALLING A CERTIFICATE BEFORE I BUY ONE?

Yes, Entrust provides trial Web server certificates (with a limited lifetime) for free at http://freecerts.entrust.com. If you can install one of these free trial certificates you will also be able to install your Entrust.net Web server certificate.

WHY DO I GET A “NO START LINE:PEM_LIB.C” OR “NO END LINE:PEM_LIB.C”MESSAGE?

The certificate text file you created for your server may contain extra spaces or characters. In most cases the file contains trailing spaces after the”-----BEGIN CERTIFICATE-----” or “-----END CERTIFICATE-----” lines. These spaces are sometimes added when you paste the certificate into a text editor. Simply remove the spaces or characters and try again.

WHY AM I ASKED FOR A PASSPHRASE WHEN THE SERVER STARTS?

You chose to encrypt the private key when you generated the key pair. It is a very good idea to protect your private key this way. Someone with access to your private key and password could decrypt the SSL-protected data sent and received by your Web server, or set up an unauthorized Web server in your name.

HOW DO I KNOW WHICH CERTIFICATE A PRIVATE KEY IS ASSOCIATED WITH?

The private key contains a series of numbers. Two of those numbers , the “modulus” and the “public exponent” form the public key. The public key data is also contained in your certificate. To find out if a particular private key is associated with a certificate you must view the private key and the certificate and compare the public key data in each. If the modulus and public exponent values match then the certificate is associated with that private key.

Use the following command to view a certificate:
ssleay x509 -noout -text -in certfile
Use the following command to view the key:ssleay rsa -noout -text -in keyfile

WHY DOESN'T THE BROWSER RECOGNISE THE ISSUER OF THE CERTIFICATE?

The user may be using an older browser that is unsupported. See Supported browsers for more information. If a new browser such as Internet Explorer 4.x or Navigator 4.x is giving this error then your server is presenting the wrong certificate to the browser. To find out which certificate you are using simply connect to your secure site using a browser and view the certificate information (in Navigator click Security and then click View Certificate.

If you are using the wrong certificate you must update your Apache configuration file to make the server present the correct certificate.

WHY DO NAVIGATOR 3.X USERS SEE A "CERTIFICATE AUTHORITY EXPIRED" MESSAGE WHEN THEY CONNECT TO MY SERVER?

They have not yet updated the root certificate in their browsers. See Managing root certificate expiry for recommendations on how to deal with this issue. You will find detailed instructions on how users can update their root certificates in Importing a root certificate into your Web browser.

HOW DO I MAKE APACHE-SSL USE A PARTICULAR KEY AND CERTIFICATE?

The configuration information for your server generally resides in a file named "httpd.conf" in your server directory structure. Update this configuration file to contain the following entries:

SSLCertificateFile </path/to/mycertfile.crt>
SSLCertificateKeyFile </path/to/mykeyfile.key>

WHY DOES THE DOCUMENTATION ASK FOR A CERTIFICATE IN PEM FORMAT?

The Apache-SSL documentation and the documentation for the SSLeay toolkit incorrectly refer to certificates as "PEM" (Privacy Enhanced Mail) files. Apache-SSL, like all SSL servers, uses the X.509 certificate format. The certificates are referred to as "PEM" files because they are Base-64 encoded, and Base-64 encoding was defined as part of the Privacy Enhanced Mail (PEM) specification.

WHERE CAN I GET MORE INFORMATION ABOUT MY SERVER?

The Apache-SSL Web site http://www.apache-ssl.org and the Apache-SSL mailing list apache-ssl@lists.aldigital.co.uk are very good sources of information about the Apache-SSL Web server.

APACHE-SSL OR APACHE (MOD_SSL)

This section provides the answers to the most commonly asked questions about Apache-SSL and Apache with mod_ssl. If you have a question that is not answered here please contact Entrust support.

Note: This section assumes that you are using SSLeay with your server. If you are using OpenSSL instead of SSLeay, you will find additional information at http://www.openssl.org.

I'M NOT SURE I'LL BE ABLE TO INSTALL MY ENTRUST.NET WEB SERVER CERTIFICATE. IS THERE A WAY I CAN TRY INSTALLING A CERTIFICATE BEFORE I BUY ONE?

Yes, Entrust provides trial Web server certificates (with a limited lifetime) for free at http://freecerts.entrust.com. If you can install one of these free trial certificates you will also be able to install your Entrust.net Web server certificate.

WHY DO I GET A "NO START LINE:PEM_LIB.C" OR "NO END LINE:PEM_LIB.C"MESSAGE?

The certificate text file you created for your server may contain extra spaces or characters. In most cases the file contains trailing spaces after the"-----BEGIN CERTIFICATE-----" or "-----END CERTIFICATE-----" lines. These spaces are sometimes added when you paste the certificate into a text editor. Simply remove the spaces or characters and try again.

1.1 WHY AM I ASKED FOR A PASSPHRASE WHEN THE SERVER STARTS?

You chose to encrypt the private key when you generated the key pair. It is a very good idea to protect your private key this way. Someone with access to your private key and password could decrypt the SSL-protected data sent and received by your Web server, or set up an unauthorized Web server in your name.

HOW DO I KNOW WHICH CERTIFICATE A PRIVATE KEY IS ASSOCIATED WITH?

The private key contains a series of numbers. Two of those numbers , the "modulus" and the "public exponent" form the public key. The public key data is also contained in your certificate. To find out if a particular private key is associated with a certificate you must view the private key and the certificate and compare the public key data in each. If the modulus and public exponent values match then the certificate is associated with that private key.

Use the following command to view a certificate:
ssleay x509 -noout -text -in certfile
Use the following command to view the key:ssleay rsa -noout -text -in keyfile

WHY DOESN'T THE BROWSER RECOGNISE THE ISSUER OF THE CERTIFICATE?

The user may be using an older browser that is unsupported. See Supported browsers for more information. If a new browser such as Internet Explorer 4.x or Navigator 4.x is giving this error then your server is presenting the wrong certificate to the browser. To find out which certificate you are using simply connect to your secure site using a browser and view the certificate information (in Navigator click Security and then click View Certificate.

If you are using the wrong certificate you must update your Apache configuration file to make the server present the correct certificate.

WHY DO NAVIGATOR 3.X USERS SEE A "CERTIFICATE AUTHORITY EXPIRED" MESSAGE WHEN THEY CONNECT TO MY SERVER?

They have not yet updated the root certificate in their browsers. See Managing root certificate expiry for recommendations on how to deal with this issue. You will find detailed instructions on how users can update their root certificates in Importing a root certificate into your Web browser.

HOW DO I MAKE APACHE-SSL USE A PARTICULAR KEY AND CERTIFICATE?

The configuration information for your server generally resides in a file named "httpd.conf" in your server directory structure. Update this configuration file to contain the following entries:

SSLCertificateFile </path/to/mycertfile.crt>
SSLCertificateKeyFile </path/to/mykeyfile.key>

WHY DOES THE DOCUMENTATION ASK FOR A CERTIFICATE IN PEM FORMAT?

The Apache-SSL documentation and the documentation for the SSLeay toolkit incorrectly refer to certificates as "PEM" (Privacy Enhanced Mail) files. Apache-SSL, like all SSL servers, uses the X.509 certificate format. The certificates are referred to as "PEM" files because they are Base-64 encoded, and Base-64 encoding was defined as part of the Privacy Enhanced Mail (PEM) specification.

Where can I get more information about my server?

The Apache-SSL Web site http://www.apache-ssl.org and the Apache-SSL mailing list apache-ssl@lists.aldigital.co.uk are very good sources of information about the Apache-SSL Web server.

NETSCAPE ENTERPRISE SERVERS

This section provides answers to the most commonly asked questions about Netscape Enterprise Servers. If you have a question that is not answered here please contact Entrust support.

WHY DO NAVIGATOR 3.X USERS SEE A “CERTIFICATE AUTHORITY EXPIRED” MESSAGE WHEN THEY CONNECT TO MY SERVER?

They have not yet updated the root certificate in their browsers. See Managing root certificate expiry for recommendations on how to deal with this issue. You will find detailed instructions on how users can update their root certificates in Importing a root certificate into your Web browser.

C2NET STRONGHOLD

This section provides the answers to the most commonly asked questions about C2Net Stronghold. If you have a question that is not answered here please contact Entrust support.

WHY DOES GETCA DISPLAY AN ERROR SAYING THAT THE CERTIFICATE DOES NOT MATCH THE KEY?

Your server is using a key that does not correspond to your Entrust.net Web server certificate. To find out if a particular private key is associated with a certificate you must view the private key and the certificate and compare the public key data in each. If the modulus and public exponent values in each file match, then the certificate is associated with that private key. Once you have found the correct certificate and key, update the Stronghold configuration file to use the correct key and certificate file.

WHY DOES INTERNET EXPLORER DISPLAY “AN ERROR OCCURRED IN THE SECURE CHANNELSUPPORT”?

Internet Explorer displays this message if the certificate installed on your server contains a public key larger than 1024 bits. Stronghold allows you to create key pairs up to 4096 bits in length. However, many browsers have problems processing keys longer than 1024 bits.

To resolve this issue, generate a 1024-bit key pair and CSR and request a new Entrust.net Web server certificate.

WHY DOES NETSCAPE NAVIGATOR DISPLAY “THE SERVER HAS ENCOUNTERED BAD DATA FROM THE CLIENT”?

Netscape Navigator displays this message if the certificate installed on your server contains a public key larger than 1024 bits. Stronghold allows you to create key pairs up to 4096 bits in length. However, many browsers have problems processing keys longer than 1024 bits.

To resolve this issue, generate a 1024-bit key pair and CSR and request a new Entrust.net Web server certificate.

WHY DO NAVIGATOR 3.X USERS SEE A “CERTIFICATE AUTHORITY EXPIRED” MESSAGE WHEN THEY CONNECT TO MY SERVER?

They have not yet updated the root certificate in their browsers. See Managing root certificate expiry for recommendations on how to deal with this issue. You will find detailed instructions on how users can update their root certificates in Importing a root certificate into your Web browser.

1.2 WHERE CAN I FIND MORE INFORMATION?

See our Apache-SSL FAQ.

MICROSOFT INTERNET INFORMATION SERVER (IIS)

This section provides the answers to the most commonly asked questions about IIS. If you have a question that is not answered here please contact Entrust support.

WHY DO I KEEP LOSING MY KEYS IN KEY MANAGER?

You may not have committed your changes. If you don't commit your changes you lose any keys generated during the session. If you lose the private key that corresponds to the CSR you sent us, you will not be able to use the certificate you receive. It is strongly recommended that you also make a backup of your keys. To do this, click Key > Export Key > Backup File. You must remember the password you choose for the key. If you write down the password, please store it in a secure place (for instance, a locked cabinet to which only you have the key).

WHY DO I SEE THE MESSAGE “INVALID PASSWORD” WHEN IMPORTING MY CERTIFICATE INTO IIS 3 KEY MANAGER?

You may be using an old version of the file "schannel.dll". For more information and an updated version of the file see the Microsoft Knowledge Base article Q179550. This problem has also been addressed in Windows NT SP 4.

This error also appears if you are using the wrong private key with your certificate.

WHY DID MY CERTIFICATE DISAPPEAR WHEN I UPGRADED TO IIS 4.0B2?

You may have installed IIS 4.0B2 over your existing IIS installation. If you've lost your keys, you should be able to recreate them from your backups. If you don't have backups you will have to request another Entrust.net Web server certificate.

WHY DO NAVIGATOR 3.X USERS SEE A “CERTIFICATE AUTHORITY EXPIRED” MESSAGE WHEN THEY CONNECT TO MY SERVER?

They have not yet updated the root certificate in their browsers. See Managing root certificate expiry for recommendations on how to deal with this issue. You will find detailed instructions on how users can update their root certificates in Importing a root certificate into your Web browser.

WHY DO NAVIGATOR 3.X USERS GET A DATABASE ERROR AFTER THEY UPDATE THEIR ROOT CERTIFICATE?

These users have updated the root certificate in their browsers but your server contains the old root certificate. To solve this problem you must update the root certificate in your server. See Installing root certificates in your Web server for details on the problem and how to resolve it.

WHY CAN'T I INSTALL MY CERTIFICATE WITH SP 3 AND 128 BIT ENCRYPTION?

You can, but you need to remove Service Pack 3 and install it again choosing 40 bit encryption. You may also have to make a registry change to make IIS 3 accept the certificate. See the the Microsoft Knowledge Base article Q174779 for details on this problem and how to resolve it.

WHY DO NAVIGATOR USERS SEE THE MESSAGE “IMPROPERLY FORMATTED DER MESSAGE” WHEN CONNECTING TO MY SERVER?

Navigator does not recognize one of the data types used in your server certificate. In most cases this is a result of using extended character sets in your certificate. To resolve the problem generate a new key and CSR that do not include extended characters (Unicode characters, for instance) and then request a new Entrust.net Web server certificate.

WHY DO USERS SEE THE MESSAGE “CONNECTION WITH SERVER COULD NOT BE ESTABLISHED”?

See The Microsoft Knowledge Base article Q164884 for details on this problem and how to resolve it.

HOW DO I BACK UP MY KEY?

To back up your key click Key > Export Key > Backup File. You must remember the password you choose for the key. If you write down the password, please store it in a secure place (for instance, a locked cabinet to which only you have the key).