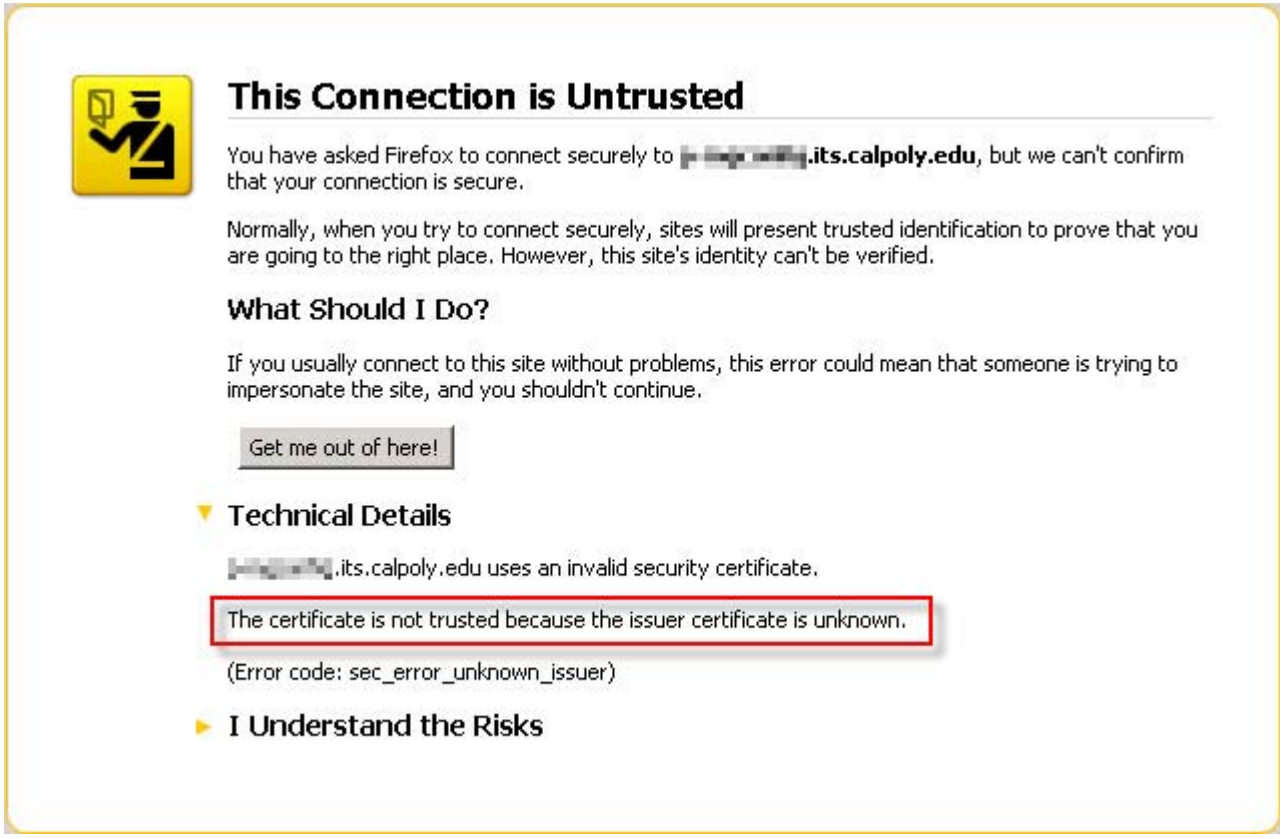
SSL Certificate Not Trusted Error - For Server Administrators

2 Added by Dan Malone, last edited by Dan Malone on Apr 25, 2011

SSL Certificate Not Trusted Error



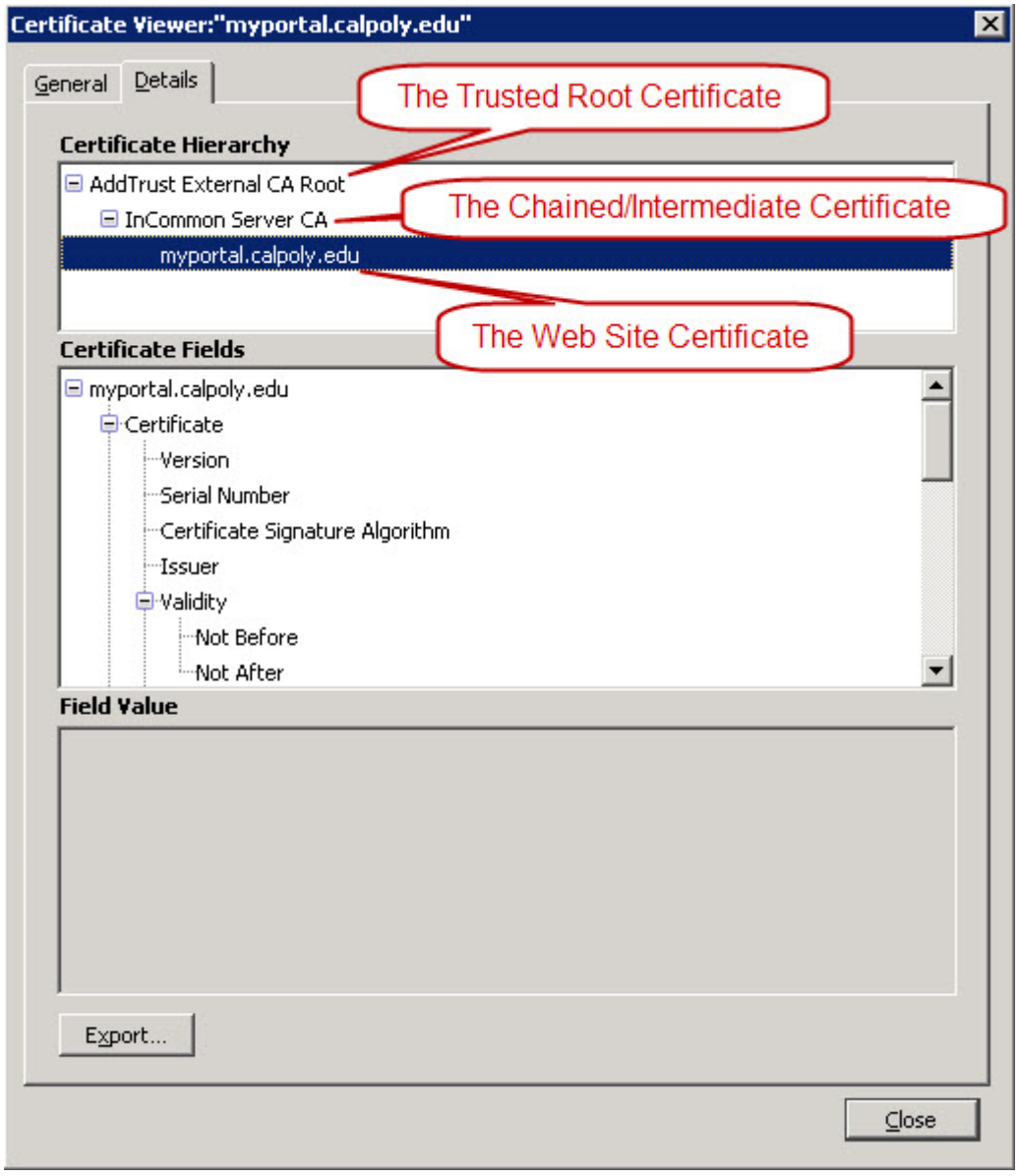
The SSL certificate not trusted error indicates that the SSL certificate is not signed or approved by a company that the browser trusts. This occurs most often for one of the following reasons:

1. The web site is using a self-signed certificate. Self-signed certificates can be generated for free but they don't provide the trust a commercial certificate authority can. You should not tell users to trust your self-signed certificate because we do not want users to feel this is good practice. A man-in-the-middle attack will look the same to a user.
2. The web site is using a free SSL Certificate. Free SSL Certificates are issued by a couple of free certificate authorities but users must follow a complex process to import the Root Certificate into their browser.
3. The web site is using an SSL certificate from a trusted certificate authority but it is missing a chain/intermediate certificate. Most trusted certificate authorities require that you install at least one other intermediate/chain certificate on the server to link your certificate up to a trusted source.

To address issues #1 and #2, Cal Poly now provides SSL certificates from a trusted certificate authority (Comodo) at no cost for Cal Poly sites. More information on this service can be found on the Operations and Production Support web site http://ops.calpoly.edu

/ssl.html.

Issue #3 is a very common one. For example, if the ITS installed their server certificate for myportal.calpoly.edu without installing the "InCommon Server CA" intermediate certificate, a web browser would give the certificate not trusted error.



Occasionally, certain browsers will give this error when others do not. This is because browsers can automatically download intermediate certificates the first time you visit a site that is properly configured. Once the intermediate certificate is installed, the browser will work on all sites using that intermediate certificate without getting this error, including a site that does not provide the intermediate certificate itself.

How to check if my server is properly configured

Because the Cal Poly Portal is properly configured, many browsers will already have the intermediate certificate installed. This makes testing a newly installed SSL certificate difficult. You can verify whether the certificate and the appropriate intermediate certificate are installed correctly by using the following process.

Process to check if a server is properly configured

1. This process requires openssl

2. Create a file called AddTrustExternalCARoot.crt with a PEM copy of the AddTrust External CA Root certificate (only).

AddTrustExternalCARoot.crt

```
-----BEGIN CERTIFICATE-----
MIIENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU
MBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTHUFkZFRydXN0IEV4dGVybmFs
IFRUUCBOZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBFeHRlcm5hbCBDQSBSb290
MB4XDTAwMDUzMDEwNDgzOFoXDTIwMDUzMDEwNDgzOFowbzELMAkGA1UEBhMCU0Ux
FDASBgNVBAoTC0FkZFRydXN0IEFCMSYwJAYDVQQLEx1BZGRUcnVzdCBFeHRlcm5h
bCBUVFAgTmV0d29yazEiMCAGA1UEAxMZQWRkVHJ1c3QgRXh0ZXJuYWwgQ0EgUm9v
dDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALf3GjPm8gAELTngTlvt
H7xsD821+iO2zt6bETOXpClMfZOfvUq8k+0DGuOPz+VtUFrWlymUWoCwSXrbLpX9
uMq/NzgtHj6RQa1wVsfwTz/oMp50ysiQVOnGXw94nZpAPA6sYapeFI+eh6FqUNzX
mk6vBbOmcZSccbNQYArHE504B4YCqOmoaSYYkKtMsE8jqzpPhNjfzp/haW+710LX
a0Tkx63ubUFfclpxCDezeWWkWaCUN/cALw3CknLa0Dhy2xSoRcRdKn23tNbE7qzN
E0S3ySvdQwAl+mG5aWpYIxG3pzOPVnVZ9c0p10a3CitlttNCbxWyuHv77+ldU9U0
WicCAwEAAaOB3DCB2TAdBgNVHQ4EFgQUrb2YejS0Jvf6xCZU7wO94CTLVBowCwYD
VR0PBAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wgZkGA1UdIwSBkTCBjoAUrb2YejS0
Jvf6xCZU7wO94CTLVBqhc6RxMG8xCzAJBgNVBAYTAlNFMRQwEgYDVQQKEwtBZGRU
cnVzdCBBQjEmMCQGA1UECxMdQWRkVHJ1c3QgRXh0ZXJuYWwgVFRQIE5ldHdvcmsx
IjAgBgNVBAMTGUFkZFRydXN0IEV4dGVybmFsIENBIFJvb3SCAQEwDQYJKoZIhvcN
AQEFBQADggEBALCb4IUlwtYj4g+WBpKdQZic2YR5gdkeWxQHIzZlj7DYd7usQWxH
YINRsPkyPef89iYTx4AWpb9a/IfPeHmJIZriTAcKhjW88t5RxNKWt9x+Tu5w/Rw5
6wwCURQtjr0W4MHfRnXnJK3s9EK0hZNwEGe6nQY1ShjTK3rMUUKhemPR5ruhxSvC
Nr4TDea9Y355e6cJDUCrat2PisP29owaQgVR1EX1n6diIWgVIEM8med8vSTYqZEX
c4g/VhsxOBi0cQ+azcgOno4uG+GMmIPLHzHxREzGBHNJdmAPx/i9F4BrLunMTA5a
mnkPIAou1Z5jJh5VkpTYghdae9C8x49OhgQ=
-----END CERTIFICATE-----
```

3. Run the following command, where *<server>:<port>* is replaced with the server and port to be tested, e.g. myportal.calpoly.edu:443 .

```
openssl s_client -CAfile AddTrustExternalCARoot.crt </dev/null -connect
<server>:<port>
```

   a. A server that is properly configured with the intermediate certificate will respond with:

```
...
Verify return code: 0 (ok)
---
DONE
```

   b. A server that is NOT properly configured with the intermediate certificate will respond with:

```
...
Verify return code: 21 (unable to verify the first certificate)
---
DONE
```

How to Fix The Untrusted Error

To fix this error, you will need to install the "InCommon Server CA" intermediate/chain certificate onto the web server in a way that delivers it to the web browser. If you have any questions about how to do this, Comodo provides detailed SSL certificate installation instructions for many different types of servers.

- Comodo Knowledge Base: https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=95&pcid=1&nav=0,1