Entrust.Net

Technical Information –
Root Expiry

Client Confidential

TABLE OF CONTENTS

ROOT CERTIFICATES

1.1 ROOT CERTIFICATE ROLLOVER

The server certificate you receive from Entrust is accepted by almost all Web browsers in use today. This is because the root certificate used by Entrust is valid in all these browsers. Browsers use the root certificate to verify the Entrust signature on your server certificate. However, Netscape Navigator 3.x was shipped with a root certificate that expired in July, 1998, and Internet Explorer 3.0 browsers were shipped without the appropriate root certificate. As a result, users of these browsers who have not imported an updated root certificate are not able to connect to your secure Web site.

Users of these browsers have two choices:

Solution #1

Users can upgrade to Microsoft Internet Explorer 4.0 or higher or Netscape Navigator version 4.0 or higher. These more recent browsers contain a root certificate that will not expire until December 31, 2020. Downloading the setup files for these browsers may take several hours with some modems.

Solution #2

Users can import a new certificate. This new certificate will allow them to connect securely to your Web server. The process of importing the new certificate takes a few minutes. If you have Navigator 3.x users you may also have to update the root certificate in your Web server.

Because many users either have already updated the root certificate or upgraded their browsers, this issue may not affect you at all. Your Web server administrator should be able to tell you how many of your site visitors use Navigator 3.x or Internet Exporer 3.0. However, we recommend you follow the instructions for managing the root certificate rollover even if only a small proportion of your user base uses Navigator 3.x.

Note: The root certificate problem affects only Netscape Navigator 3.x and Internet Explorer 3.0. A new root certificate that expires in 2020 comes pre-installed in Navigator 4.x and IE 4.x. IE 3.0x (for example, IE 3.01 and 3.02) included the old root certificate but SSL was implemented in those browsers in such a way that the user does not see an error when connecting to a secure Web site.

1.1.1 When will other root certificates expire?

Because every Certification Authority limits the validity period of its root certificate, all CAs are affected by root certificate expiration. For example, the Verisign Inc. root certificate installed in every version of Netscape Navigator up to 4.05 will expire at midnight, December 31, 1999. This means that on January 1, 2000, People with any version of Netscape Navigator lower than 4.06 who visit a Web site secured with a Verisign certificate will see a “Certificate Authority is Expired Message”.

The Verisign root certificate in Internet Explorer 3.x will also expire at midnight December 31, 1999. However, because of the way IE 3.x implemented SSL, users will not see an error.

1.1.2 Why did the root certificate expire?

It was generated with a short lifespan to ensure maximum security. Since that time however, it has become clear that root certificates with a much longer lifespan are equally secure. Most public Certification Authorities are now using roots that are valid for about 20 years. Fortunately we are not the only ones who installed “short-term” root certificates into Web browsers. For example, the Verisign Inc. root certificate included in Netscape Navigator 4.05 or lower expires at midnight, December 31, 1999.

1.1.3 Which browsers are affected?

Only Netscape Navigator 3.x and Internet Explorer 3.0 are affected by this problem. A new root certificate which expires in 2020 comes pre-installed in Navigator 4.x and IE 4.x. IE 3.0x included the old root certificate but SSL was implemented in those browsers in such a way that the user does not see an error when connecting to a Web site protected with an Entrust certificate.

ROOT CERTIFICATES

1.2 MANAGING ROOT CERTIFICATE EXPIRY

If people visit your secure Web site with Netscape Navigator 3.x or Internet Explorer 3.0 we recommend that you follow the steps in this section to ensure that they can connect smoothly. For general information about the root certificate expiry problem, see Root certificate rollover.

Follow these steps to provide a smooth transition for users:

If you are using Internet Information Server 3.0 or 4.0, make sure you have imported the new root certificate. These Web servers were shipped with the old root certificate. See Installing root certificates in your Web server for details and instructions.

Provide a simple way for users to update the root certificates in their browsers. For your convenience, Entrust has developed a pair of CGI programs that you can use for this purpose. If you implement these CGI programs as recommended, users will only have to perform the root certificate update a single time. The first program ("bcheck.cgi") detects the type of browser that a user is running. You might want to place a link to it on the page where people switch into secure mode. If the browser is not Netscape Navigator 3.x or Microsoft Internet Explorer 3.0, the user is passed through to a URL you define. Otherwise, the user is passed to the second Entrust-supplied CGI program ("upgrade.pl"). This Perl script checks for a cookie that is set when the user updates the root certificate. If the cookie has been set the user is passed through to a URL you define. If the cookie has not been set the user can be passed to a page on the Entrust Web site that contains instructions on how to update the root certificate. Once the user has updated the root certificate this one time the cookie is set. The user will not be asked to perform the root certificate update the next time he or she visits your Web site. Please see the comments in the CGI scripts for detailed instructions. If you choose not to use the Entrust CGI program, you can provide your users with the instructions in Importing a root certificate into your Web browser.

That's all there is to it. If you follow these steps users who have upgraded their browsers or imported the new root certificate will be able to connect smoothly to your secure Web site.
If you are having difficulty finding what you're looking for, please e-mail us.

ROOT CERTIFICATES

1.3 INSTALLING ROOT CERTIFICATES IN YOUR WEB SERVER

Microsoft Internet Information Server 3.0 and 4.0 shipped with an old root (or CA) certificate which expired in July 1998. As a result, users of Navigator 3.x who have updated their root certificate will get a “database error” message when they attempt to connect to one of these servers. To resolve the problem you will need to update the root certificate in your server database. Follow the instructions below that apply to you.

1.3.1 How to install a new root certificate in IIS 4.0

You install the certificate using a utility named IISCA. Follow these steps:

1. Ensure that the Microsoft Authenticode package is installed on the computer that hosts the Web server. Authenticode is available at http://msdn.microsoft.com/downloads/tools/authcodeie4/authcodeie4.asp.

2. Ensure that you have a copy of the new Thawte CA certificate in binary format. Right click this link to the Thawte CA certificate and choose Save Target As... (in Microsoft Internet Explorer) or choose Save Link As... (in Netscape Navigator).

3. Run the Registry Editor and open the following key:

localMachine\System\CurrentControlSet\
Control\SecurityProviders\SCHANNEL\
CertificationAuthorities\ThawteServerCA

4. Right click the “Enabled” icon and select “Modify”. Change the '1' to a '0' to disable the root.

5. Exit the Registry Editor.

6. Open a command prompt in the “bin” folder of the Internet Client SDK and run the following commands:

certmgr -add serverbasic.crt -s -r localMachine \System\CurrentControlSet\
Control\SecurityProviders\
SCHANNEL\CertificationAuthorities
certmgr -add serverbasic.crt -s -r currentUser \Software\Microsoft\SystemCertificates\Root

7. Now run the IISCA utility by entering IISCA at a command prompt. This utility is normally installed in <WinDir>\System32\InetSrv.

You have just installed a new trusted Certification Authority. Test out IIS by connecting to your secure port using a copy of Navigator 3.0 in which the new root certificate has been installed.

1.3.2 How to install a new root certificate in IIS 3.0

You install the certificate using a utility named IISCA. Follow these steps:

1. Ensure that the Microsoft Authenticode package is installed on the computer that hosts the Web server. Authenticode is available at http://msdn.microsoft.com/downloads/tools/authcodeie4/authcodeie4.asp.

2. Ensure that you have a copy of the new Thawte CA certificate in binary format. Right click this link to the Thawte CA certificate and choose Save Target As... (in Microsoft Internet Explorer) or choose Save Link As... (in Netscape Navigator).

3. Run the Registry Editor and open the following key:

localMachine\System\CurrentControlSet\
Control\SecurityProviders\SCHANNEL\
CertificationAuthorities\ThawteServerCA

4. Right click the “Enabled” icon and select “Modify”. Change the '1' to a '0' to disable the root.

5. Exit the Registry Editor.

6. Open a command prompt in the “bin” folder of the Internet Client SDK and run the following commands:

certmgr -add serverbasic.crt -s -r localMachine \System\CurrentControlSet\
Control\SecurityProviders
\SCHANNEL\CertificationAuthorities
certmgr -add serverbasic.crt -s -r localMachine \System\Microsoft\
Cryptography\CertificateStore

7. Now run the IISCA utility by entering IISCA at a command prompt. This utility is normally installed in <WinDir>\System32\InetSrv.

You have just installed a new trusted Certification Authority certificate. Test out IIS by connecting to your secure port using a copy of Navigator 3.0 in which the new root certificate has been installed.