Entrust.Net

Technical Information – Installing Certificates

Client Confidential

TABLE OF CONTENTS

1. APPACHE (MOD_SSL)

1.1 INSTALLING CERTIFICATES IN APACHE USING SSLEAY

If your certificate request was successful you received an email from Entrust.net that contains a link to a certificate retrieval page on the Entrust Web site. This page contains at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appears here). The chain certificate contains the Entrust Root CA public key and it is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation Overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
2. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
3. Enable SSL in your Web server as described in your server's documentation.

That completes the certificate installation process. Users are able to connect to your Entrust-secured Web site.

How to install the Entrust chain certificate

You install the Entrust chain certificate in three main steps:

- Save the certificate in the directory identified by the SSLCACertificatePath entry (in “httpd.conf”).
- Calculate a hash value for the certificate.
- Create a symbolic link to the certificate file using the hash value as the link name.

The steps below assume that SSLCACertificatePath is set to <SSLTOP>/CA in your <httpd.conf> file. If you are using a different path, please substitute the correct path where appropriate.

1. Ensure that you have saved the chain certificate as a text file. See How to save your certificates in a file for instructions.

2. Copy the certificate file to the directory <SSLTOP>/CA/. For example: cp /tmp/entrustchaincert.txt &lt;SSLTOP&gt;/CA/entrustchaincert.pem

3. Change your current directory to the CA directory (<SSLTOP>/CA/).

4. Calculate a hash of the certificate file using the x509 utility that comes with SSLeay. For example: ssleay x509 -hash -noout /FONT>
   The hash value is displayed (for example, &quot;4b24ae9b&quot;).

5. Create a symbolic link to the certificate file (for example, entrustchaincert.pem). The name of the link will be the hash value you just calculated with a &quot;.0&quot; extension as shown below.
   ln -s entrustchaincert.pem &lt;hash_value&gt;.0

6. Delete the chain certificate file you created in Step 1 (for example, rm /tmp/entrustchaincert.txt).

7. Stop and then restart your server.

You have just installed the Entrust chain certificate.

How to install your Entrust.net Web server certificate

1. Ensure that you have saved your Entrust.net Web server certificate as a text file. See How to save your certificates in a file for instructions.

2. Copy the certificate into the <SSLTOP>/certs/ directory. For example: mv /tmp/entrustsitecert.txt <SSLTOP>/certs/
   Where: SSLTOP is your SSL root folder.

3. Ensure that the SSLCertificateFile directive (in httpd.conf) points to the Entrust.net Web server certificate file.

4. Copy the key file that corresponds to your Entrust.net Web server certificate into the <SSLTOP>/private/ directory.

5. Ensure that the SSLCertificateKeyFile directive (in httpd.conf) points to the key file.

6. Stop and restart your Web server.

You have just installed your Entrust.net Web server certificate.

How to save your certificates in a file

1. Open a text editor. You will save your certificates using this text editor.

2. Open a Web browser and go to the URL that appears in the confirmation email you received from Entrust.

3. Your certificates are displayed. The Entrust.net Web server certificate is in the section named “Entrust.net Web server certificate” and the chain certificate is in the section named “Entrust chain certificate”. The certificate will look similar to the following example:

```
-----BEGIN CERTIFICATE-----
MIISDOIUlkmlsRRlkSlIWLISdsSKJlalOSISLKjwBg
NVBAgAALOJdlwjam4gQ2FwZTESMBAGA1UEBxMJQ2Fw
ZSBUb3duMRQwEgYDVQQKEwHLOWDvcnR1bml0aTEYMB
YGKi2UECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQ
DExF3d3cuZm9yd2FyZC5jby56YTBaMA0GCSqGSIb3D
QEHHKJWAAklmLKSuljSOIjsfBWu5WLHD/G4BJ+Pobi
C9d7S6pDvAjuyC+dPAnL0d91tXdm2j190D1kgDoSp5
ZyGSgwJh2V7diuuPlHDAgEDoAAwDQYJVVjkksohvcN
AQEEBQADQQBf8LSLKknlsklSSLlworrr334ZmXD1Av
```

```
UjuDPCWzFupRIlliq7UR8Z0wiJUUsllkfq/IuuIlz6B
oq6htdJklil/wdhh
-----END CERTIFICATE-----
```

4. Copy the Entrust chain certificate to your clipboard. Remember to include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

5. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

6. Save the certificate as a file (for example, “/tmp/entrustchaincert.txt”).

7. Copy the Entrust.net Web server certificate to your clipboard. Remember to include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

8. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

9. Save the certificate as a file (for example, “/tmp/entrustsitecert.txt”).
   Note: If you have received more than one certificate you will have to perform the previous two steps for each certificate using unique filenames.

10. Close your text editor.

11. Make backup copies of both the Entrust.net Web server certificate and the Entrust chain certificate and store them in a secure location.

If you are having difficulty finding what you're looking for, please e-mail us.

APPACHE – SSL

1.2 INSTALLING CERTIFICATES IN APACHE USING SSLEAY

If your certificate request was successful you received an email from Entrust.net that contains a link to a certificate retrieval page on the Entrust Web site. This page contains at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appear here). The chain certificate contains the Entrust Root CA public key and is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
2. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
3. Enable SSL in your Web server as described in your Web servers documentation.

That completes the certificate installation process. Users are now able to connect to your Entrust-secured Web site.

How to install the Entrust chain certificate

You install the Entrust chain certificate in three main steps:

- Save the certificate in the directory identified by the SSLCACertificatePath entry (in “httpd.conf”)
- Calculate a hash value for the certificate
- Create a symbolic link to the certificate file using the hash value as the link name.

The steps below assume that SSLCACertificatePath is
set to <SSLTOP>/CA in your “httpd.conf” file. If you are using a different path, please substitute the correct path where appropriate.

1. Ensure that you have saved the chain certificate as a text file. See How to save your certificates in a file for instructions.

2. Copy the certificate file to the directory &lt;SSLTOP&gt;/CA/. For example: cp /tmp/entrustchaincert.txt &lt;SSLTOP&gt;/CA/entrustchaincert.pem

3. Change to the CA directory (&lt;SSLTOP&gt;/CA/).

4. Calculate a hash of the certificate file using the x509 utility that comes with SSLeay. For example: ssleay x509 -hash -noout /FONT>
   The hash value is displayed (for example, &quot;4b24ae9b&quot;).

5. Create a symbolic link to the certificate file (for example, entrustchaincert.pem). The name of the link is the hash value you just calculated with a &quot;.0&quot; extension as shown below.

```
ln -s entrustchaincert.pem &lt;hash_value&gt;.0
```

6. Delete the chain certificate file you created in Step 1 of this procedure (for example, rm /tmp/entrustchaincert.txt).

7. Stop and then restart your server.

You have just installed the Entrust chain certificate.

How to install your Entrust.net Web server certificate

1. Ensure that you have saved your Entrust.net Web server certificate as a text file. See How to save your certificates in a file for instructions.

2. Copy the certificate into the <SSLTOP>/certs/ directory. For example:
   mv /tmp/entrustsitecert.txt <SSLTOP>/certs/
   Where: SSLTOP is your SSL root folder.

3. Ensure that the SSLCertificateFile directive (in httpd.conf) points to the Entrust.net Web server certificate file.

4. Copy the key file that corresponds to your Entrust.net Web server certificate into the <SSLTOP>/private/ directory.

5. Ensure that the SSLCertificateKeyFile directive (in httpd.conf) points to the key file.

6. Stop and restart your Web server.

You have just installed your Entrust.net Web server certificate.

How to save your certificates in a file

1. Open a text editor. You will save your certificates using this text editor.

2. Open a Web browser and go to the URL that appears in the confirmation email you received from Entrust.

3. Your certificates are displayed. The Entrust.net Web server certificate is in the section named “Entrust.net Web server certificate” and the chain certificate is in the section named “Entrust chain certificate”. The certificates look similar to this example:

```
-----BEGIN CERTIFICATE-----
MIISDOIUlkmlsRRlkSllWLISdsSKJlalOSISLKjwBg
NVBAgAALOJdlwjam4gQ2FwZTESMBAGA1UEBxMJQ2Fw
ZSBUb3duMRQwEgYDVQQKEwHLOWDvcnR1bml0aTEYMB
YGKi2UECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQ
DExF3d3cuZm9yd2FyZC5jby56YTBaMA0GCSqGSIb3D
QEHHKJWAAklmLKSuljSOIjsfBWu5WLHD/G4BJ+Pobi
C9d7S6pDvAjuyC+dPAnL0d91tXdm2j190D1kgDoSp5
ZyGSgwJh2V7diuuPlHDAgEDoAAwDQYJVVjkksohvcN
AQEEBQADQQBf8LSLKknlsklSSLlworrr334ZmXD1Av
UjuDPCWzFupRIlliq7UR8Z0wiJUUsllkfq/IuuIlz6B
oq6htdJklil/wdhh
-----END CERTIFICATE-----
```

4. Copy the Entrust chain certificate to your clipboard. Remember to include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

5. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

6. Save the certificate as a file (for example, “/tmp/entrustchaincert.txt”).

7. Copy the Entrust.net Web server certificate to your clipboard. Remember to include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

8. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

9. Save the certificate as a file (for example, “/tmp/entrustsitecert.txt”).
   Note: If you have received more than one certificate you must perform the previous two steps for each certificate using unique filenames.

10. Close your text editor.

11. Make backup copies of both the Entrust.net Web server certificate and the Entrust chain certificate and store them in a secure location.

If you are having difficulty finding what you are looking for, please e-mail us.

O’REILLY WEBSITE PROFESSIONAL 2.X

1.3 INSTALLING CERTIFICATES IN O'REILLY WEBSITE PROFESSIONAL 2.X

If your certificate request was successful you received an email from Entrust.net that contains a link to your certificates on the Entrust Web site. This page contains at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appears here). The chain certificate contains the Entrust Root CA public key which is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Verify that the Thawte Server CA root certificate is installed in your server's Trusted Roots store, as described in Locating the Thawte Server CA root certificate.
2. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
3. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
4. Enable SSL in your Web server as described in your Web server documentation.

That completes the certificate installation process. Users are now able to connect to your Entrust-secured Web site.

Locating the Thawte Server CA root certificate

1. Open the WebSite Server Properties window (in Microsoft Windows NT, right-click the WebSite Pro icon in the Windows system tray and select "WebSite server properties").

2. From the WebSite Server Properties application, select the Key Ring tab.

3. Check the Trusted Roots box.

4. Look for Thawte Server CA in the certificate list.

5. If there is no entry for Thawte Server CA, you must add it to the Key Ring. Obtain the certificate from http://www.entrust.net/support/serverbasic.txt and install it following the instructions given in How to install the Entrust chain certificate. If it is in the list, proceed directly to the next set of instructions.

How to install the Entrust chain certificate

1. Save the chain certificate as a text file. See How to save your certificates in a file for instructions.

2. Open the WebSite Server Properties window (in Microsoft Windows NT, right-click the WebSite Pro icon in the Windows system tray and select “WebSite server properties” from the pop-up menu).

3. Click the Key Ring tab.

4. Check the Trusted roots box.

5. Click Add Trusted Root.... The Find dialog box appears.

6. Select the file that contains the Entrust chain certificate (for example, c:\certificates\entrustchaincert.crt).

7. Click Open. The Entrust chain certificate appears in the list of trusted roots with the name Entrust.net Secure Server Certification Authority.

8. Click the OK button to close the WebSite Server Properties window.

You have just installed the Entrust chain certificate in your registry. The chain certificate has the name “Entrust.net” Secure Server Certification Authority. Now you can install your Entrust.net Web server certificate(s).

How to install your Entrust.net Web server certificate

To install your Entrust.net Web server certificate, attach it to the key pair you generated when you created your CSR. Follow these steps:

1. Save your Entrust.net Web server certificate as a text file. See How to save your certificates in a file for instructions.

2. Open the WebSite Server Properties window (in Microsoft Windows NT, right-click the WebSite Pro icon in the Windows system tray and select “WebSite server properties” from the pop-up menu).

3. Click the Key Ring tab.

4. Right-click the key pair you created when you generated your CSR and select Attach Certificate.... The Find dialog box appears.

5. Select the file that contains your Entrust.net Web server certificate. Note: If you did not save the file with a .pem extension, select All files in the “Save as type” field.

6. Click the Open button.

You have just installed your Entrust.net Web server certificate. Now follow the instructions in your Web server's documentation to enable SSL.
Note: If you purchased more than one Entrust.net certificate, repeat the above steps for each additional certificate before enabling SSL.

How to save your certificates in a file

1. Open a text editor. You will save your certificates using this text editor.

2. Open a Web browser and go to the URL that appears in the confirmation email you received from Entrust. Your certificates are displayed. The Entrust.net Web server certificate is in the section named “Entrust.net Web server certificate” and the chain certificate is in the section named “Entrust chain certificate”. The certificates look like this example:

```
-----BEGIN CERTIFICATE-----
MIISDOIUlkmlsRRlkSllWLISdsSKJlalOSISLKjwBgNV
BAgAALOJdlwjam4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwHLOWDvcnR1bml0aTEYMBYGKi2U
ECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3c
uZm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEHHKJWAAk
lmLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAju
yC+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diu
uPlHDAgEDoAAwDQYJVVjkksohvcNAQEEBQADQQBf8LSL
KknlsklSSLlworrr334ZmXD1AvUjuDPCWzFupRIlliq7
UR8Z0wiJUUsllkfq/IuuIlz6oq6htdJklil/wdhh
-----END CERTIFICATE-----
```

3. Copy the Entrust chain certificate to your clipboard. You must include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

4. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

5. Save the certificate as a file. If you are installing the certificate in a Microsoft Windows-based Web server the filename should have the extension .crt (for example,”entrustchaincert.crt”).

6. Copy the Entrust.net Web server certificate to your clipboard. Remember to include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

7. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

8. Save the certificate as a file. If you are installing the certificate in a Microsoft Windows-based Web server the filename should have the extension .crt (for example, “entrustservercert.crt”). **Note**: If you have received more than one certificate you must perform this step and the previous step once for each certificate.

9. Close your text editor.

If you are having difficulty finding what you are looking for, please e-mail us.

NETSCAPE ENTERPRISE SERVER 3.5X AND 3.6X

1.4 INSTALLING CERTIFICATES IN NETSCAPE ENTERPRISE SERVER 3.51

If your certificate request was successful you received an email from Entrust.net that contains a link to your certificates on the Entrust Web site. This page will contain at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them will appear here). The chain certificate contains the Entrust Root CA public key and is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
2. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
3. Enable SSL in your Web server as described in your server's documentation.

That completes the certificate installation process. Users are now able to connect to your Entrust-secured Web site.

How to install the Entrust chain certificate

You install the Entrust chain certificate in Netscape Enterprise Server as a “Trusted Certificate Authority” (CA). Follow these steps:

1. Save the chain certificate as a text file. See How to save your certificates in a file for instructions.

2. Log on to the Netscape administration server.

3. In the General Administration section click Keys &amp; Certificates.

4. Click Install Certificate. The Install a Server Certificate page appears.

5. Select Trusted Certificate Authority (CA).

6. Enter a name for the chain certificate in the Certificate Name field. Choose a name you can remember easily.

7. Select Message is in this file and enter the path and name of the text file you saved in Step 1 of this procedure (for example, C:\Enterprise\entrustchaincert.crt).

8. Click the OK button. The Add Server CA Certificate page appears.

9. Verify the information in the certificate and click Add Certificate. A confirmation dialog box appears.

10. Click the OK button in the first confirmation dialog box, then click the OK button in the second confirmation dialog box.

11. Stop and restart both the Web server that will use this certificate and the Admin server to ensure that your changes take effect. If you are using the Windows NT version of Netscape Enterprise Server, Entrust recommends that you do this by opening the Services control in the Windows Control Panel and stopping and restarting the Netscape Enterprise Server and Netscape Administration Server services.

Once you have installed the chain certificate you are ready to install your Entrust.net Web server certificate(s). Follow the steps in How to install your Entrust.net Web server certificate.

How to install your Entrust.net Web server certificate

1. Save your Entrust.net Web server certificate as a text file. See How to save your certificates in a file for instructions.

2. Log on to the Netscape Administration Server.

3. In the General Administration section click Keys &amp; Certificates.

4. Click Install Certificate. The Install a Server Certificate page appears.

5. Select This Server in the Certificate For section. You do not need to complete the Certificate Name field since you are requesting a certificate for this server.

6. From the Alias drop-down menu, select the key pair alias that you chose when you generated the CSR for your Entrust.net Web server certificate.

7. Click the OK button. The Add Server Certificate screen appears.

8. Verify the information in the certificate and then click Add Certificate. A confirmation dialog box appears.

9. Click the OK button in the first confirmation dialog box, then click the OK button in the second confirmation dialog box.

10. Stop and restart both the Web server that will use this certificate and the Admin server to ensure that your changes take effect. If you are using the Windows NT version of Netscape Enterprise Server, Entrust recommends that you do this by opening the Services control in the Windows Control Panel and stopping and restarting the Netscape Enterprise Server and Netscape Administration Server services.

Once you have installed the chain certificate and Entrust.net Web server certificate follow the instructions in your Web servers documentation to enable SSL.

How to save your certificates in a file

1. Open a text editor. You will save your certificates using this text editor.

2. Open a Web browser and go to the URL that appears in the confirmation email you received from Entrust. Your certificates are displayed. The Entrust.net Web server certificate is in the section named “Entrust.net Web server certificate” and the chain certificate is in the section named “Entrust chain certificate”. The certificates look similar to this example:

-----BEGIN CERTIFICATE-----
MIISDOIUlkmlsRRlkSlIWLISdsSKJlalOSISLKjwBgNVBAg
AALOJdlwjam4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR
QwEgYDVQQKEwHLOWDvcnR1bml0aTEYMBYGKi2UECxMPT25s
aW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cuZm9yd2FyZC5
jby56YTBaMA0GCSqGSIb3DQEHHKJWAAklmLKSuljSOIjsfB
Wu5WLHD/G4BJ+PobiC9d7S6pDvAjuyC+dPAnL0d91tXdm2j
190D1kgDoSp5ZyGSgwJh2V7diuuPlHDAgEDoAAwDQYJVVjk
ksohvcNAQEEBQADQQBf8LSLKknlsklSSLlworrr334ZmXD1
AvUjuDPCWzFupRIlliq7UR8Z0wiJUUsllkfq/IuuIlz6oq6
htdJklil/wdhh
-----END CERTIFICATE-----

3. Copy the Entrust chain certificate to your clipboard. You must include the "----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines.

4. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

5. Save the certificate as a file. If you are installing the certificate in a Microsoft Windows-based Web server the filename should have the extension .crt (for example, "entrustchaincert.crt").

6. Copy the Entrust.net Web server certificate to your clipboard. Remember to include the "----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines.

7. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

8. Save the certificate as a file. If you are installing the certificate in a Microsoft Windows-based Web server the filename should have the extension .crt (for example, "entrustservercert.crt"). Note: If you have received more than one certificate you must perform this step and the previous step once for each certificate.

9. Close your text editor.

If you are having difficulty finding what you're looking for, please e-mail us.

LOTUS DOMINO R5

1.5 INSTALLING CERTIFICATES IN A LOTUS DOMINO R5 WEB SERVER

If your certificate request was successful you received an email from Entrust.net that contains a link to your certificates on the Entrust Web site. This page contains at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appears here). The chain certificate contains the Entrust Root CA public key and is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Note: Before you begin the installation procedure, make backup copies of both your Entrust.net Web server certificate and the Entrust chain certificate, and store them in a secure location.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Install the Thawte Server CA trusted root certificate as described in How to install the Thawte server CA root certificate.
2. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
3. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
4. Enable Secure Sockets Layer (SSL) in your Web server as described in How to Enable SSL in your Web server.

That completes the certificate installation process. Users are now able to connect to your Entrust-secured Web site.

How to install the Thawte server CA root certificate

1. Open a Web browser and go to http://www.entrust.net/support/serverbasic.txt. This Web page contains the Thawte server CA trusted root certificate.

2. Copy the certificate to your clipboard. You must include the “----BEGIN CERTIFICATE----“ and “----END CERTIFICATE----“ lines.

3. Open the Server Certificate Administration application on your Domino Web server.

4. Select the 3. Install Trusted Root Certificate into Key Ring option.

5. Paste the Thawte root certificate into the appropriate text entry field.

6. Click the Merge Trusted Root Certificate into Key Ring button.

You have installed the Thawte server CA root certificate.

How to install the Entrust chain certificate

1. Open the confirmation email you received from Entrust.net.

2. Click on the link to the certificate retrieval page on the Entrust Web site.

3. Select the certificate in the Entrust chain certificate section. You must include the “----BEGIN CERTIFICATE----“ and “----END CERTIFICATE----“ lines, and copy it to the clipboard.

4. Open the Server Certificate Administration application on your Domino Web server.

5. Select the 3. Install Trusted Root Certificate into Key Ring option.

6. Select Clipboard in the Certificate Source section.

7. Paste the chain certificate in the Certificate from Clipboard field.

8. Click the Merge Trusted Root Certificate into Key Ring button.

You have installed the Entrust chain certificate.

How to install your Entrust.net Web server certificate

1. Open the confirmation email you received from Entrust.net.

2. Click on the link to the certificate retrieval page on the Entrust Web site.

3. Select the certificate in the Entrust.net Web server certificate section. You must include the “----BEGIN CERTIFICATE----“ and “----END CERTIFICATE----“ lines, and copy it to the clipboard.

4. Open the Server Certificate Administration application on your Domino Web server.

5. Select the 4. Install Certificate into Key Ring option.

6. Paste the Entrust.net Web server certificate into the appropriate text entry field.

7. Click the Merge Certificate into Key Ring button.

You have installed your Entrust.net Web server certificate.

How to Enable SSL in your Web server

1. Edit the current server document in the Domino Administrator.

2. Select the Port tab.

3. Type the absolute path name of the key ring file that the server uses in the SSL Key File field. For example, C:\Lotus\SSL\keyfile.kyr.

4. Enable the SSL Port Status field in the Web HTTP/HTTPS section.

5. Restart the Domino Web server.

MICROSOFT WINDOWS 2000 / INTERNET INFORMATION SERVER 5.0

1.6 INSTALLING CERTIFICATES IN MICROSOFT WINDOWS 2000 / INTERNET INFORMATION SERVER 5.0

If your certificate request was successful you received an email from Entrust.net that contains a link to your certificates on the Entrust Web site. This page contains at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appears here). The chain certificate contains the Entrust Root CA public key which is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
2. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
3. Enable SSL in your Web server as described in your Web server documentation.

That completes the certificate installation process. Users are now able to connect to your Entrust-secured Web site.

How to install the Entrust chain certificate

1. Create a new text file with the extension .CRT, instead of the usual .TXT extension. For example, MyServer.CRT.

2. Copy the Server certificate into the .CRT file and save it to your hard drive. Ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

3. Browse to the location where the file was saved and open it. The Microsoft Certificate Wizard appears.

4. Select the Install Certificate option. The Certificate Import Wizard appears.

5. Click the Next button to proceed.

6. Select Place all certificates into the following store and click the Browse button.

7. Select Show physical stores, expand Intermediate Certification Authorities and select Local Computer.

8. Click the Next button to proceed.

9. Click the Finish button to complete the installation. A message appears telling you that the install was successful.

You have just installed the Entrust chain certificate in your registry. The chain certificate has the name Entrust.net Secure Server Certification Authority. Now you can install your Entrust.net Web server certificate.

How to install your Entrust.net Web server certificate

1. Create a new text file with the extension .CRT, instead of the usual .TXT extension. For example, MyServer.CRT.

2. Copy the Server certificate into the .CRT file and save it to your hard drive. Ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

3. Open the Internet Information Service: Start > Programs > Administrative Tools > Internet Services Manager.

4. Right-click on your Default website and select the Properties option from the list.

5. Select the Directory Security tab.

6. Click the Server Certificate button in the Secure Communications section. The Web Server Certificate Wizard appears.

7. Click the Next button to proceed.

8. Select the Process the pending request and install the certificate option and click the Next button.

9. Browse to the location where you saved the Server Certificate.

10. Select the server certificate and click the Next button.

11. Click the Finish button.

12. Stop your Web server and restart it.

You have just installed your Entrust.net Web server certificate. Your server is ready to establish 128-bit encrypted sessions. You must now enable SSL in your Web server as described in your Web server documentation.

If you are having difficulty finding what you are looking for, please e-mail us.

MICROSOFT INTERNET INFORMATION SERVER 4.0

1.7 INSTALLING CERTIFICATES IN MICROSOFT INTERNET INFORMATION SERVER 4.0

If your certificate request was successful you received an email from Entrust.net that contains a link to your certificates on the Entrust Web site. This page will contain at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appears here). The chain certificate contains the Entrust Root CA public key and is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Ensure that you have installed Service Pack 4 for Windows NT on the computer that hosts your Web server. You will find Service Pack 4 at http://www.microsoft.com/windows/downloads/default.asp.
2. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
3. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
4. Enable SSL in your Web server as described in your server's documentation.

That completes the certificate installation process. Users are now able to connect to your Entrust-secured Web site.

How to install the Entrust chain certificate

You install the chain certificate using the Certificate Manager Import wizard included in Service Pack 4 for Windows NT. Please ensure that you have installed Service Pack 4 before you perform the steps below.

1. Save the chain certificate as a text file. See How to save your certificates in a file for instructions.

2. Open the file that contains the chain certificate in Windows Explorer (for example, double-click the file). The Certificate dialog box appears.

3. In the General tab Click Install Certificate.... The Certificate Manager Import Wizard appears.

4. Click Next and select Place all certificates into the following store.

5. Click Browse... The Select Certificate Store dialog box appears.

6. Select Show Physical Stores.

7. Expand Intermediate Certification Authority by clicking the “+” sign beside the item in the dialog box.

8. Select Local Computer and click the OK button.

9. Click Next.

10. Click Finish. A confirmation dialog appears.

11. Click the OK button.

12. Restart the computer to ensure that the registry settings take effect.

You have just installed the Entrust chain certificate in the correct location in your registry. The chain certificate has the name Entrust.net Secure Server Certification Authority. You may now install your Entrust.net Web server certificate.

How to install your Entrust.net Web server certificate

1. Save your Entrust.net Web server certificate as a text file. See How to save your certificates in a file for instructions.

2. Run the Internet Service Manager.

3. Select your Web site and click the Key Manager icon. The Key Manager appears.

4. Right-click the key that was created when you generated the CSR and select Install Key Certificate.... The Open dialog box appears.

5. Select the file that contains your Entrust.net Web server certificate and click Open. The Password dialog box appears.

6. Enter the password you chose when you created the key pair and click the OK button. The Server Bindings dialog appears.

7. Click the OK button unless you want to use this certificate with specific IP addresses and port numbers.

8. Now save your changes. To do this, click Computers &gt; Commit Changes Now, and then click the OK button in the confirmation dialog box.

9. Click the OK button.

That completes the certificate installation process. You have just installed your Entrust.net Web server certificate.

How to save your certificates in a file

1. Open a text editor. You will save your certificates using this text editor.

2. Open a Web browser and go to the URL that appears in the confirmation email you received from Entrust. Your certificates are displayed. The Entrust.net Web server certificate is in the section named “Entrust.net Web server certificate” and the chain certificate is in the section named “Entrust chain certificate”. The certificates look something like this:

```
-----BEGIN CERTIFICATE-----
MIISDOIUlkmlsRRlkSlIWLISdsSKJlalOSISLKjwBgNV
BAgAALOJdlwjam4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwHLOWDvcnR1bml0aTEYMBYGKi2U
ECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3c
uZm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEHHKJWAAk
lmLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAju
yC+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diu
uPlHDAgEDoAAwDQYJVVjkksohvcNAQEEBQADQQBf8LSL
KknlsklSSLlworrr334ZmXD1AvUjuDPCWzFupRIlliq7
UR8Z0wiJUUsllkfq/IuuIlz6oq6htdJklil/wdhh
-----END CERTIFICATE-----
```

3. Copy the Entrust chain certificate to your clipboard. You must include the "----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines.

4. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

5. Save the certificate as a file. If you are installing the certificate in a Microsoft Windows-based Web server the filename should have the extension .crt (for example, "entrustchaincert.crt").

6. Copy the Entrust.net Web server certificate to your clipboard. Remember to include the "----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines.

7. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

8. Save the certificate as a file. If you are installing the certificate in a Microsoft Windows-based Web server the filename should have the extension .crt (for example, "entrustservercert.crt"). Note: If you have received more than one certificate you will have to perform this and the previous step once for each certificate.

9. Close your text editor.

If you are having difficulty finding what you are looking for, please e-mail us.

MICROSOFT INTERNET INFORMATION SERVER 2.X AND 3.X

1.8 INSTALLING CERTIFICATES IN MICROSOFT INTERNET INFORMATION SERVER 2.X AND 3.X

If your certificate request was successful you received an email from Entrust.net that contains a link to your certificates on the Entrust Web site. This page contains at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appears here). The chain certificate contains the Entrust Root CA public key and is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Ensure that you have installed Service Pack 4 for Windows NT on the computer that hosts your Web server. You will find Service Pack 4 at http://www.microsoft.com/windows/downloads/default.asp.
2. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
3. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
4. Enable SSL in your Web server as described in your server's documentation.

That completes the certificate installation process. Users are now able to connect to your Entrust-secured Web site.

How to install the Entrust chain certificate

You install the chain certificate using the Certificate Manager Import wizard included in Service Pack 4 for Windows NT. Please ensure that you have installed Service Pack 4 before you perform the steps below.

1. Save the chain certificate as a text file. See How to save your certificates in a file for instructions.

2. Open the file that contains the chain certificate in Windows Explorer (for example, double-click the file). The Certificate dialog box appears.

3. In the General tab click Install Certificate... The Certificate Manager Import Wizard appears.

4. Click Next and select Place all certificates into the following store.

5. Click Browse... The Select Certificate Store dialog box appears.

6. Select Show Physical Stores.

7. Expand Intermediate Certification Authority by clicking the “+” sign beside the item in the dialog box.

8. Select Local Computer and click the OK button.

9. Click Next.

10. Click Finish. A confirmation dialog box appears.

11. Click the OK button.

12. Restart the computer to ensure that the registry settings take effect.

You have just installed the Entrust chain certificate in the correct location in your registry. The chain certificate has the name “Entrust.net” Secure Server Certification Authority. You may now install your Entrust.net Web server certificate.

How to install your Entrust.net Web server certificate

1. Save your Entrust.net Web server certificate as a text file. See How to save your certificates in a file for instructions.

2. Run the Internet Service Manager (click Start > Programs > Microsoft Internet Server > Internet Service Manager).

3. Select your Web site and click the Key Manager icon. The Key Manager appears.

4. Right-click the key that was created when you generated the CSR and select Install Key Certificate.... The Open dialog box appears.

5. Select the file that contains your Entrust.net Web server certificate and click Open. The Password dialog box appears.

6. Enter the password you chose when you created the key pair and click the OK button. The Server Connection dialog box appears.

7. Click the OK button unless you want to use this certificate with specific IP addresses and port numbers.

8. Now save your changes. To do this, click Servers > Commit Changes Now, and then click Yes in the confirmation dialog box.

You have just installed your Entrust.net Web server certificate.

How to save your certificates in a file

1. Open a text editor. You will save your certificates using this text editor.

2. Open a Web browser and go to the URL that appears in the confirmation email you received from Entrust. Your certificates are displayed. The Entrust.net Web server certificate is in the section named Entrust.net Web server certificate and the chain certificate is in the section named Entrust chain certificate. Each certificate begins with the line “----BEGIN CERTIFICATE-----“ and ends with “-----END CERTIFICATE-----“. The certificates look like the following example:

```
-----BEGIN CERTIFICATE-----
MIISDOIUlkmlsRRlkSlIWLISdsSKJlalOSISLKjwBgNV
BAgAALOJdlwjam4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwHLOWDvcnR1bml0aTEYMBYGKi2U
ECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3c
uZm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEHHKJWAAk
lmLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAju
yC+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diu
uPlHDAgEDoAAwDQYJVVjkksohvcNAQEEBQADQQBf8LSL
KknlsklSSLlworrr334ZmXD1AvUjuDPCWzFupRIlliq7
UR8Z0wiJUUsllkfq/IuuIlz6oq6htdJklil/wdhh
-----END CERTIFICATE-----
```

3. Copy the Entrust chain certificate to your clipboard. You must include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

4. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

5. Save the certificate as a file. If you are installing the certificate in a Microsoft Windows-based Web server the filename should have the extension “.crt” (for example, “entrustchaincert.crt”).

6. Copy the Entrust.net Web server certificate to your clipboard. Remember to include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

7. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

8. Save the certificate as a file. If you are installing the certificate in a Microsoft Windows-based Web server the filename should have the extension “.crt” (for example, “entrustservercert.crt”). Note: If you have received more than one certificate you will have to perform this and the previous step once for each certificate.

9. Close your text editor.

If you are having difficulty finding what you are looking for, please e-mail us.

C2NET STRONGHOLD

1.9 INSTALLING CERTIFICATES IN C2NET STRONGHOLD

If your certificate request was successful you received an email from Entrust.net that contains a link to a certificate retrieval page on the Entrust Web site. This page contains at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appears here). The chain certificate contains the Entrust Root CA public key and is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
2. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
3. Enable SSL in your Web server as described in your server's documentation.

That completes the certificate installation process. Users are now able to connect to your Entrust-secured Web site.

How to install the Entrust chain certificate

On startup, Stronghold loads certificates from the file specified by the SSLCACertificateFile entry in its “httpd.conf” file. To install the Entrust chain certificate, simply add it to this file. Follow these steps:

1. Ensure that you have saved the chain certificate as a text file. See How to save your certificates in a file for instructions.
2. Open your “httpd.conf” file and find the SSLCACertificateFile entry. The file specified by this entry contains the certificates that Stronghold loads on startup. You must add the Entrust chain certificate to this file. By default the entry will be SLCACertificateFile=”<server_root>/ssl/CA/client-rootcerts.pem”. You will find “httpd.conf” in the directory <server_root>/conf.
3. Open the file identified by SSLCACertificateFile (for example, <server_root>/ssl/CA/client-rootcerts.pem) in a text editor.
4. Open the file that contains the Entrust chain certificate in a text editor (by default this will be /tmp/entrustchaincert.txt).
5. Copy the chain certificate (including the “-----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines to the clipboard.
6. Paste the chain certificate into the file identified by SSLCACertificateFile. In most cases you will want to insert the chain certificate at the end of the file and add a comment to identify the certificate.
7. Save the modified file and close the text editor.
8. Delete the chain certificate file you created in Step 1 (for example, rm /tmp/entrustchaincert.txt).
9. Restart your server using <server_root>/bin/reload-server.

You have just installed the Entrust chain certificate.

How to install your Entrust.net Web server certificate

1. Ensure that you have saved your Entrust.net Web server certificate as a text file. See How to save your certificates in a file for instructions.

2. Install the new certificate using getca as shown below. This utility is normally installed in <server_root>/bin.

   getca myhostname < /tmp/entrustsitecert.txt

   Where: myhostname is the common name of the Web server for which the certificate was requested (for instance, “lion” if you requested a certificate for lion.entrust.com), and /tmp/entrustsitecert.txt is the name of the file you created in Step 1 of this procedure. This will save the certificate in the file <server_root>/ssl/certs/myhostname.cert.

3. Delete the Entrust.net Web server certificate file you created in Step 1 of this procedure (for example, rm /tmp/entrustsitecert.txt).

4. Restart your server using <server_root>/bin/reload-server.

You have just installed your Entrust.net Web server certificate.

How to save your certificates in a file

1. Open a text editor. You will save your certificates using this text editor.

2. Open a Web browser and go to the URL that appears in the confirmation email you received from Entrust. Your certificates are displayed. The Entrust.net Web server certificate is in the section named Entrust.net Web server certificate and the chain certificate is in the section named Entrust chain certificate. The certificates look like this example:

```
-----BEGIN CERTIFICATE-----
MIISDOIUlkmlsRRlkSlIWLISdsSKJlalOSISLKjwBgNV
BAgAALOJdlwjam4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwHLOWDvcnR1bml0aTEYMBYGKi2U
ECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3c
uZm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEHHKJWAAk
lmLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7SpDvAjuy
C+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diuu
PlHDAgEDoAAwDQYJVVjkksohvcNAQEEBQADQQBf8LSLK
knlsklSSLlworrr334ZmXD1AvUjuDPCWzFupRIlliq7U
R8Z0wiJUUsllkfq/IuuIlz6oq6htdJklil/wdhh
-----END CERTIFICATE-----
```

3. Copy the Entrust chain certificate to your clipboard. You must include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

4. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

5. Save the certificate as a file (for example, “/tmp/entrustchaincert.txt”).

6. Copy the Entrust.net Web server certificate to your clipboard. Remember to include the "----BEGIN CERTIFICATE---" and "----END CERTIFICATE----" lines.

7. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

8. Save the certificate as a file (for example, "/tmp/entrustsitecert.txt"). Note: If you have received more than one certificate you will have to perform this and the previous step once for each certificate using unique filenames.

9. Close your text editor.

10. Make backup copies of both the Entrust.net Web server certificate and the Entrust chain certificate and store them in a secure location.

If you are having difficulty finding what you are looking for, please e-mail us.

BEA WEBLOIC 4.5.X

1.10 BEA WEBLOGIC 4.5.X INSTALLATION INSTRUCTIONS

If your certificate request was successful you have received an email from Entrust.net that contains a link to your certificates on the Entrust Web site. This page contains at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appears here). The chain certificate contains the Entrust Root CA public key and is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Install the Entrust chain certificate and your Entrust.net Web server certificate as described in How to install certificates.
2. Enable Secure Sockets Layer (SSL) in your Web server as described in How to enable SSL in your Web server.

That completes the certificate installation process. Users are now able to connect to your Entrust-secured Web site.

How to install certificates

To install the chain certificate and the Entrust.net Web server certificate:

1. Copy the private key generated by your Web server just before you created your Certificate Signing request (CSR). The private key is stored in a file called www_mydomain_com-key.der. The file is located in the WebLogic Server root directory. The default root directory is called /myserver.
2. Save both your Entrust.net Web server certificate and the Entrust chain certificate as text files, but use .PEM as the file extension instead of the usual .TXT extension. For example, Webcert.PEM. See How to save your certificates in a file for instructions.
3. Copy both .PEM files to the WebLogic Server root directory. The default root directory is called /myserver.

You are ready to enable SSL in your Web server.

How to enable SSL in your Web server

1. Locate the weblogic.properties file on your Web server and open it.

2. Edit the file to reflect the following properties and corresponding values:

Parameter	Default value	Description/Action
weblogic.system.SSLListenPort	443	The port number for the SSL listener. The value cannot be zero.
weblogic.security.ssl.enable	True	This parameter enables SSL. SSL

		is disabled if the value is set to "False"
weblogic.security.key.server	-	This parameter specifies the name of your private key file. For example, www_mydomain_com-key.der.
weblogic.security.certificate.server	-	This parameter specifies the name of the .PEM file you created for the Web server certificate issued by Entrust.net. For example, Webcert.PEM.
weblogic.security.certificate.authority	-	This parameter specifies the name of .PEM file you created for the Entrust chain certificate. For example, Chaincert.PEM.

3. Restart WebLogic Server 4.5.x.

You have completed the certificate installation process. SSL with Server Authentication is now enabled on your server. Browsers accessing your site using https:// in the URL will establish a secure SSL session with your server.

How to save your certificates in a file

1. Open a text editor. You will save your certificates using this text editor.

2. Open a Web browser and go to the URL that appears in the confirmation email you received from Entrust. Your certificates are displayed.

   The Entrust.net Web server certificate is in the section named Entrust.net Web server certificate and the chain certificate is in the section named Entrust chain certificate. The certificates look similar to this sample:

```
-----BEGIN CERTIFICATE-----
MIISDOIUlkmlsRRlkSlIWLISdsSKJlalOSISLKjwBgNV
BAgAALOJdlwjam4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwHLOWDvcnR1bml0aTEYMBYGKi2U
ECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3c
uZm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEHHKJWAAk
lmLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAju
yC+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diu
uPlHDAgEDoAAwDQYJVVjkksohvcNAQEEBQADQQBf8LSL
KknlsklSSLlworrr334ZmXD1AvUjuDPCWzFupRIlliq7
UR8Z0wiJUUsllkfq/IuuIlz6oq6htdJklil/wdhh
-----END CERTIFICATE-----
```

3. Copy the Entrust chain certificate to your clipboard. You must include the “----BEGIN CERTIFICATE-----“ and “-----END CERTIFICATE-----“ lines.

4. Paste the certificate into the text editor and ensure that the entire text is flushed to the left with no leading or trailing whitespace. If there are any extra spaces the server will not recognize the format of the file and you will not be able to install the certificate.

5. Save the certificate as a file. For example, Entrustservercert.pem.

   Note: If you have received more than one certificate you will have to perform this step and the previous step for each certificate.

6. Close your text editor.

7. Make backup copies of both your Entrust.net Web server certificate and the Entrust chain certificate, and store them in a secure location.

If you are having difficulty finding what you are looking for, please e-mail us.

RAVEN SSL 1.4.1 MODULE FOR APACHE SUPPORT

1.11 INSTALLING CERTIFICATES IN RAVEN SSL 1.4.1 MODULE FOR APACHE SUPPORT

If your certificate request was successful you received an email from Entrust.net that contains a link to a certificate retrieval page on the Entrust Web site. This page will contain at least two certificates: the Entrust chain certificate and your Entrust.net Web server certificate (if you ordered more than one Entrust.net Web server certificate, each of them appears here). The chain certificate contains the Entrust Root CA public key and is signed by Thawte Consulting. Thawte is a Root CA in all major browsers. By installing the chain certificate in your Web server you create a chain of trust between end users and your Entrust.net Web server certificate.

Installation overview

You must install both the chain certificate and your Entrust.net Web server certificate to provide secure access to your Web server. Follow these steps:

1. Install your Entrust.net Web server certificate as described in How to install your Entrust.net Web server certificate.
2. Install the Entrust chain certificate as described in How to install the Entrust chain certificate.
3. Enable SSL in your WebServer as described in How to configure the Apache run-time configuration file.
4. Follow the instructions to restart the Apache WebServer with Raven SSL.

That completes the installation process. Users will now be able to connect to your Entrust-secured Web site.

How to install the Entrust.net WebServer Certificate:

1. Copy the signed certificate issued by Entrust.net, and save it to a file. Be sure to include the “-----BEGIN CERTIFICATE REQUEST-----“ and “-----END CERTIFICATE REQUEST-----“ lines, and everything in between.

2. From the RavenCTL PKI Management Interface, select [2] Install Signed Certificate.

3. At the prompt, enter the absolute path to the file created above. Raven will copy the file to the [install-prefix]/raven/module/pki/certs directory, and append a .cert extension during the installation process.

How to install the Entrust chain certificate

1. Locate and open the ca-bundle.cert file in the [install-prefix]/raven/module/pki/certs directory.

2. Copy the entire Entrust chain certificate, including the “-----BEGIN CERTIFICATE -----“ and “-----END CERTIFICATE -----“ lines, and everything in between.

3. Paste the Entrust chain certificate into the ca-bundle.cert file. It can be entered at the beginning or end of the file, or between existing entries. There is no need to add any other data to match the format of existing entries.

4. Save and close the ca-bundle.cert file.

How to configure the Apache run-time configuration file

1. Locate and open the httpsd.conf file in the Apache web server's [serverroot]/conf directory. The [serverroot] specifies the path to the server's root directory. This is typically /usr/local/apache.

2. Edit this file to point the Raven SSL module to the new web server certificate and associated key, and the Entrust chain certificate.

3. Within the section defined for the virtual host listening on the chosen SSL port, edit (or add if necessary), the following properties:

SSLEngine - Set to “on” to enable SSL for this virtual host.

SSLCertificateFile - Set to the absolute path of the installed Entrust web server certificate. This is typically [install-prefix]/raven/module/pki/certs/www.mydomain.com.cert.

SSLCertificateKeyFile - Set to the absolute path of the key file generated in Step 5 of Generating a Certificate and Key. This is typically [install-prefix]/raven/module/pki/keys/www.mydomain.com.key.

SSLCACertificateFile - Set to the absolute path of the ca-bundle.cert file editied when you installed the Entrust Chain Certificate. This is typically [install-prefix]/raven/module/pki/certs/ca-bundle.cert

4. Save and close the httpsd.conf file.

How to restart the Apache Web Server with Raven SSL

1. Stop the Apache web server.
2. Restart the Apache web server using by entering httpsdctl startssl. You will have to include the absolute path to httpsdctl if your PATH is not set correctly.
3. Enter the pass phrase you used in Step 3 of Generating and Submitting the CSR.

SSL with Server Auth has now been enabled on your server. Browsers accessing your site with https:// in the url (note the 's' after http) will enter a Secure SSL session with your server.

If you are having difficulty finding what you are looking for, please e-mail us.