



Entrust® Certificates Update

For FedLine® access solutions

The process to update your Entrust Certificates is quick, easy and should have minimal impact on your institution. **For customers using non-Windows® operating systems please follow your vendor's operating instructions for performing the update.**

Getting Started

Please read the following before proceeding with the required Entrust Certificate update:

- You will install two Entrust Certificates during this process: (1) Root Certificate "**Entrust CA (2048)**" and (2) Root Certificate "**Entrust Root CA – G2**".

You may need administrator-level access to your institution's computer(s) to perform this update.

- Do not remove any existing Entrust Certificates.
- There are three sections in this guide. If you are working on a computer that is connected to the Internet, you will need to complete Section 1 in addition to Section 3. If you are working on a computer that is **not** connected to the Internet, you will need to complete Section 2 in addition to Section 3.
 - Section 1: Update Your Entrust Certificates – with an Internet-connected computer
 - Section 2: Update Your Entrust Certificates – with a **non** Internet-connected computer
 - Section 3: Verify Your Current Entrust Certificates

Questions

If you have any questions about this guide or the update process, please contact the Customer Contact Center at **(888) 333-7010**, and select **Option 1** for technical support.

Section 1: Update Your Entrust Certificates – with an Internet-connected computer

1. Open an Internet Explorer® browser and visit the Entrust SSL Certificates Web page at <http://www.entrust.net/developer/index.cfm> (Off-site Link)

2. On the Entrust SSL Certificates Web page, click “Download Root Certificates”

Root Certificates

Entrust has four public roots that are available for download. The following table explains the different applications of each Entrust CA. To obtain any of these root certificates click the “Download” button below the following table.

Certification Authority	Extended Validation (EV)	Server Auth	Client Auth	Secure Email	Code Signing	Certificate Thumbprint (SHA-1)
Entrust Secure Server CA *Trust Uses	✓	✓	✓	✓	✓	99A6 9BE6 1AFE886B 4D2B 82007CB8 54FC 317E1539
Entrust Root CA *Trust Uses	✓	✓	✓	✓	✓	B31E B1B7 40E36C84 02DA DC37D44D F5D4 674952F9
Entrust CA (2048) *Trust Uses	✓	✓	✓	✓	✓	5030 0609 1D97 D4F5 AE39 F7CB E792 7D7D 652D 3431
Entrust Root CA - G2 *Trust Uses	✓	✓	✓	✓	✓	8CF4 27FD 790C 3AD1 6606 8DE8 1E57 EFBB 9322 72D4

[Download Root Certificates](#)

3. On the Entrust SSL Certificates download page, select “Personal Use” and click “Download Certificates”

Entrust SSL Certificates

Securing Your Online Business

[Products](#) [Buy](#) [Customer Service](#) [Support](#) [Resources](#) [Affiliates](#) [Customers](#) [About Entrust](#)

Resources

[White Papers](#)
[Enrollment Guides](#)
[Technical Requirements](#)
[Legal Agreements](#)
[Root Certificates](#)

Download

Please identify the reason for downloading the Entrust Root Certificate:

- Personal Use
 Embedding within an application

[Download Certificates](#)

4. On the following Web page, ensure that the “Root Certificates” tab is selected.

Download the second Root Certificate listed, “**Entrust CA (2048)**”, by clicking on the File Download link “**entrust_2048_ca.cer**”

Root Certificates | EV Chain Certificates | Non-EV Chain Certificates

Entrust Secure Server CA
File Download:
entrust_ssl_ca.cer
entrust_ssl_ca.der
Thumbprint: 99A6 9BE6 1AFE 886B 4D2B 8200 7CB8 54FC 317E 1539
Base 64 Format:
-----BEGIN CERTIFICATE-----
MIIE2DCCBEGgAwIBAgIEN0rSQzANBgkqhkiG9w0BAQUFADCBwzELMAk
GA1UE
BhMCMCVVMxFDASBgNVBAoTC0VudHJ1c3QubmV0MTswOQYDVQQLZzJ3d
3cuZW50
cnVzdC5uZXQvQ1BTIGluY29ycC4gYnkgcml0eTAeFw05OTA1MjUxNjM5
NDBBaMIH
dGhvcmI0eTAeFw05OTA1MjUxNjM5NDBBaMIHDMQsw
COYDVC...


Entrust CA (2048)
File Download: entrust_2048_ca.cer
Thumbprint: 5030 0609 1D97 D4F5 AE39 F7CB E792 7D7D 652D 3431
Base 64 Format:
-----BEGIN CERTIFICATE-----
MIIEKjCCAxKgAwIBAgIEOGPe+DANBgkqhkiG9w0BAQUFADCBtDEUMBIG
A1UEChMLRW50cnVzdC5u


5. In the dialogue box that appears, click “Open”



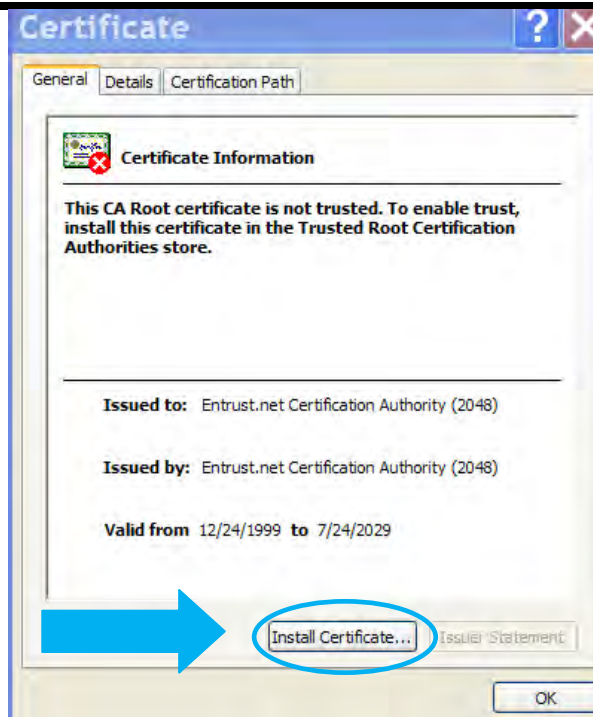
File Download - Security Warning

Do you want to open or save this file?

 Name: entrust_2048_ca.cer
Type: Security Certificate, 1.48KB
From: www.entrust.net

 While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. [What's the risk?](#)

6. In the *Certificate* menu, click **“Install Certificate...”**



7. In the Certificate Import Wizard *Welcome* Screen, click **“Next >”**

8. In the Certificate Import Wizard *Certificate Store* Screen, select **“Automatically select the certificate store based on the type of certificate”** and click **“Next >”**



9. In the Certificate Import Wizard *Completing the Certificate Import* Screen, click **“Finish”**

10. Once you are prompted with the following screen notifying you that the import was successful, click **“OK”**



11. After you have clicked "OK" your browser should remain on the Entrust certificate download site. You will now download the second certificate.

Scroll to the bottom of the Entrust page and download the last Root Certificate listed, "Entrust Root CA – G2", by clicking on the File Download link "[entrust_g2_ca.cer](#)"

Entrust Root CA - G2

File Download:

[entrust_g2_ca.cer](#)

Thumbprint: 8CF4 27FD 790C 3AD1 6606 8DE8 1E57 EFBB 9322 72D4

Base 64 Format:

```
-----BEGIN CERTIFICATE-----
MIIEPjCCAyagAwIBAgIIESIOMKDANBgkqhkiG9w0BAQsFADCbvjELMAkGA1
UEBhMC
VVMxJFAUBGNVBAoTUDUvudHJ1c3QsIEluYy4xKDAmBgNVBAsTH1NIZSB3
d3cuZW50
cnVzdC5uZXQvbGVnYWwtdGVybXMxOTA3BgNVBAsTMChjKSAyMDA5IEVv
dHJ1c3Qs
IEluYy4gLSBmb3IgaXV0aG9yaXpIZCB1c2Ugb25seTEyMDA5IEVv
W50cnVz
dCBSb290IENicnRpZmlyYXRpb24gQXV0aG9yaXR5IC0gRzlwHhcNMDkwN
zA3MTcy
NTU0WWhcNMzAxMjA3Mjc1NTU0WjCBvjELMAkGA1UEBhMCVVMxJFAUBGN
VBAoTUDUv
dHJ1c3QsIEluYy4xKDAmBgNVBAsTH1NIZSB3d3cuZW50cnVzdC5uZXQvb
```



12. Follow steps 5 – 10 above to complete the second Root Certificate download

You have now downloaded both Root Certificates. Please move on to Section 3 to verify your current Entrust Certificates.

Section 2: Update Your Entrust Certificates – with a non Internet-connected computer

1. Access an Internet-connected computer. Open an Internet Explorer browser and visit the Entrust SSL Certificates Web page at <http://www.entrust.net/developer/index.cfm> (Off-site Link)

2. On the Entrust SSL Certificates Web page, click “Download Root Certificates”

Root Certificates

Entrust has four public roots that are available for download. The following table explains the different applications of each Entrust CA. To obtain any of these root certificates click the “Download” button below the following table.

Certification Authority	Extended Validation (EV)	Server Auth	Client Auth	Secure Email	Code Signing	Certificate Thumbprint (SHA-1)
Entrust Secure Server CA *Trust Uses	✓	✓	✓	✓	✓	99A6 9BE6 1AFE886B 4D2B 82007CB8 54FC 317E1539
Entrust Root CA *Trust Uses	✓	✓	✓	✓	✓	B31E B1B7 40E36C84 02DA DC37D44D F5D4 674952F9
Entrust CA (2048) *Trust Uses	✓	✓	✓	✓	✓	5030 0609 1D97 D4F5 AE39 F7CB E792 7D7D 652D 3431
Entrust Root CA - G2 *Trust Uses	✓	✓	✓	✓	✓	8CF4 27FD 790C 3AD1 6606 8DE8 1E57 EFBB 9322 72D4

[Download Root Certificates](#)

3. On the Entrust SSL Certificates download page, select “Personal Use” and click “Download Certificates”

Entrust SSL Certificates

Securing Your Online Business

Products Buy Customer Service Support Resources Affiliates Customers About Entrust

Resources

- White Papers
- Enrollment Guides
- Technical Requirements
- Legal Agreements
- Root Certificates

Download

Please identify the reason for downloading the Entrust Root Certificate:

Personal Use

Embedding within an application

[Download Certificates](#)

4. On the following Web page, ensure that the “Root Certificates” tab is selected.

Download the second Root Certificate listed, “Entrust CA (2048)”, by clicking on the File Download link “[entrust_2048_ca.cer](#)”

Root Certificates | EV Chain Certificates | Non-EV Chain Certificates

Entrust Secure Server CA

File Download: [entrust_ssl_ca.cer](#)
[entrust_ssl_ca.der](#)

Thumbprint: 99A6 9BE6 1AFE 886B 4D2B 8200 7CB8 54FC 317E 1539

Base 64 Format:

```
-----BEGIN CERTIFICATE-----
MIIE2DCCBEGgAwIBAgIEN0rSQzANBgkqhkiG9w0BAQUFADCBwZELMAK
GA1UE
BhMCMVVMxVFDASBgNVBAoTC0VudHJ1c3QubmV0MTswOQYDVQQLEzJ3d
3cuZW50
cnVzdC5uZXQvQ1BTIGluY29ycC4gYnkgcmVmLiAobGitaXRzIGxpYWluKTE
|
MCMGA1UECxMCKGMpIDE5OTkgRW50cnVzdC5uZXQvTGitaXRIZDE6MD
gGA1UE
AxMxRW50cnVzdC5uZXQvU2VjdXJlIEN0rSQzANBgkqhkiG9w0BAQUFAD
1
dGhvcml0eTAeFw05OTA1MjUxNjA5NDNBaFw0xOTA1MjUxNjM5NDNBMIHD
MQsw
COVDMVVMxVFDASBgNVBAoTC0VudHJ1c3QubmV0MTswOQYDVQQLEzJ3d
3cuZW50
-----END CERTIFICATE-----
```

Entrust CA (2048)

File Download: [entrust_2048_ca.cer](#)

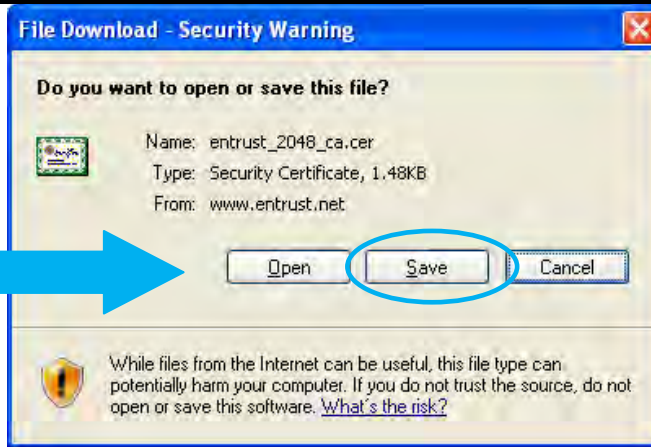
Thumbprint: 5030 0609 1D97 D4F5 AE39 F7CB E792 7D7D 652D 3431

Base 64 Format:

```
-----BEGIN CERTIFICATE-----
MIIEKjCCAxKgAwIBAgIEOGPe+DANBgkqhkiG9w0BAQUFADCBtDEUMBIG
A1UEChMLRW50cnVzdC5u
-----END CERTIFICATE-----
```

5. In the dialogue box that appears, click **“Save”**

Save the certificate to a removable drive



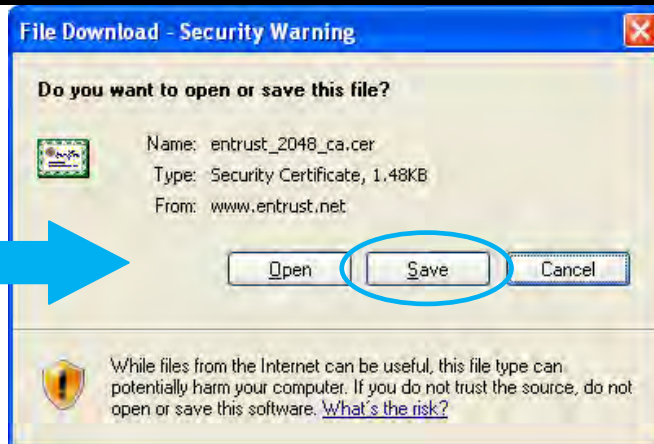
6. You will now download the second certificate.

Scroll to the bottom of the Entrust page and download the last Root Certificate listed, **“Entrust Root CA – G2”**, by clicking on the File Download link **“entrust_g2_ca.cer”**



7. In the dialogue box that appears, once again click **“Save”**

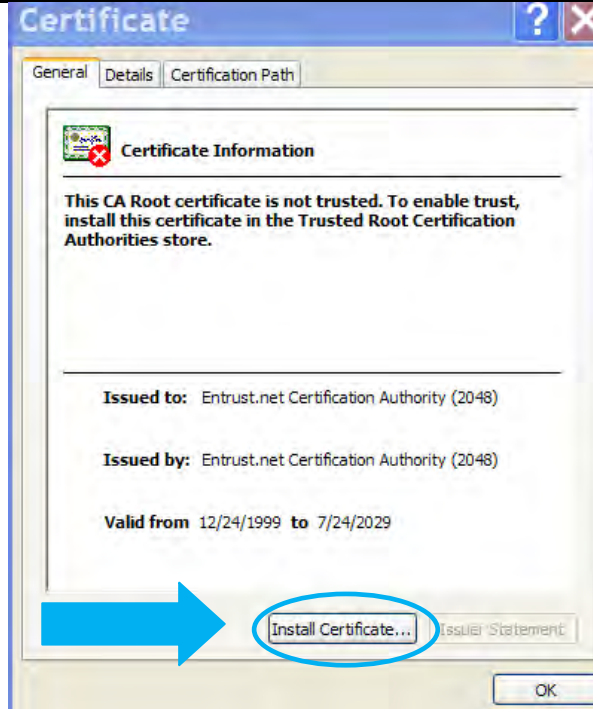
Save the certificate to the same removable drive used for step 5.



8. Insert the removable drive into the computer(s) that is **not** connected to the Internet, which utilizes the FedLine Advantage and FedLine Web access solutions, Check 21 SecureTransport Client and FedImage and FedImage Services Gateway.

9. Double click on the File Download link **“entrust 2048 ca.cer”** available in your removable drive menu

In the *Certificate* menu, click **“Install Certificate...”**



10. In the Certificate Import Wizard *Welcome Screen*, click **“Next >”**

11. In the Certificate Import Wizard *Certificate Store Screen*, select **“Automatically select the certificate store based on the type of certificate”** and click **“Next >”**



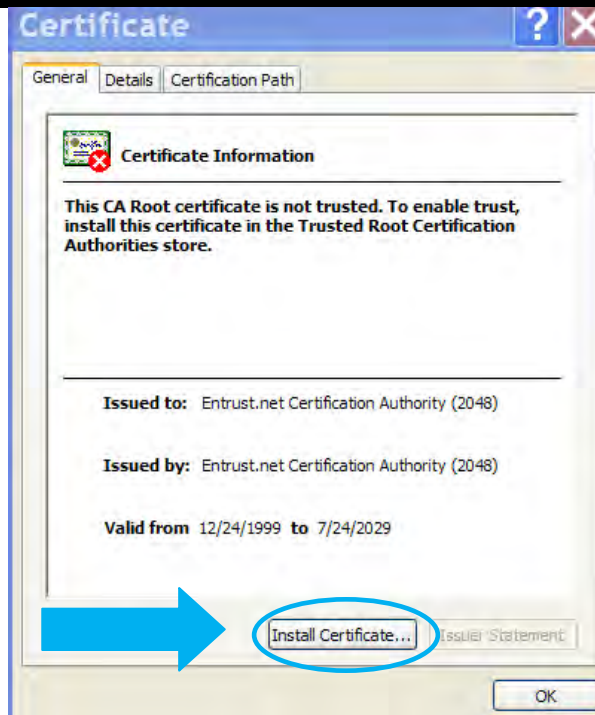
12. In the Certificate Import Wizard *Completing the Certificate Import Screen*, click **“Finish”**

13. Once you are prompted with the following screen notifying you that the import was successful, click **“OK”**.



14. To download the second certificate, double click on the File Download link “[entrust_g2_ca.cer](#)” available in your removable drive menu

In the *Certificate* menu, click “**Install Certificate...**”



15. Follow steps 10 – 13 above to complete the second Root Certificate download.

You have now downloaded both Root Certificates on your computer. The process outlined in Section 2 should be repeated for all non Internet-connected computers which utilize the FedLine Advantage and FedLine Web access solutions, Check 21 SecureTransport Client and FedImage and FedImage Services Gateway. Please move on to Section 3 to verify your current Entrust Certificates.

Section 3: Verify Your Current Entrust Certificates

- Open an Internet Explorer® browser
- Open the "Tools" menu
- Select "Internet Options"
- Select the "Content" tab
- Click "Certificates"
- Select the "Trusted Root Certification Authorities" tab
- Scroll down to verify you have **both** of the following certificates in your trusted certificate root store
 - Entrust.net Certification Authority (2048), **Expiration Year 2029**
 - Entrust Root Certification Authority - G2, **Expiration Year 2030**
 - **Do not remove any existing Entrust Certificates**



"FedLine," "FedLine Advantage," "FedImage" and "FedLine Web" are registered service marks of the Federal Reserve Banks. A complete list of marks owned by the Federal Reserve Banks is available at FRBservices.org.

Entrust® is a trademark or a registered trademark of Entrust, Inc. in the United States and certain countries

"Windows" and "Internet Explorer" are registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

"SecureTransport" is a trademark of Axway Inc, formerly Tumbleweed Communications Corp.