# **How to add a trusted Certificate Authority certificate to Internet Explorer or Microsoft Edge**

<https://www.techrepublic.com/article/how-to-add-a-trusted-certificate-authority-certificate-to-internet-explorer-or-microsoft-edge/>

Adding a trusted Certificate Authority certificate to your browser to suppress intrusive security warnings will allow your users better peace of mind.



Image: XtockImages, Getty Images/iStockphoto

Web browsers utilize Secure Sockets Layer (SSL) to encrypt traffic between client systems and server computers in order to protect confidential data such as social security information, credit card details, and the like.

**More about cybersecurity**

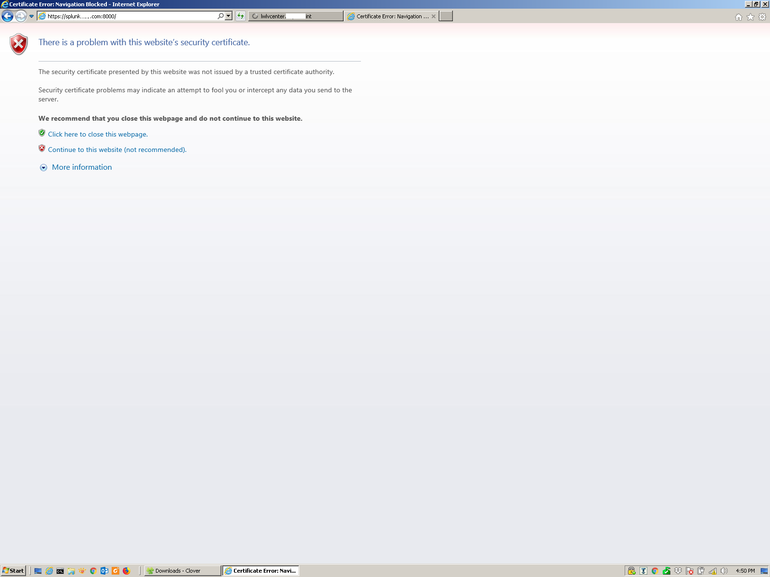
* [Cybercriminals exploiting coronavirus outbreak with virus-themed sales on the dark web](https://www.techrepublic.com/article/cybercriminals-exploiting-coronavirus-outbreak-with-virus-themed-sales-on-the-dark-web/)
* [How to become a cybersecurity pro: A cheat sheet](https://www.techrepublic.com/article/cheat-sheet-how-to-become-a-cybersecurity-pro/)
* [Gallery: 20 terrifying uses of artificial intelligence](https://www.techrepublic.com/pictures/10-terrifying-uses-of-artificial-intelligence/)
* [Kubernetes security guide (free PDF)](https://www.techrepublic.com/resource-library/downloads/kubernetes-security-guide-free-pdf/)

In order for an SSL certificate to work properly, the entity that issued the certificate (also known as a Certificate Authority or CA) must also be trusted by the web browser, which involves installing the issuer certificate so that the browser knows that issuer is valid and reliable.

Commonly used Certificate Authorities such as Verisign, DigiCert, Entrust, Comodo, or other big names are automatically trusted by most browsers. However, if you utilize an untrusted internal Certificate Authority to generate SSL certificates for internal resources, you will be nagged by your browser when you attempt to connect.

The Internet Explorer 11 web browser will show something similar to this in **Figure A**.

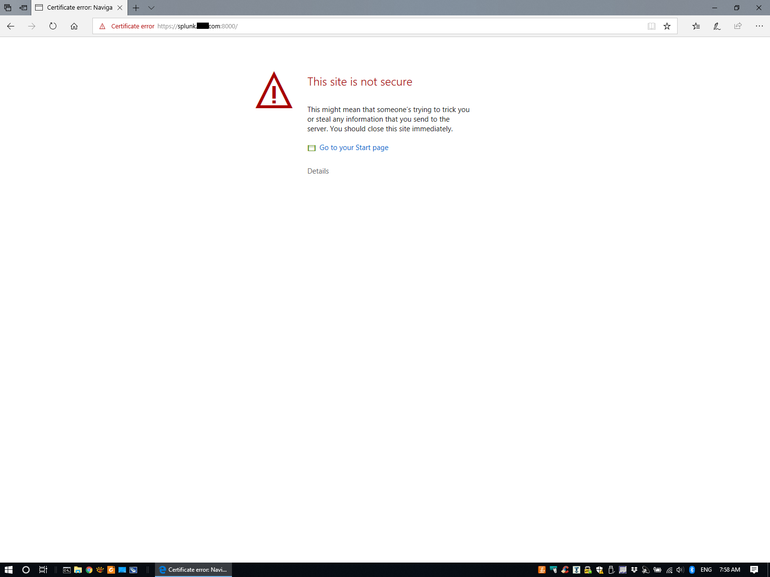
**Figure A**



To continue you have to click Continue To This Website (Not Recommended).

The Microsoft Edge browser will display the following in **Figure B**.

**Figure B**



Clicking Details and then Go On To The Webpage (Not Recommended) will permit the access.

However, while these tips for both browsers lead you to the site, you'll have to do this for EVERY site for which your internal CA issued an SSL certificate.

Furthermore, this may bode poorly for system admins who have urged users to read and follow browser security warnings. They would look foolish contradicting themselves to tell users to, "just ignore the warning and proceed to the site."

**SEE:**[**IT leader's guide to big data security**](http://www.techproresearch.com/downloads/it-leader-s-guide-to-big-data-security/)**(Tech Pro Research)**

Fortunately, there's a better way. You can configure your system(s) to trust all certificates from a Certificate Authority by installing that system's SSL certificate as a Trusted Root Certificate Authority. That way, the browser will never prompt you again about accessing any site with a certificate from that CA, and your users can take security prompts seriously.

**Note:** This article focuses on Microsoft's Internet Explorer 11 and Edge browsers; [I previously covered how to do this in Firefox and Chrome](https://www.techrepublic.com/article/how-to-add-a-trusted-certificate-authority-certificate-to-chrome-and-firefox/). The steps in this tutorial were accurate at the time this article was written, but future versions of these browsers may involve different menu options.

**How to obtain your CA certificate**

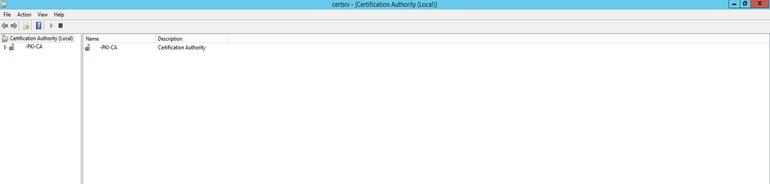
First you need to get a copy of that SSL certificate from your CA in DER format. If your CA runs Windows follow the steps below. Otherwise, research the details for your particular operating system.

Go to Control Panel on the CA machine.

Open the Administrative Tools folder.

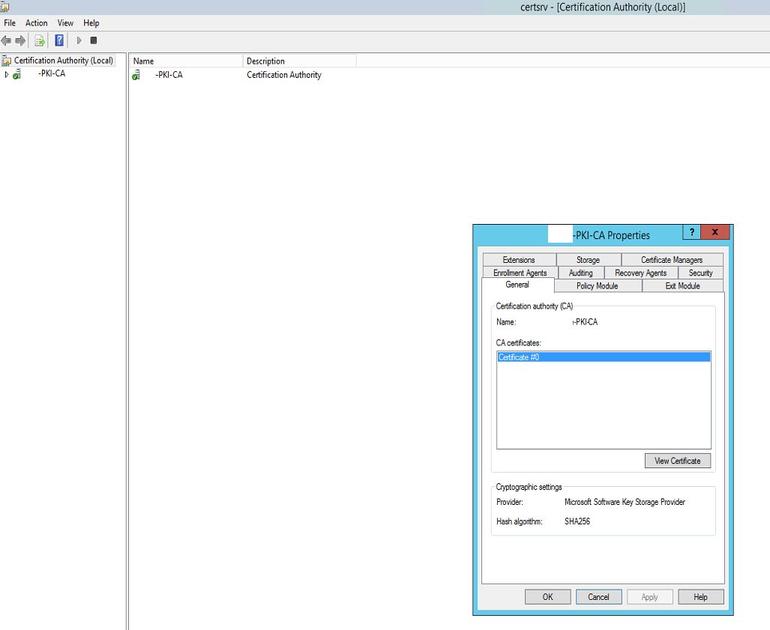
Double-click Certification Authority **(Figure C)**.

**Figure C**



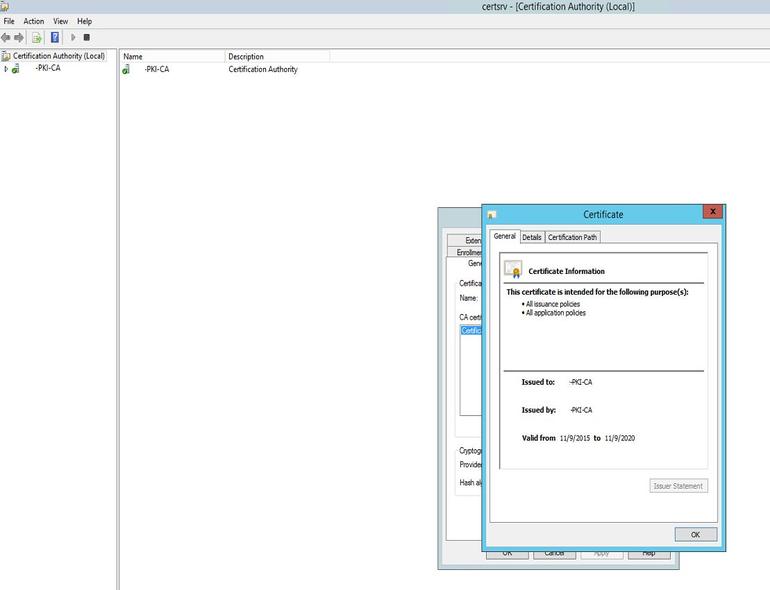
Right-click the server and then choose Properties **(Figure D)**.

**Figure D**



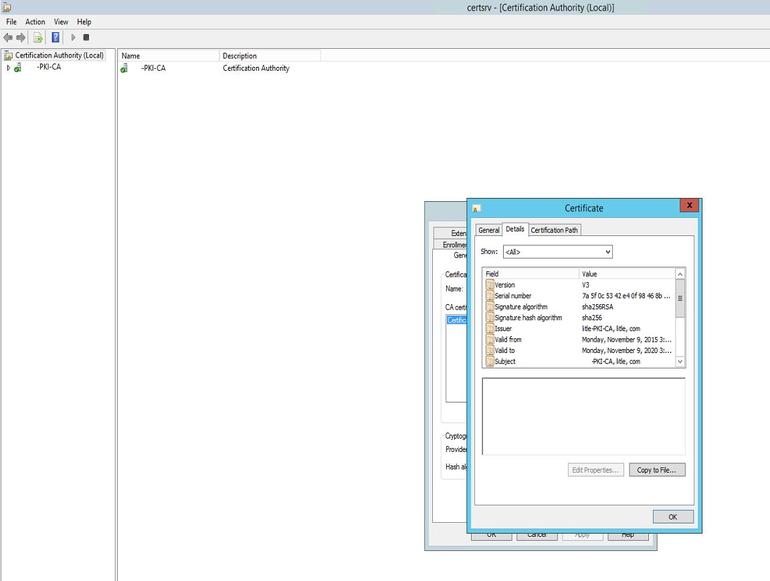
Click View Certificate **(Figure E)**.

**Figure E**



Click the Details tab **(Figure F)**.

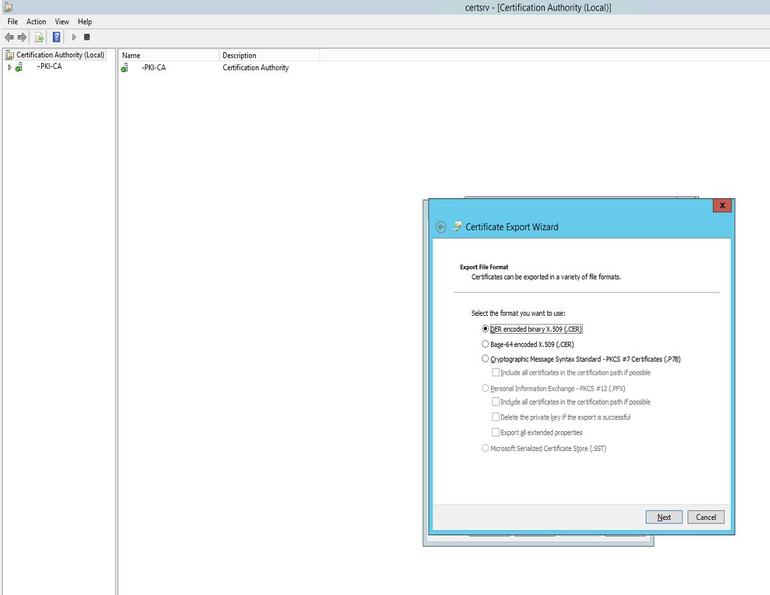
**Figure F**



Click Copy To File.

Click Next **(Figure G)**.

**Figure G**



Leave DER Encoded Binary X.509 (.CER) checked and then click Next.

Specify the file name (c:\CA\_certificate.cer for instance) and then click Next.

Click Finish.

The certificate will be saved to the location you specified.

**How to add the CA certificate as a Trusted Root Authority to Internet Explorer/Microsoft Edge**

If you are using Active Directory, your best bet is to utilize Group Policy so that all systems in your organization will trust certificates from the Certificate Authority, which will also apply to Internet Explorer or Microsoft Edge.

**Utilizing Group Policy to configure Windows systems to trust your CA**

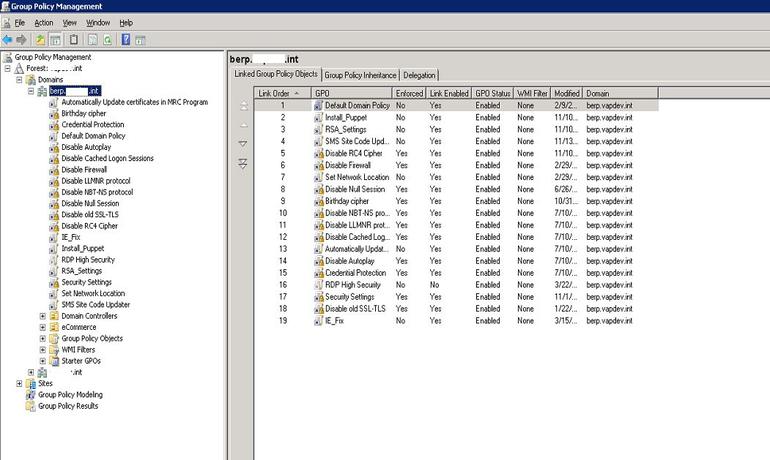
Copy the certificate to your domain controller.

Go to the Control Panel.

Open Administrative Tools.

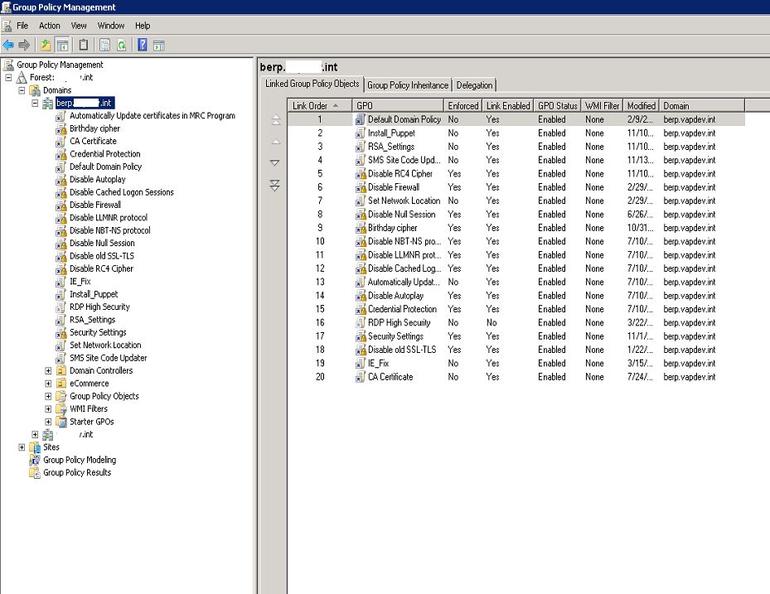
Open Group Policy Management **(Figure H)**.

**Figure H**



Right-click your domain and choose Create A GPO In This Domain And Link It Here. Provide a name for the Group Policy Object, such as CA certificate, and then click OK **(Figure I)**.

**Figure I**



Right-click the new GPO and then click Edit.

Expand Policies.

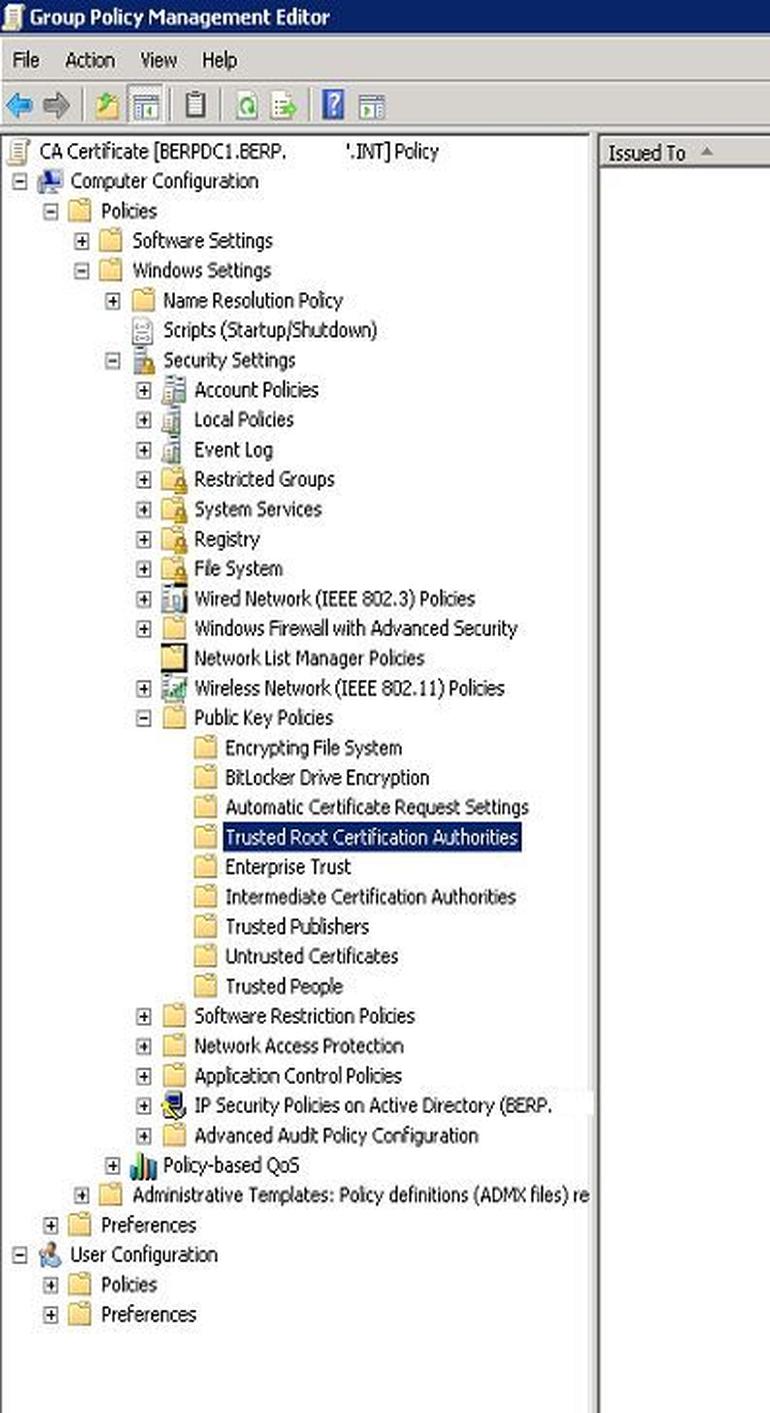
Expand Windows Settings.

Expand Security Settings.

Expand Public Key Policies.

Right-click Trusted Root Certification Authorities And Choose Import **(Figure J)**.

**Figure J**



Click Next.

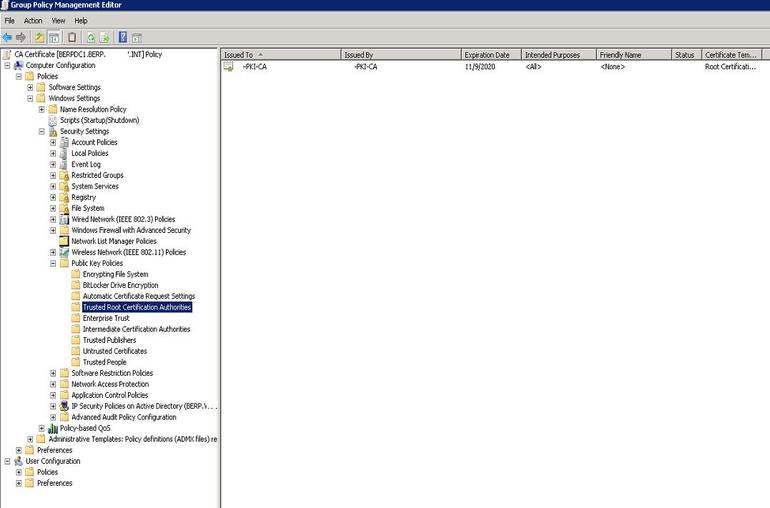
Click Browse and then browse to and select the CA certificate you copied to this computer.

Click Next.

Click Finish and then OK.

You should then see the certificate shown in the right-hand field **(Figure K)**.

**Figure K**



Client machines should begin trusting the Certificate Authority in short order.

**How to manually configure a Windows system to trust your CA**

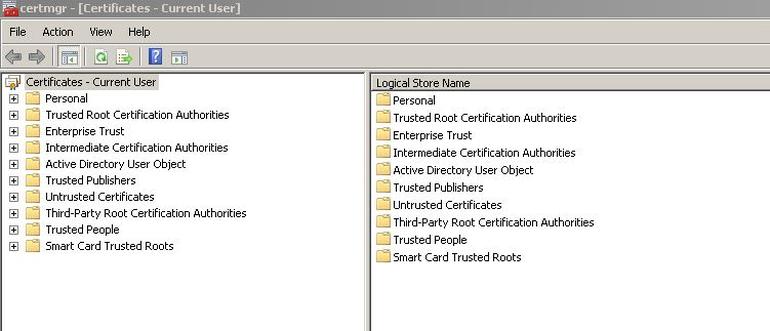
If you're not running Active Directory in your organization, you can't leverage Group Policy, but you can manually add the CA certificate as a Trusted Root Certification Authority on the Windows host in order to trust the related SSL certificates. This will work for both Internet Explorer or Microsoft Edge.

First, copy your CA certificate to the host machine you want to work on.

Open a Command Prompt and run Certificate Manager with the following command **(Figure L)**.

certmgr.msc

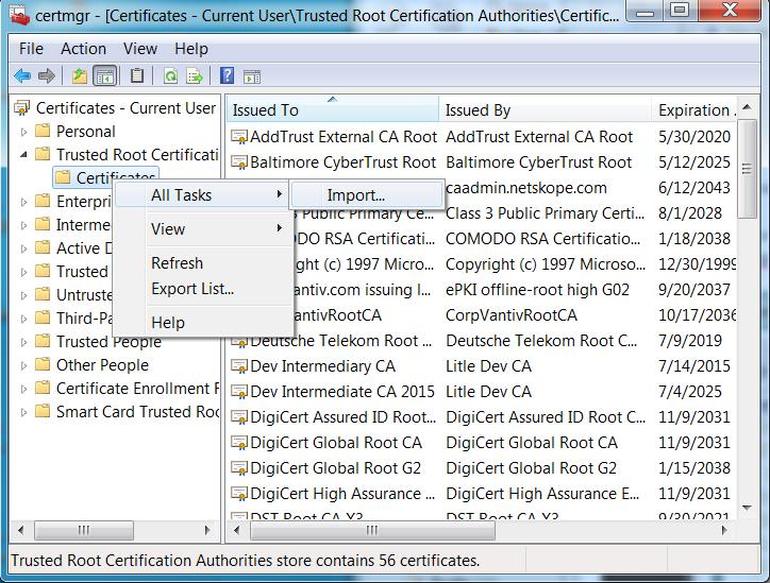
**Figure L**



Administrator

In the left-hand frame, expand Trusted Root Certificates, and then right-click on Certificates and select All Tasks->Import **(Figure M)**.

**Figure M**



In the Certificate Import Wizard click Next **(Figure N)**.

**Figure N**

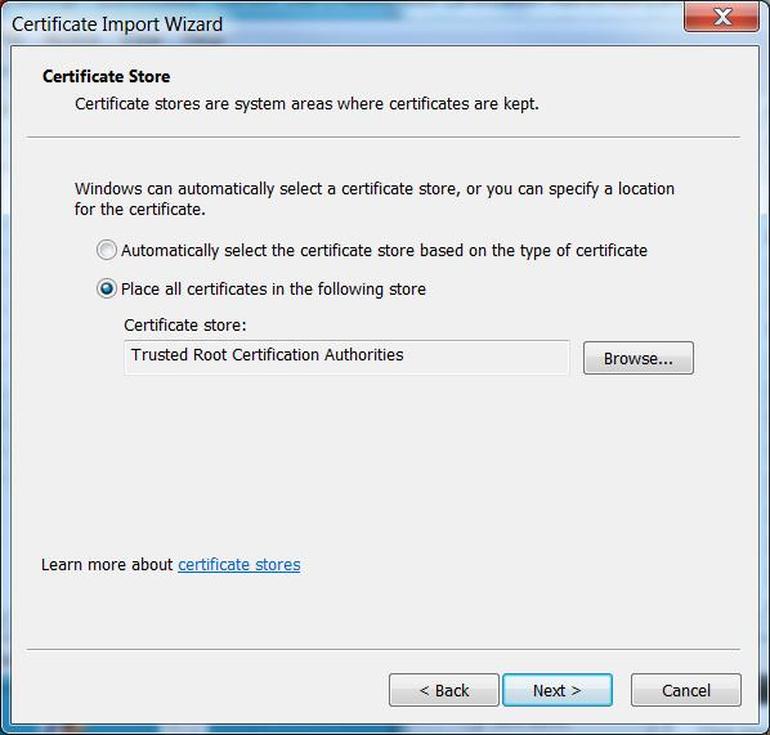


Click Next, and then click Browse and then browse to and select the CA certificate you copied to this computer.

For Place All Certificates In The Following Store select Trusted Root Certification Authorities.

Click Next**(Figure O)**.

**Figure O**



Click Finish.

Click Yes to any final prompt.

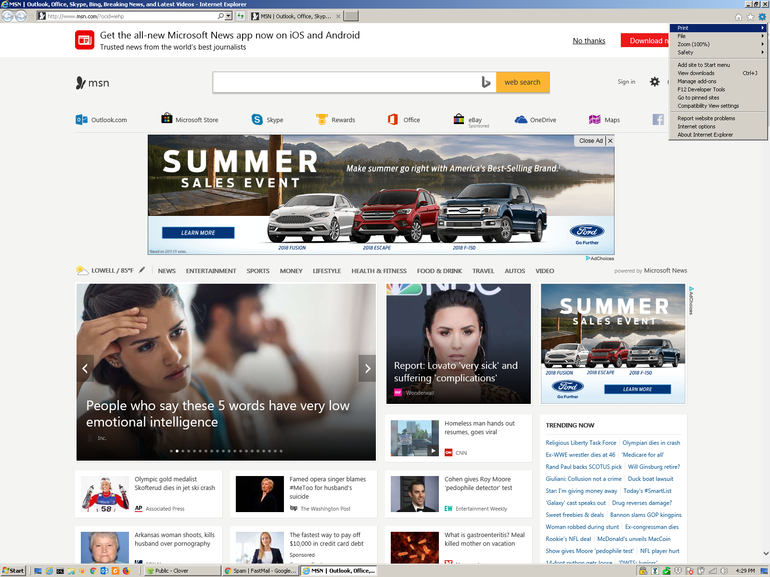
**How to manually add the CA certificate within Internet Explorer**

What if you just want to add the root CA within Internet Explorer or Edge? Well, unfortunately you can't view that with Edge--apparently this is a security feature designed to prevent tampering with certificates directly via the browser--but you can for Internet Explorer. Follow these steps to perform the operation.

Copy the CA certificate to the host machine you want to work on.

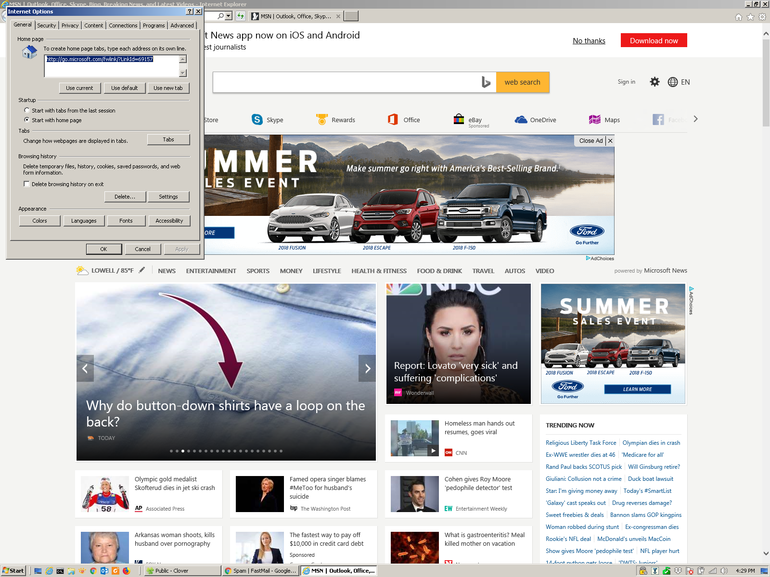
Open Internet Explorer and then click the gear icon in the upper right **(Figure P)**.

**Figure P**



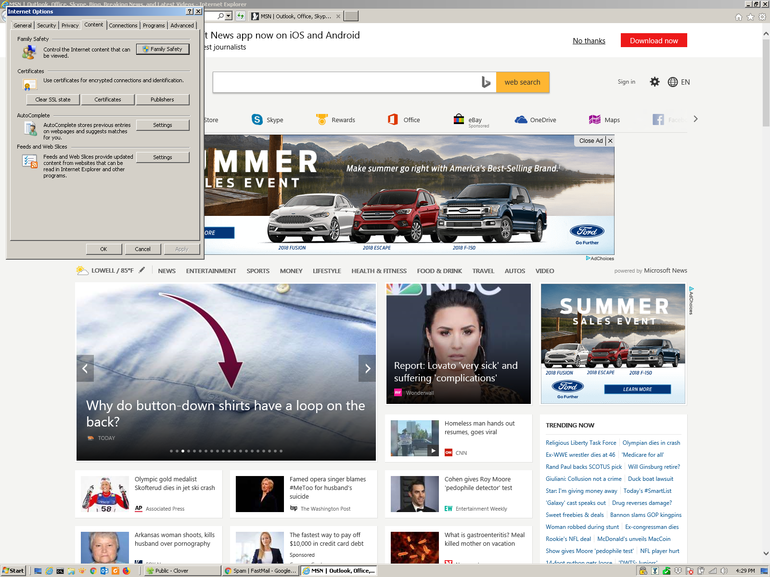
Click Internet Options **(Figure Q)**.

**Figure Q**



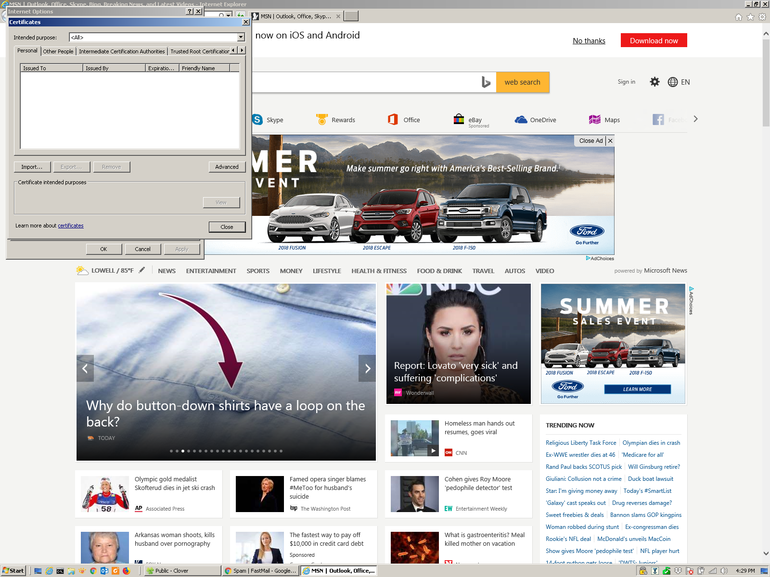
Select the Content tab**(Figure R)**.

**Figure R**



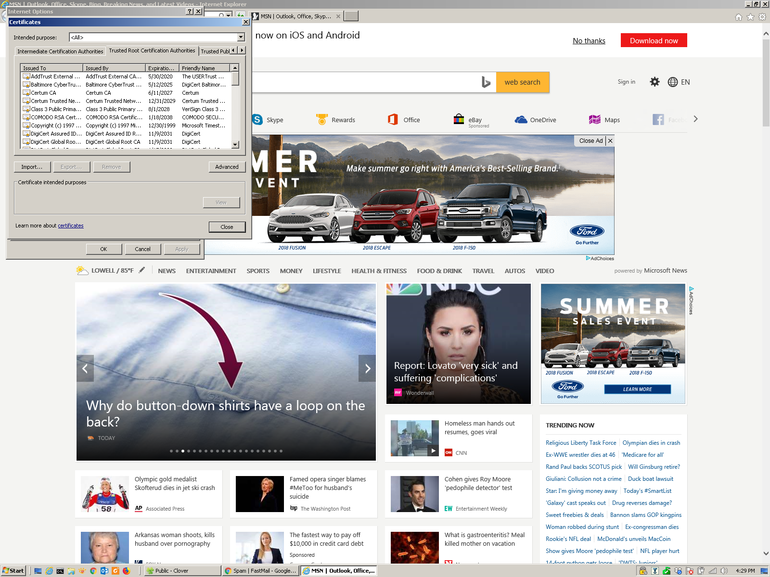
Click Certificates **(Figure S)**.

**Figure S**



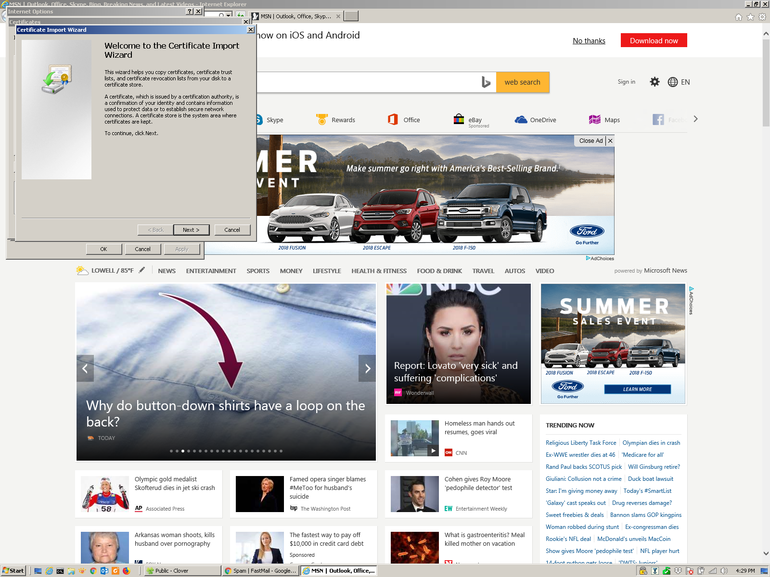
Click the Trusted Root Certification Authorities tab **(Figure T)**.

**Figure T**



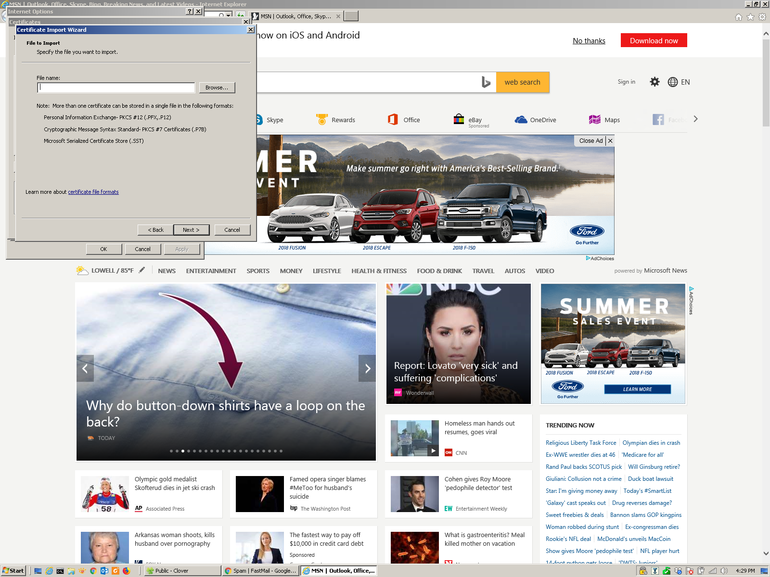
Click Import **(Figure U)**.

**Figure U**



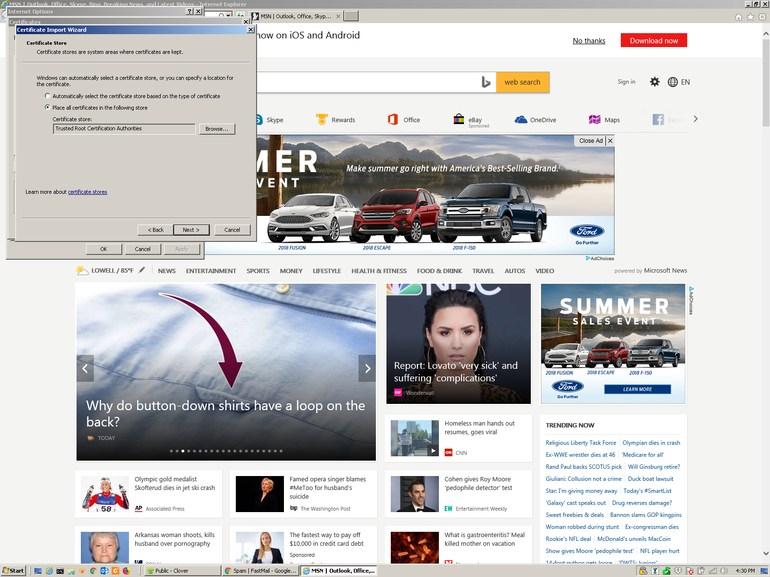
Click Next **(Figure V)**.

**Figure V**



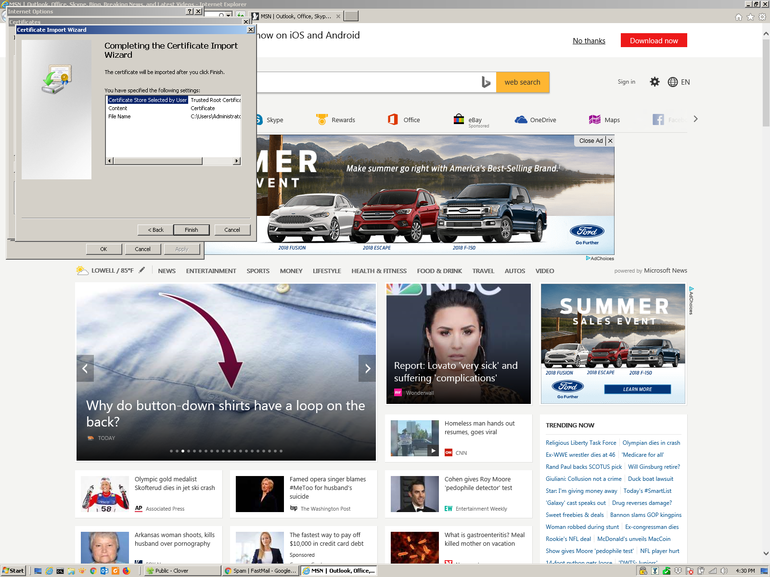
Browse to the location of the CA certificate you saved locally then double-click it **(Figure W)**.

**Figure W**



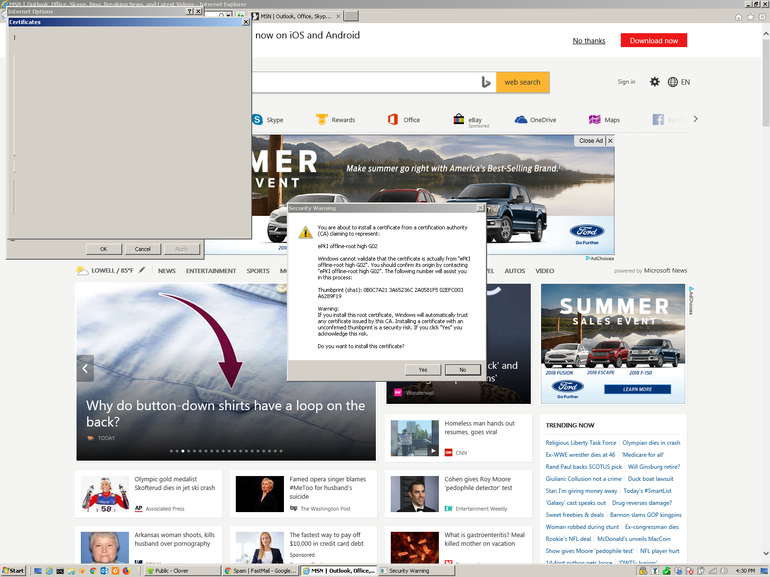
Ensure the Place All Certificates In The Following Store field is set to Trusted Root Certification Authorities and then click Next **(Figure X)**.

**Figure X**



Click Finish **(Figure Y)**.

**Figure Y**



Answer Yes to the confirmation prompt.

Internet Explorer should now trust the Certificate Authorities and stop providing security warnings.