How to add a trusted CA certificate to Chrome and Firefox

by **Scott Matteson** in **Security** on July 25, 2018, 4:19 PM PST

This detailed walk-through explains a variety of approaches to adding a trusted certificate authority to the Chrome and Firefox browsers.

Image: iStock/XtockImages

Web browsers use Secure Sockets Layer (SSL) to encrypt traffic between client systems and server computers to protect confidential data such as social security information and credit card details. For an SSL certificate to work properly, the entity that issued the certificate (also known as a certificate authority) must also be trusted by the web browser, which involves installing the issuer certificate so the browser knows that issuer is valid and reliable.

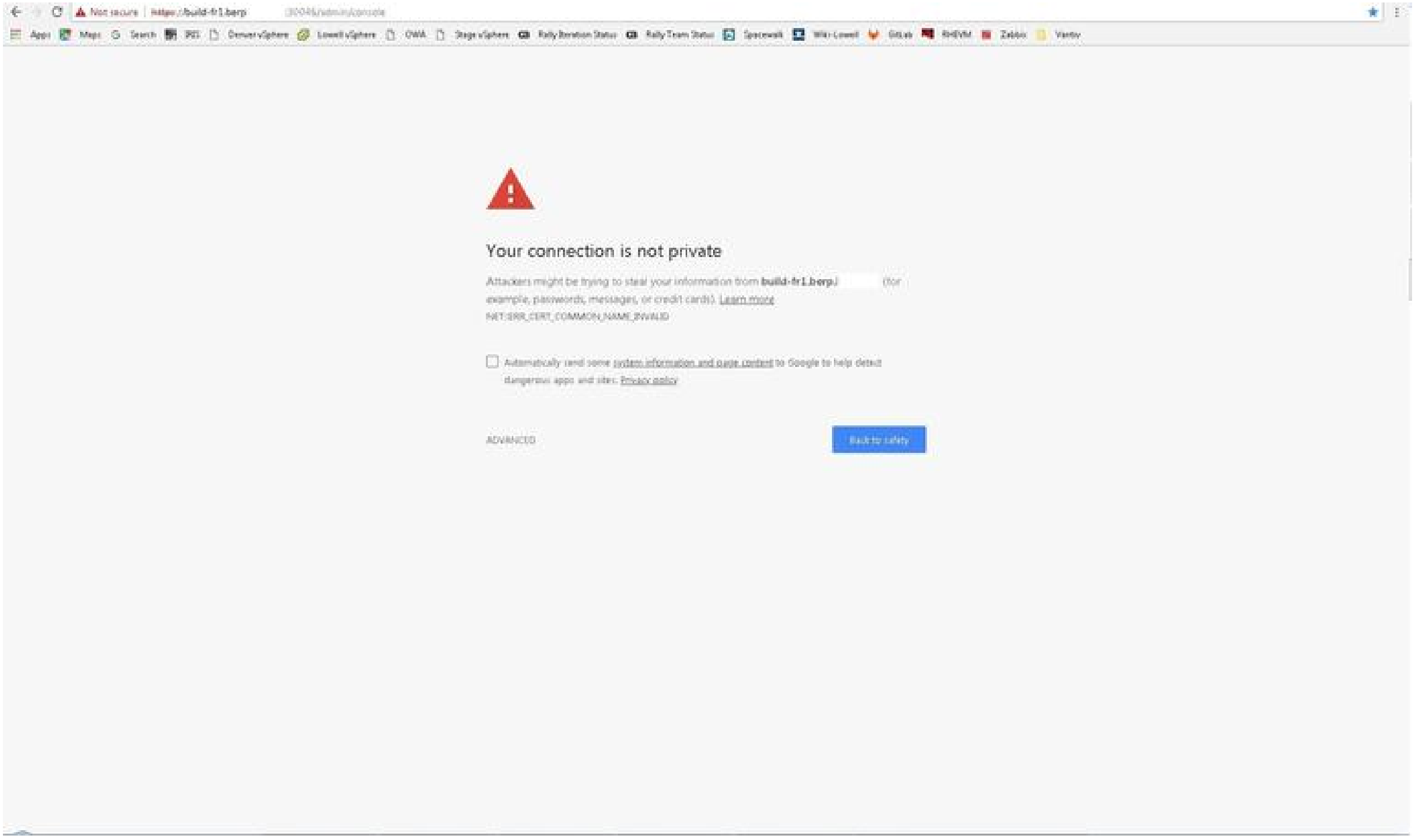
Commonly used certificate authorities, such as Verisign, DigiCert, and Entrust, are automatically trusted by most browsers. However, if you use an untrusted internal

Manage Cookies

certificate authority to generate SSL certificates for internal resources, you will be nagged by your browser when you attempt to connect.

The Chrome web browser will show something similar to **Figure A**.

Figure A


Not secure | https://build-fr1.berp :30046/admin/console
Apps Maps Search Denver vSphere Lowell vSphere OWA Stage vSphere Rally Iteration Status Rally Team Status Spacewalk Wiki-Lowell GitLab RHEVM Zabbix Vantiv

Your connection is not private

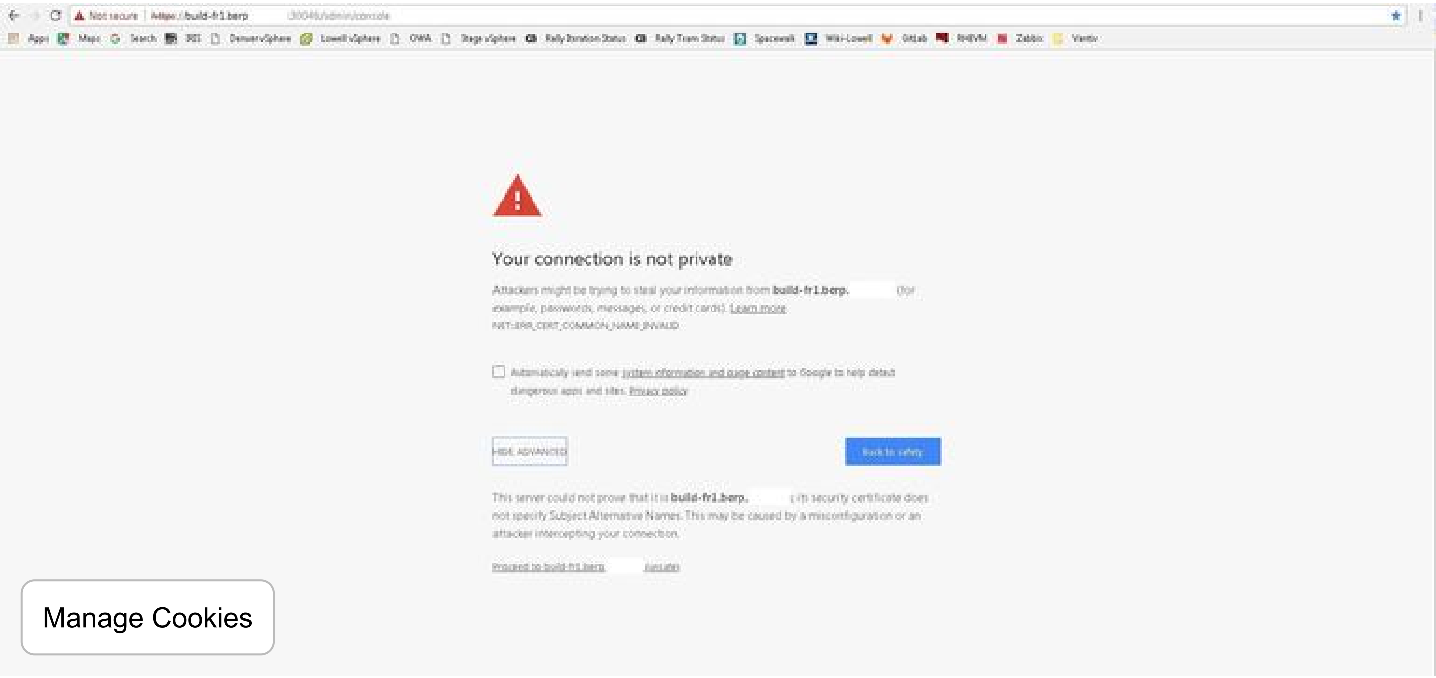
Attackers might be trying to steal your information from **build-fr1.berp.** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

This necessitates clicking Advanced (**Figure B**). Then you must click Proceed To [*host name*] to continue.

Figure B


Not secure | https://build-fr1.berp :30046/admin/console
Apps Maps Search Denver vSphere Lowell vSphere OWA Stage vSphere Rally Iteration Status Rally Team Status Spacewalk Wiki-Lowell GitLab RHEVM Zabbix Vantiv

Your connection is not private

Attackers might be trying to steal your information from **build-fr1.berp.** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

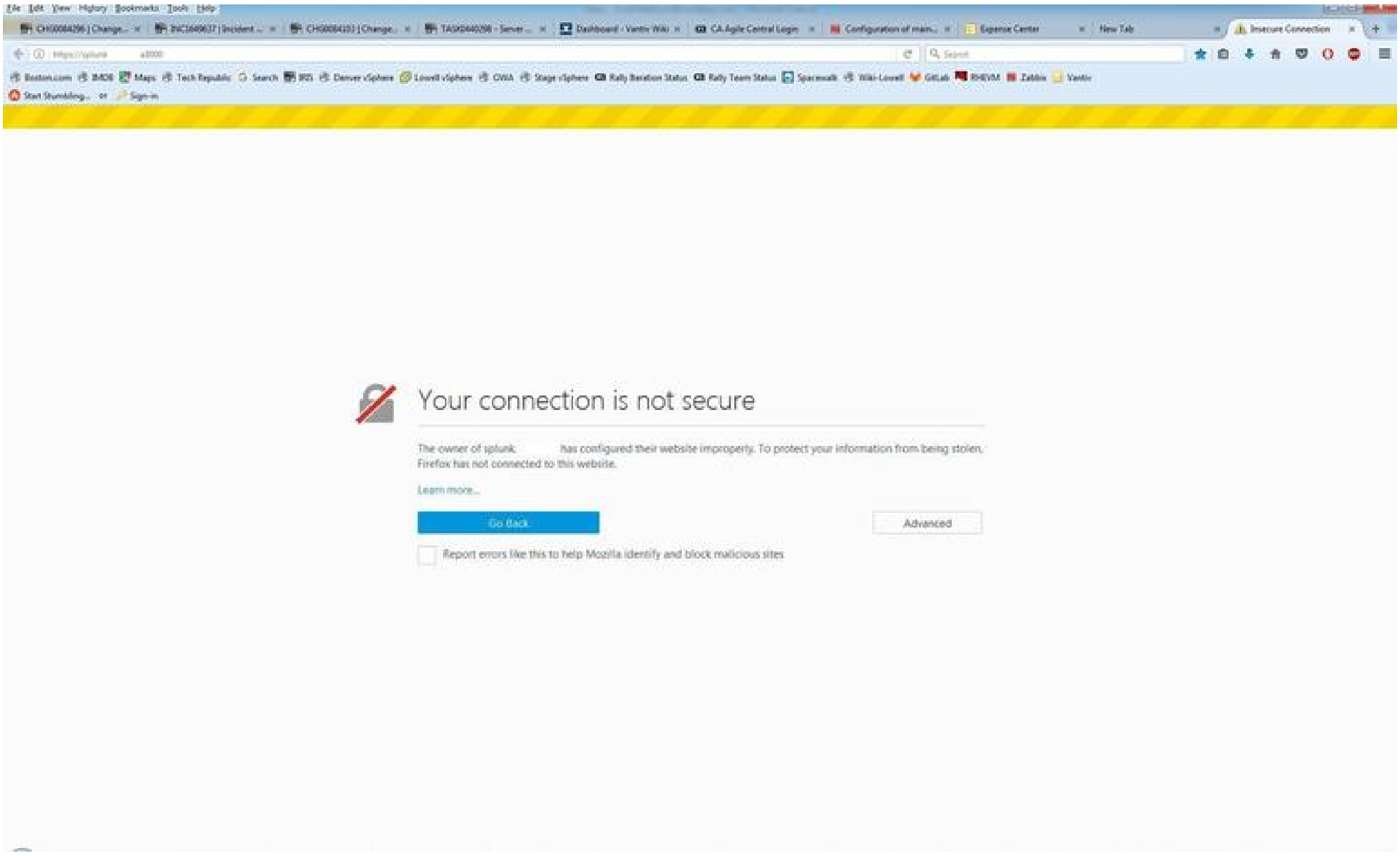
HIDE ADVANCED
Back to safety

This server could not prove that it is **build-fr1.berp.** ; its security certificate does not specify Subject Alternative Names. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to build-fr1.berp. (unsafe)

The Firefox browser will display content resembling **Figure C**. Click Advanced, then Add Exception (**Figure D**). Clicking Confirm Security Exception will permit the access.

Figure C



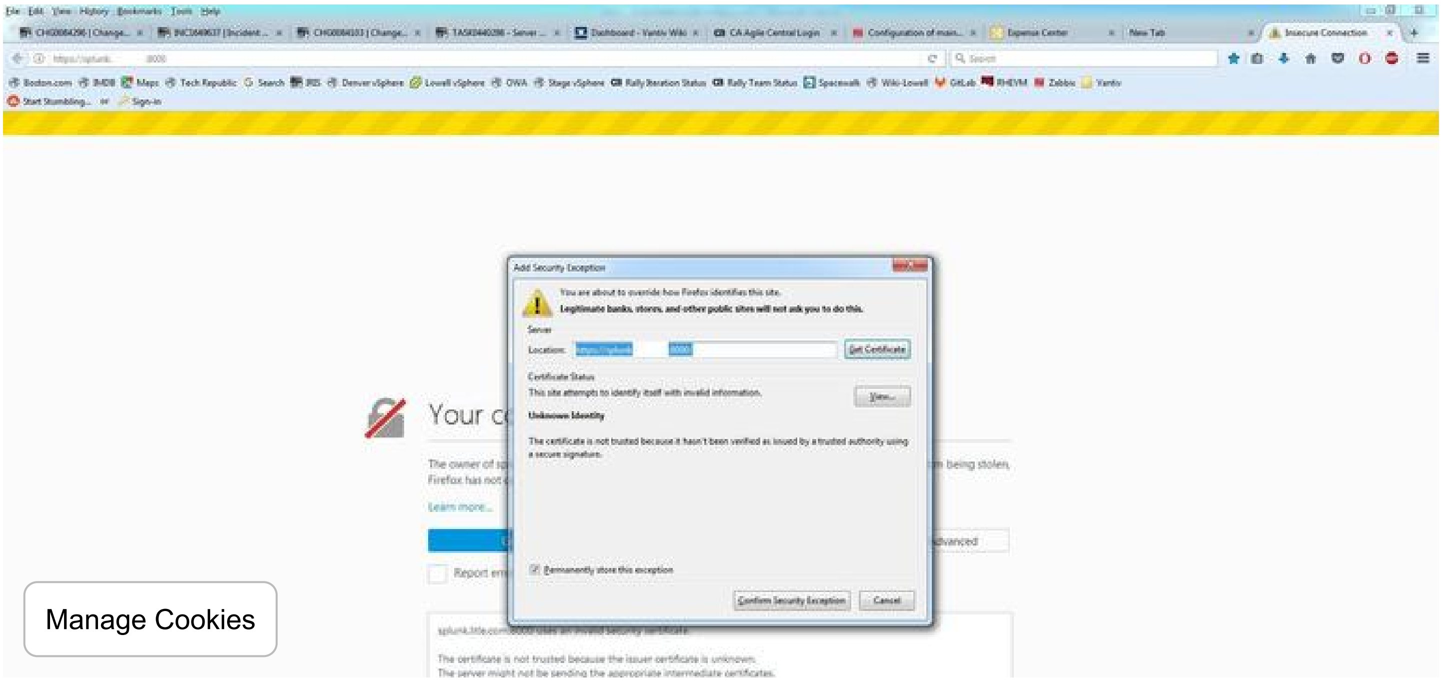
Your connection is not secure

The owner of splunk. has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

Figure D



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location:

Certificate Status

This site attempts to identify itself with invalid information.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.

An additional root certificate may need to be imported.

Error code: SEC_ERROR_UNKNOWN_ISSUER

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

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, Chrome and Firefox will never prompt you again about accessing any site with a certificate from that CA.

Note: This article focuses on these two third-party browsers; a future article will cover Internet Explorer/Microsoft Edge. Steps listed here are accurate at the time of this writing, but future versions of these browsers may involve different menu options.

SEE: Hiring kit: IT audit director (http://www.techproresearch.com/downloads/hiring-kit-it-audit-director/) (Tech Pro Research)

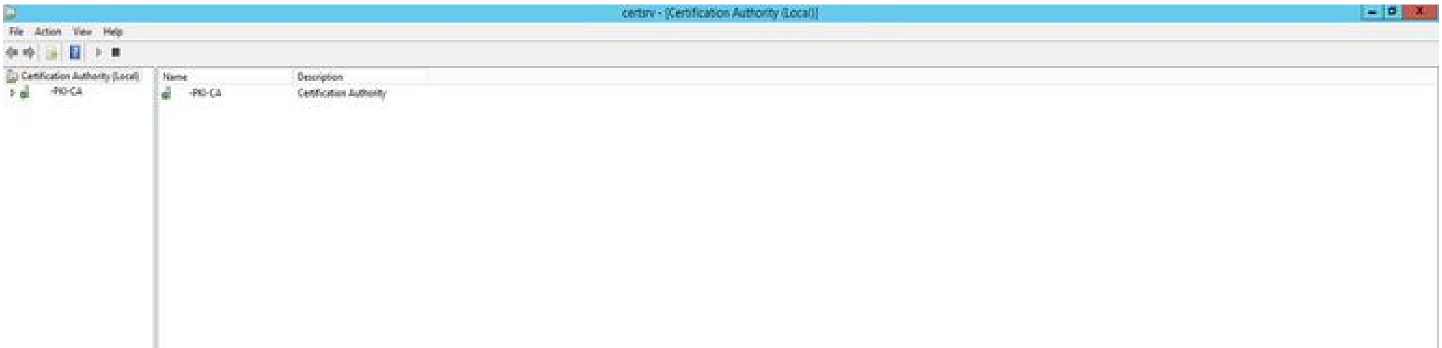
Obtain your CA certificate

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. (If not, you'll need to research the details for your particular operating system.)

Go to Control Panel and open the Administrative Tools folder.

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

Figure E



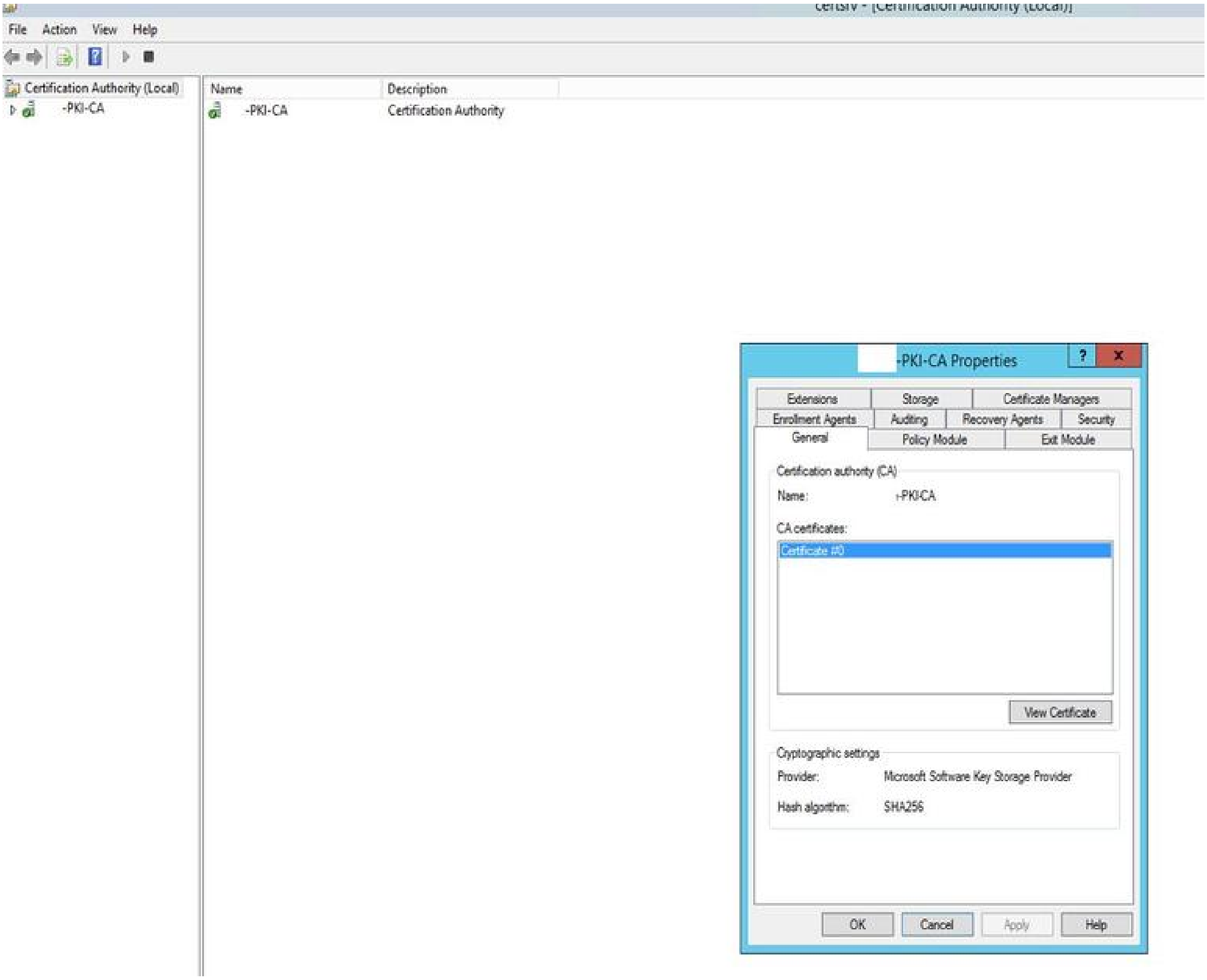
certsrv - [Certification Authority (Local)]

Name	Description
-PKI-CA	Certification Authority

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

F

certsrv - [Certification Authority (Local)]



-PKI-CA Certification Authority

Certification authority (CA)

Name: -PKI-CA

CA certificates:

Certificate #0

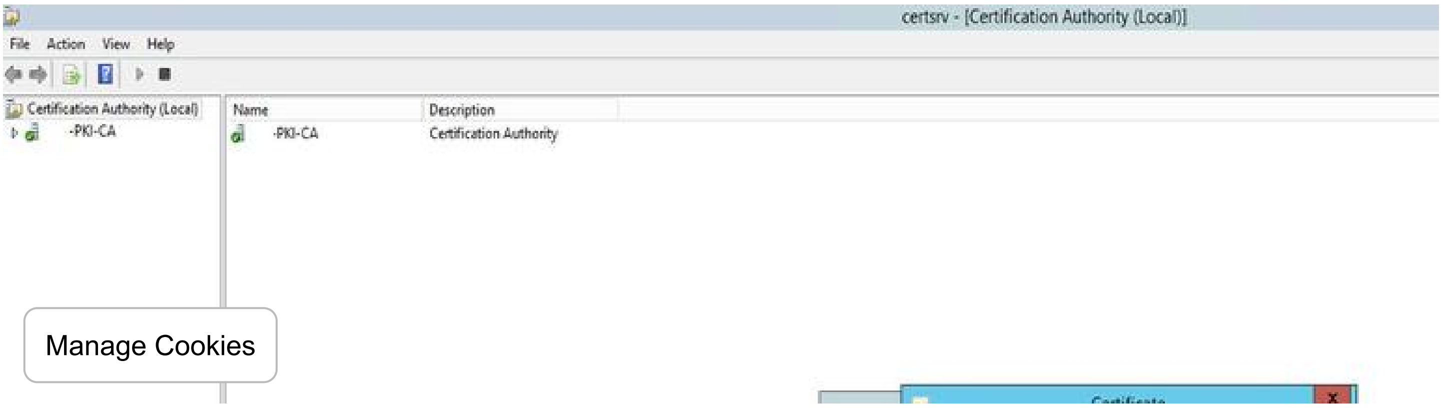
Cryptographic settings

Provider: Microsoft Software Key Storage Provider

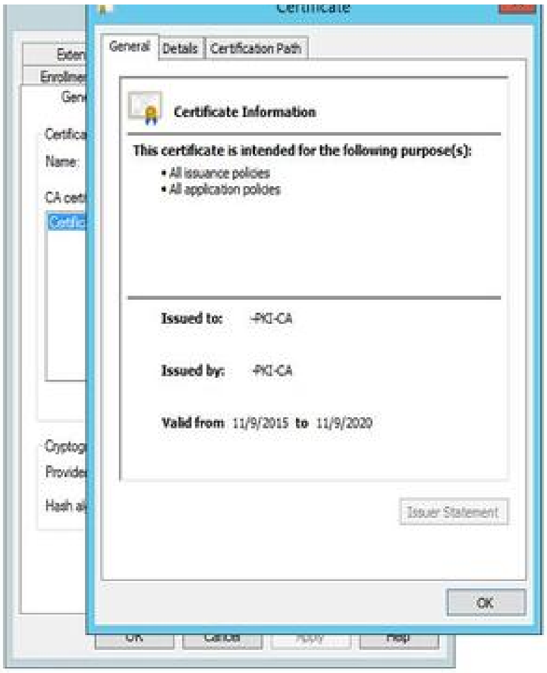
Hash algorithm: SHA256

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

Figure G


certsrv - [Certification Authority (Local)]
File Action View Help
Certification Authority (Local)
-PKI-CA
Name
Description
Certificate

-PKI-CA Certification Authority



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

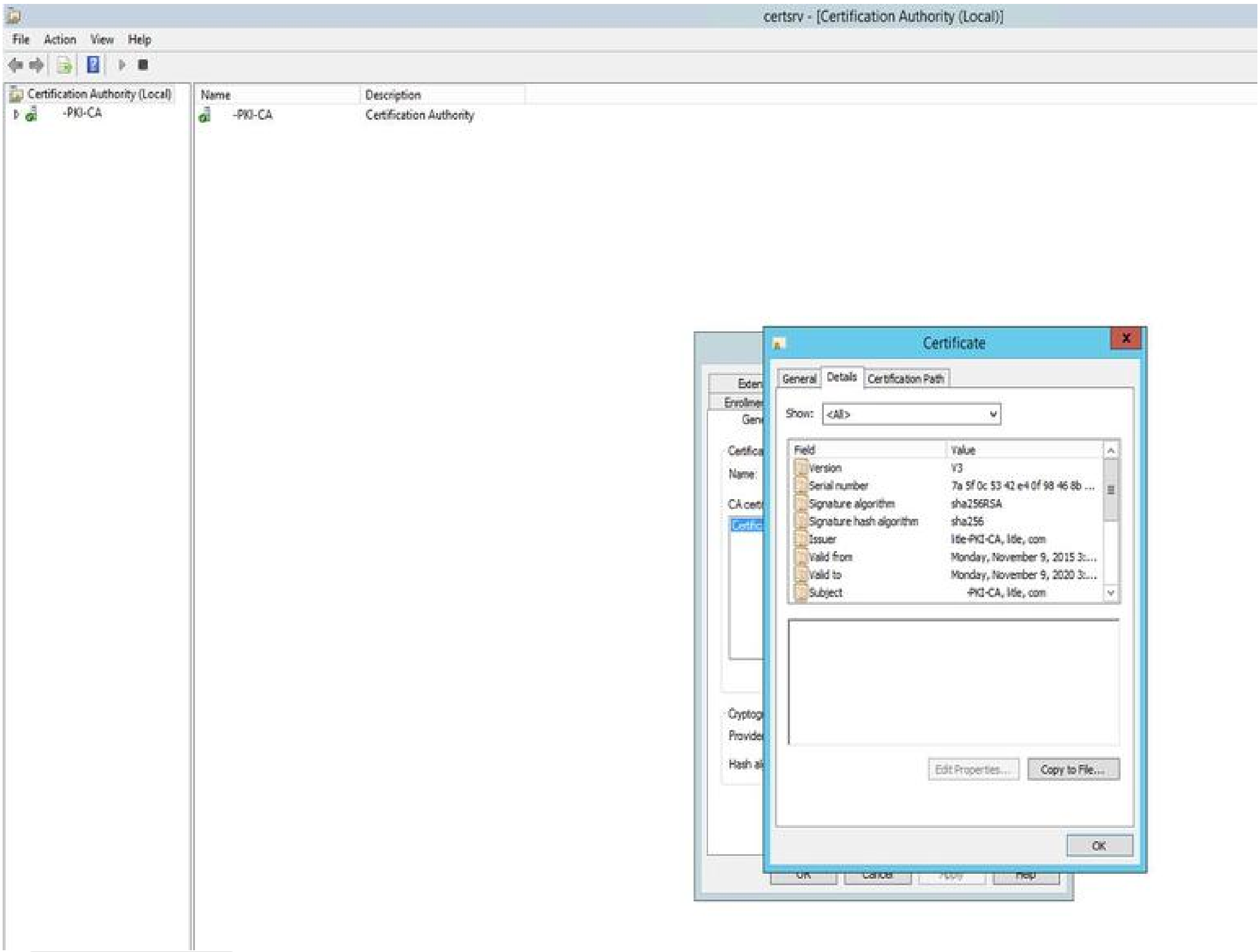
Issued to: -PKI-CA

Issued by: -PKI-CA

Valid from 11/9/2015 to 11/9/2020

Click the Details tab (**Figure H**).

Figure H



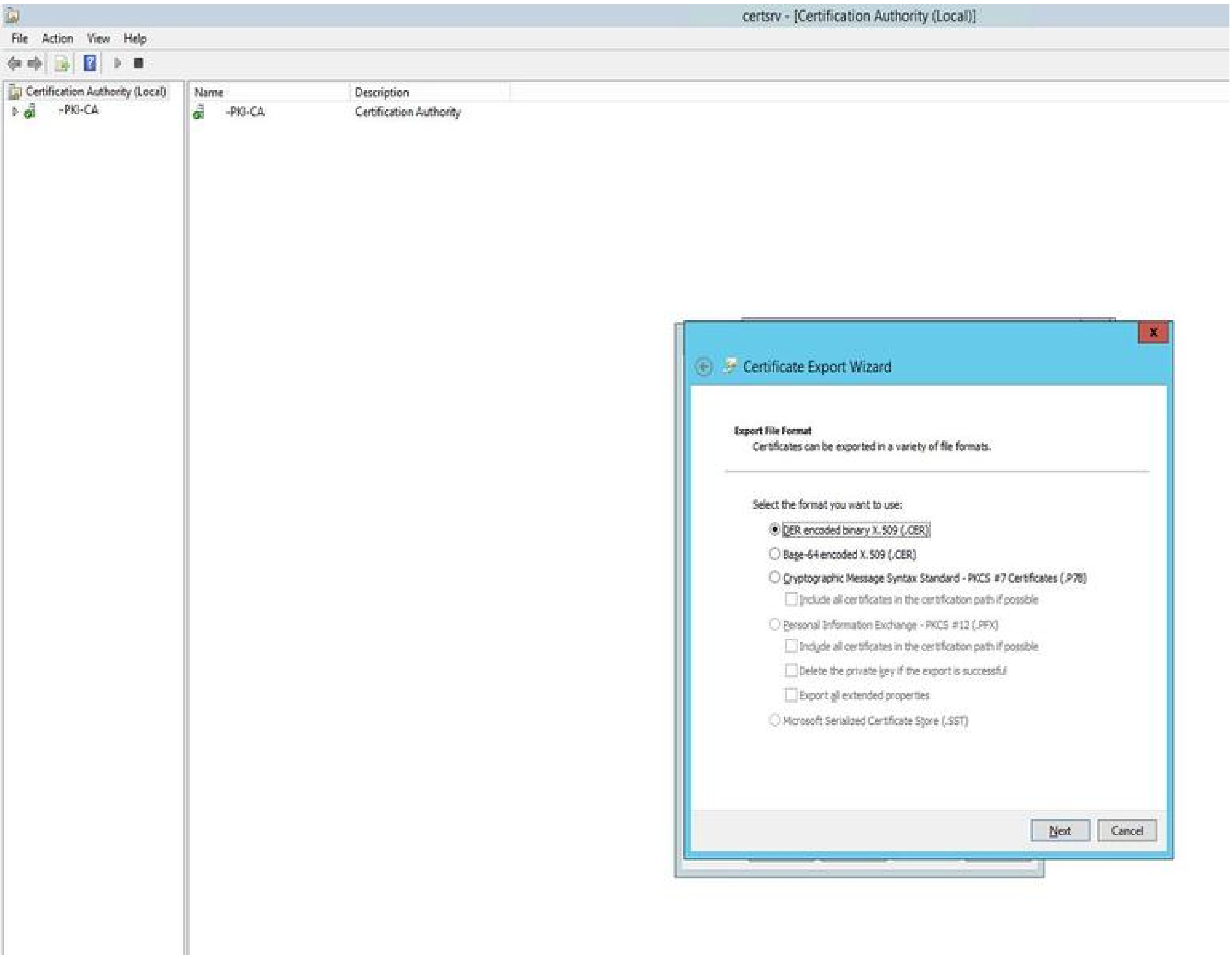
Name	Description
-PKI-CA	Certification Authority

Show: <All>

Field	Value
Version	V3
Serial number	7a 5f 0c 53 42 e4 0f 98 46 8b ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Idle-PKI-CA, Idle, com
Valid from	Monday, November 9, 2015 3:...
Valid to	Monday, November 9, 2020 3:...
Subject	-PKI-CA, Idle, com

C e, then click Next (**Figure I**).

Figure I


certsrv - [Certification Authority (Local)]
File
Action
View
Help
Certification Authority (Local)
-PKI-CA
Name
Description
-PKI-CA
Certification Authority
Certificate Export Wizard
Next
Cancel

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
- ○ Microsoft Serialized Certificate Store (.SST)

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

Specify the filename (c:\CA_certificate.cer, for instance) and click Next, then click Finish.

The certificate will be saved to the location you specified.

Adding the CA certificates as a trusted root authority to Chrome

If you're using Active Directory, your best best is to use Group Policy so all systems in your organization will trust certificates from the CA. Chrome will trust the certificate if deployed in this manner.

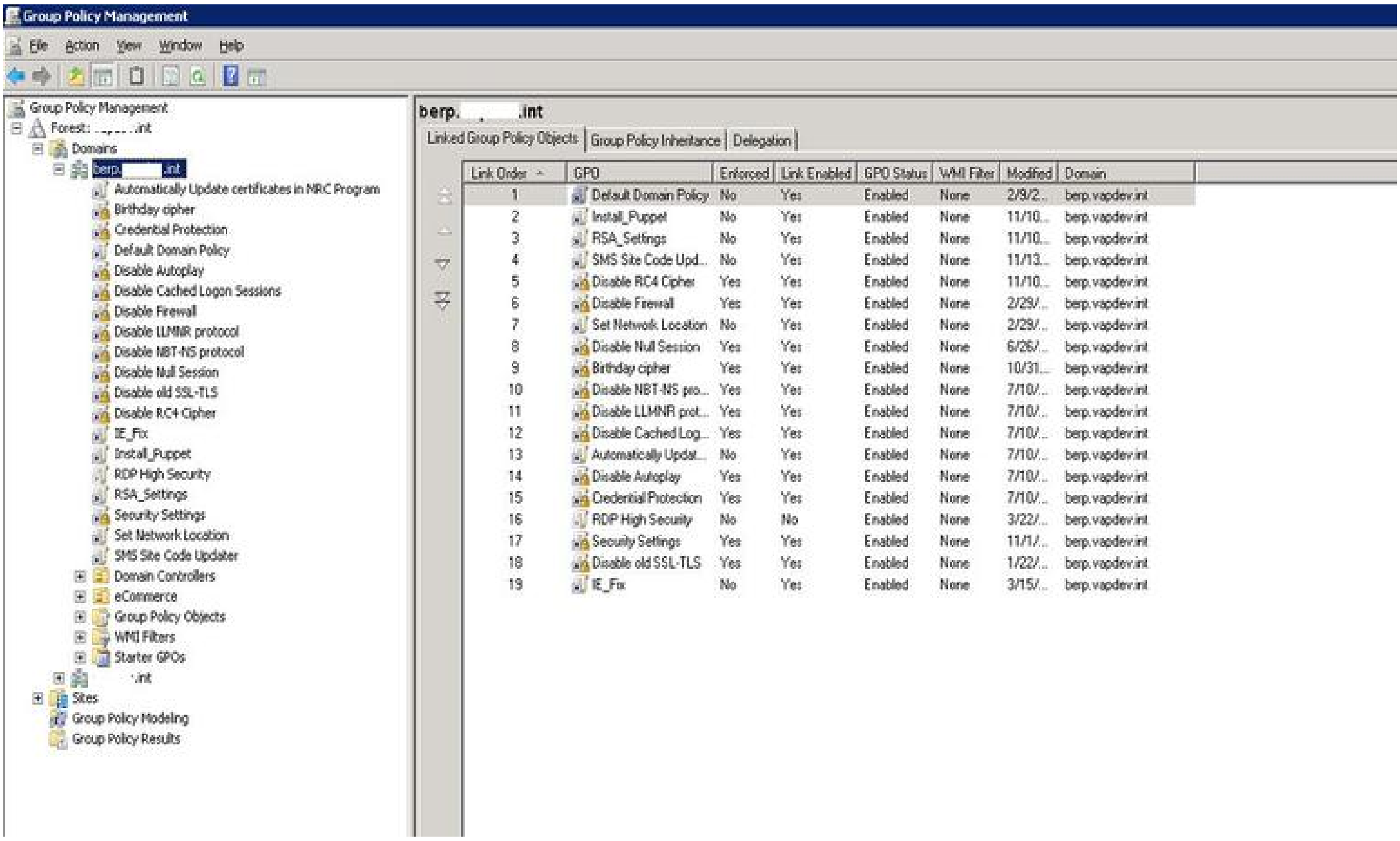
Utilizing Group Policy to configure Windows systems to trust your CA

Copy the certificate to your domain controller.

Go to the Control Panel and open Administrative Tools.

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

Figure J

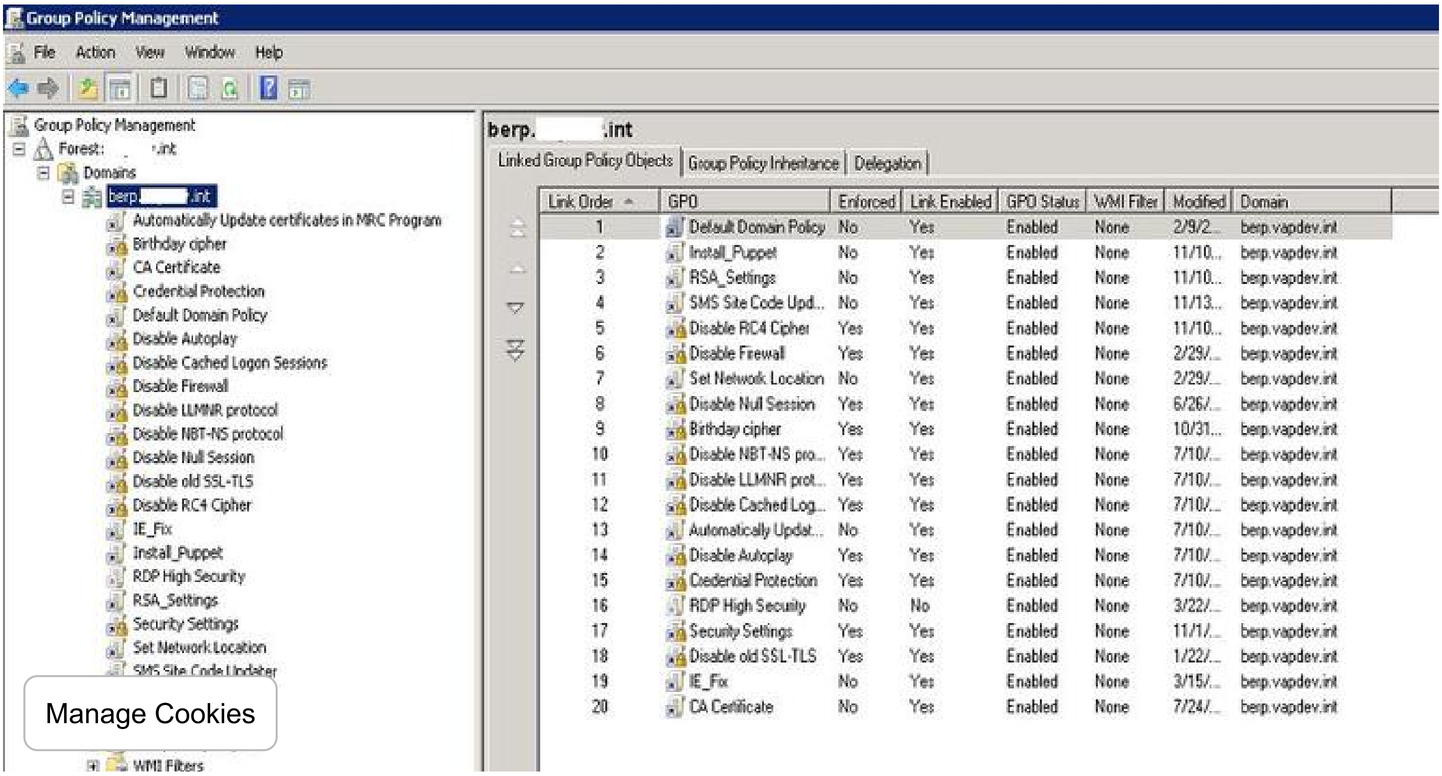


Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Default Domain Policy	No	Yes	Enabled	None	2/9/2...	berp.vapdev.int
2	Install_Puppet	No	Yes	Enabled	None	11/10...	berp.vapdev.int
3	RSA_Settings	No	Yes	Enabled	None	11/10...	berp.vapdev.int
4	SMS Site Code Upd...	No	Yes	Enabled	None	11/13...	berp.vapdev.int
5	Disable RC4 Cipher	Yes	Yes	Enabled	None	11/10...	berp.vapdev.int
6	Disable Firewall	Yes	Yes	Enabled	None	2/29/...	berp.vapdev.int
7	Set Network Location	No	Yes	Enabled	None	2/29/...	berp.vapdev.int
8	Disable Null Session	Yes	Yes	Enabled	None	6/26/...	berp.vapdev.int
9	Birthday cipher	Yes	Yes	Enabled	None	10/31...	berp.vapdev.int
10	Disable NBT-NS pro...	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
11	Disable LLMNR prot...	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
12	Disable Cached Log...	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
13	Automatically Updat...	No	Yes	Enabled	None	7/10/...	berp.vapdev.int
14	Disable Autoplay	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
15	Credential Protection	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
16	RDP High Security	No	No	Enabled	None	3/22/...	berp.vapdev.int
17	Security Settings	Yes	Yes	Enabled	None	11/1/...	berp.vapdev.int
18	Disable old SSL-TLS	Yes	Yes	Enabled	None	1/22/...	berp.vapdev.int
19	IE_Fix	No	Yes	Enabled	None	3/15/...	berp.vapdev.int

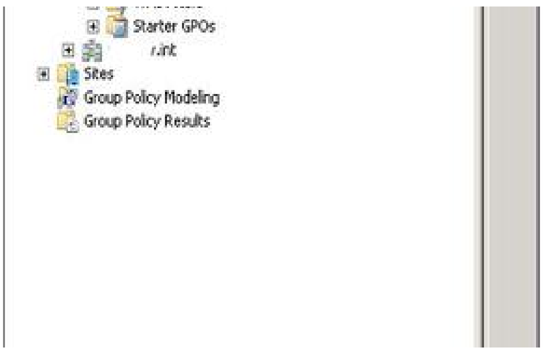
Right-click your domain and choose Create A GPO In This Domain And Link It Here.

Provide a name for the Group Policy Object, such as *CA Certificate*, and click OK (**Figure K**).

Figure K



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Default Domain Policy	No	Yes	Enabled	None	2/9/2...	berp.vapdev.int
2	Install_Puppet	No	Yes	Enabled	None	11/10...	berp.vapdev.int
3	RSA_Settings	No	Yes	Enabled	None	11/10...	berp.vapdev.int
4	SMS Site Code Upd...	No	Yes	Enabled	None	11/13...	berp.vapdev.int
5	Disable RC4 Cipher	Yes	Yes	Enabled	None	11/10...	berp.vapdev.int
6	Disable Firewall	Yes	Yes	Enabled	None	2/29/...	berp.vapdev.int
7	Set Network Location	No	Yes	Enabled	None	2/29/...	berp.vapdev.int
8	Disable Null Session	Yes	Yes	Enabled	None	6/26/...	berp.vapdev.int
9	Birthday cipher	Yes	Yes	Enabled	None	10/31...	berp.vapdev.int
10	Disable NBT-NS pro...	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
11	Disable LLMNR prot...	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
12	Disable Cached Log...	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
13	Automatically Updat...	No	Yes	Enabled	None	7/10/...	berp.vapdev.int
14	Disable Autoplay	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
15	Credential Protection	Yes	Yes	Enabled	None	7/10/...	berp.vapdev.int
16	RDP High Security	No	No	Enabled	None	3/22/...	berp.vapdev.int
17	Security Settings	Yes	Yes	Enabled	None	11/1/...	berp.vapdev.int
18	Disable old SSL-TLS	Yes	Yes	Enabled	None	1/22/...	berp.vapdev.int
19	IE_Fix	No	Yes	Enabled	None	3/15/...	berp.vapdev.int
20	CA Certificate	No	Yes	Enabled	None	7/24/...	berp.vapdev.int



Right-click the new GPO and click Edit.

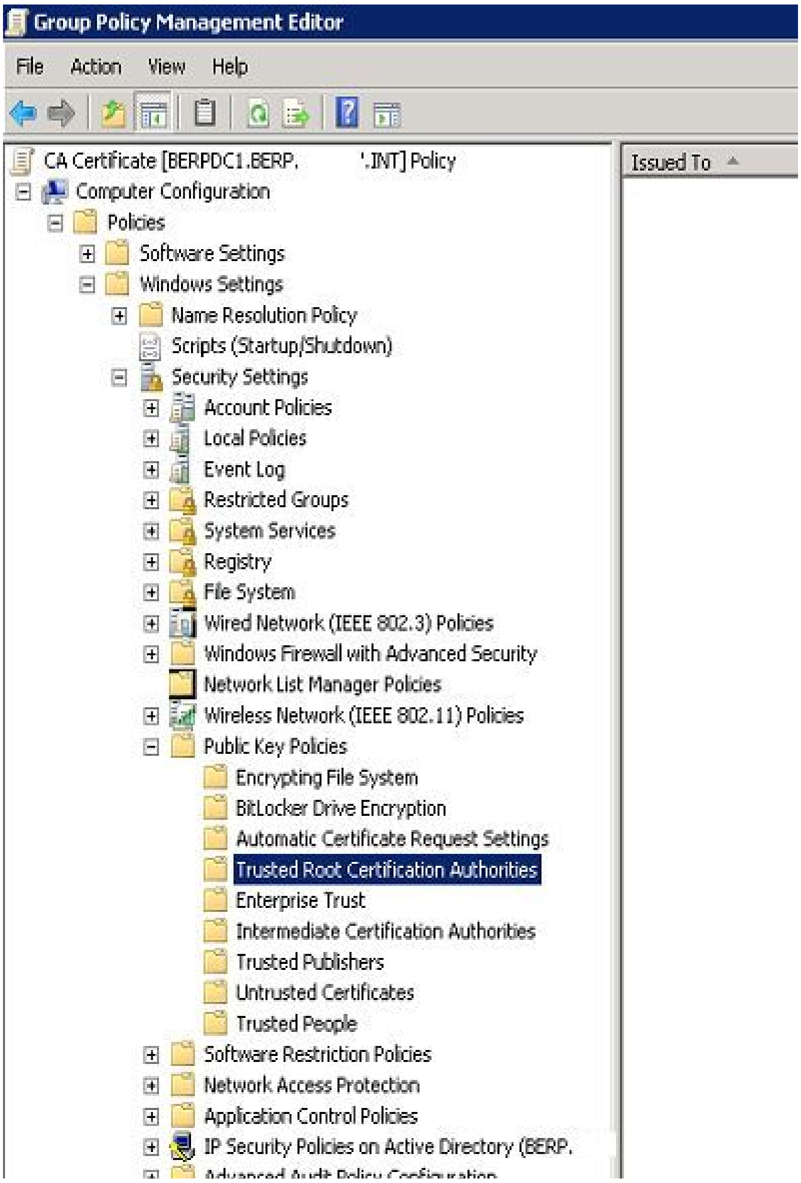
Expand Policies.

Expand Windows Settings.

Expand Security Settings.

Expand Public Key Policies (**Figure L**).

Figure L


Group Policy Management Editor
File Action View Help
CA Certificate [BERPDC1.BERP. '.INT] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
BitLocker Drive Encryption
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (BERP.
Advanced Audit Policy Configuration
Issued To

Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) re
Preferences
User Configuration
Policies
Preferences

Right-click Trusted Root Certification Authorities and choose Import.

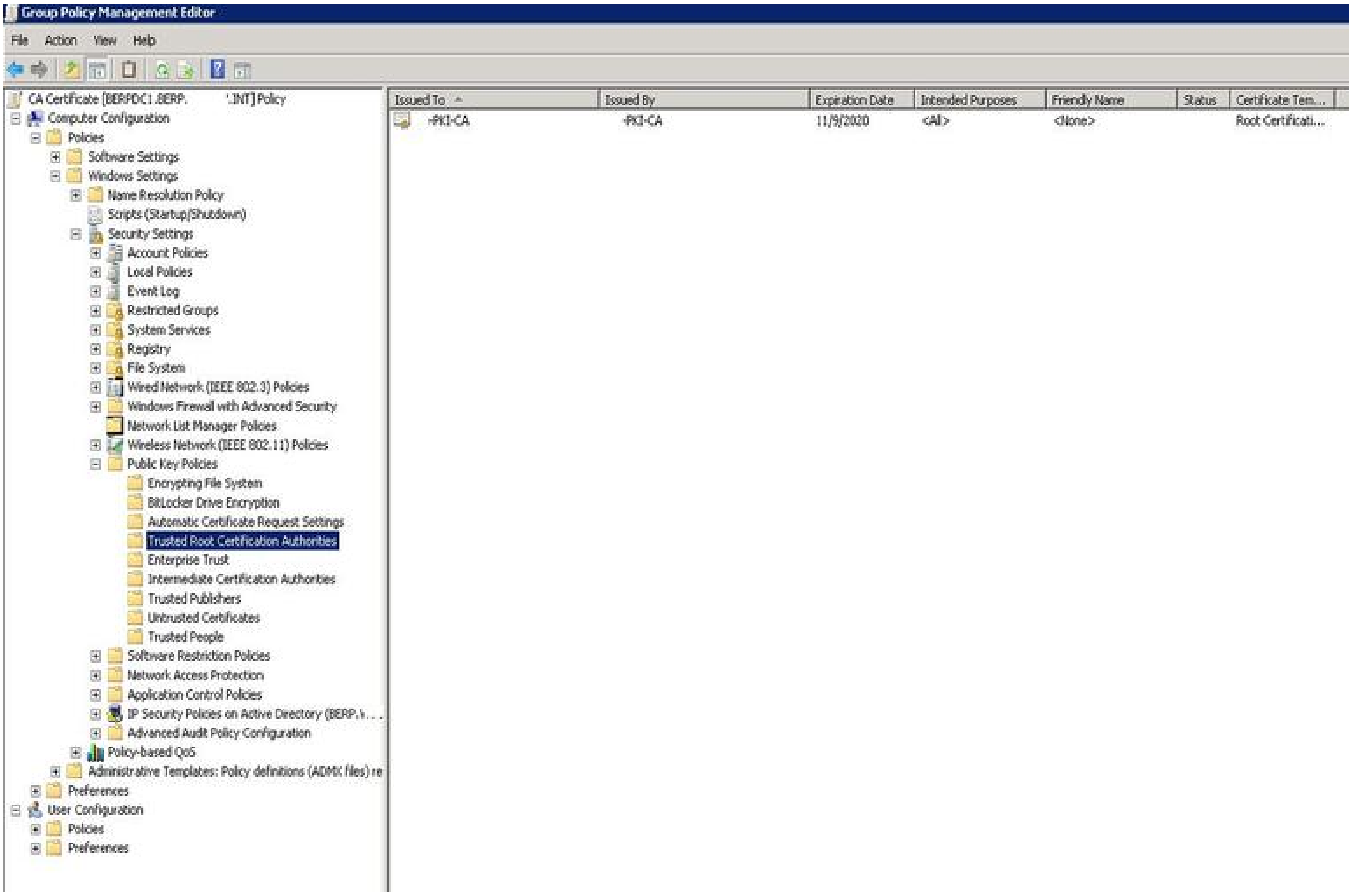
Click Next.

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

Click Next, click Finish, then click OK.

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

Figure M


Group Policy Management Editor
File Action View Help
CA Certificate [BERPDC1.BERP. '.INT] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
BitLocker Drive Encryption
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (BERP.\...
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) re
Preferences
User Configuration
Policies
Preferences

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
-PKI-CA	-PKI-CA	11/9/2020	<All>	<None>		Root Certificati...

If you're not running Active Directory in your organization, you can't leverage Group Policy, but you can manually add the CA certificate on a host to trust the related SSL certificates.

Note that you can add the certificate in Chrome, but it's advisable to add it in Windows itself, since that will cover other apps that might connect to the website.

SEE: IT pro's guide to effective patch management (https://www.techrepublic.com/resource-library/whitepapers/it-pro-s-guide-to-effective-patch-management/) (free TechRepublic PDF)

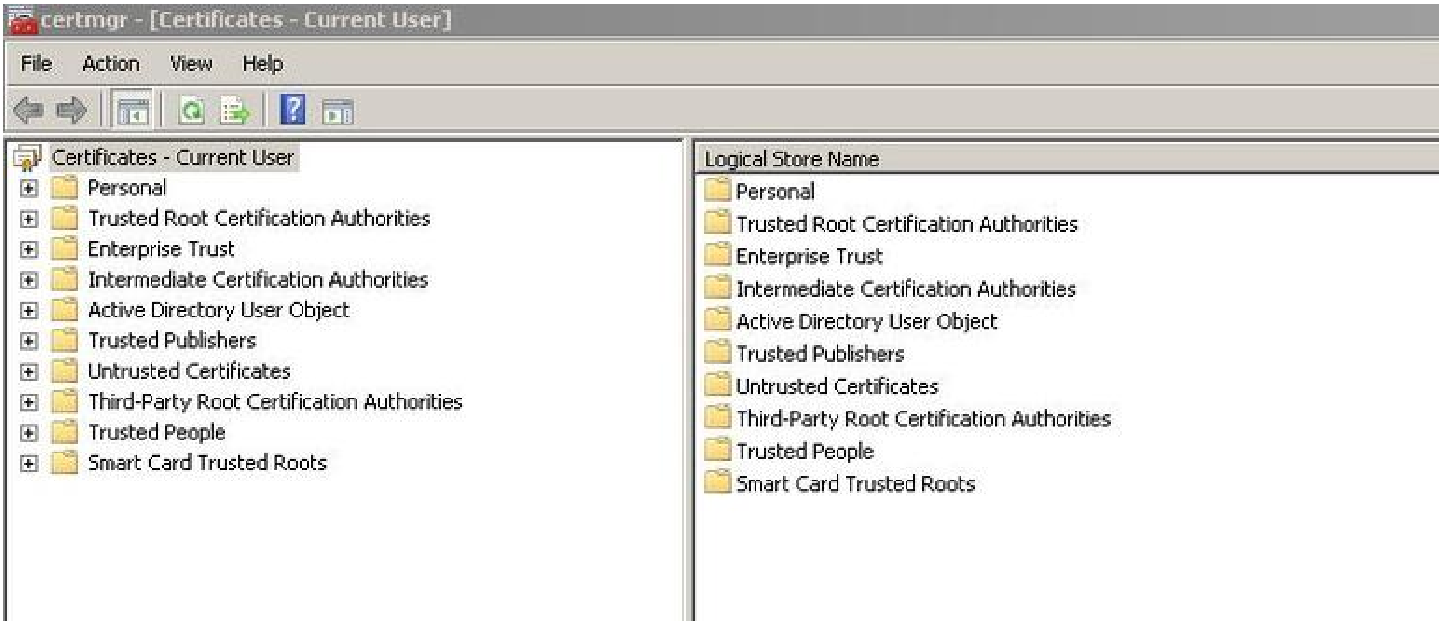
Manually configuring a Windows system to trust your CA

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 N**):

certmgr.msc

Figure N

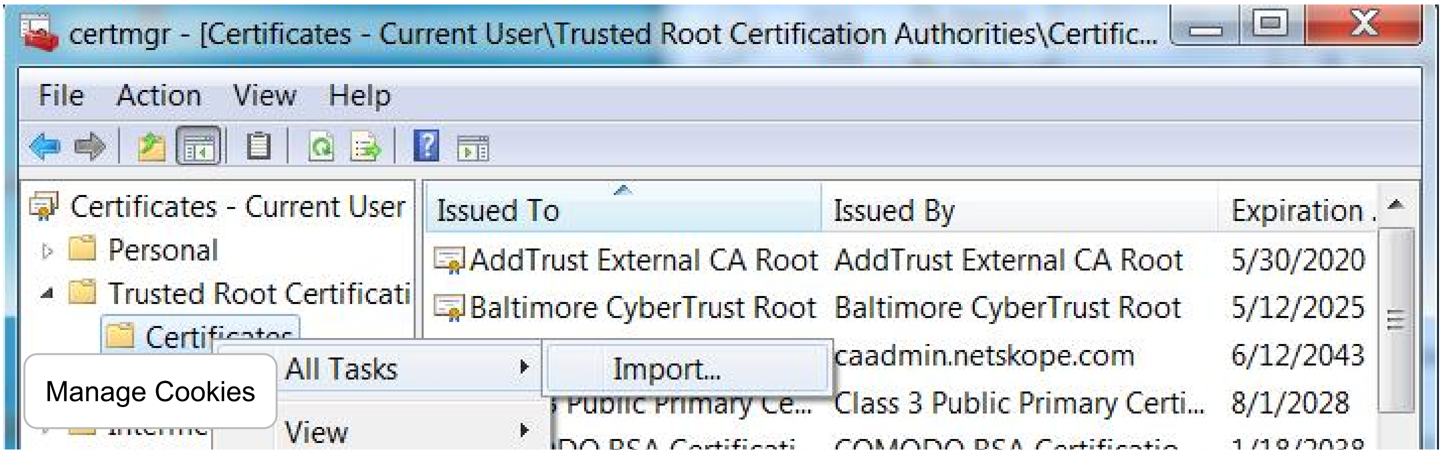


Certificates - Current User
- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Smart Card Trusted Roots

Logical Store Name
- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Smart Card Trusted Roots

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

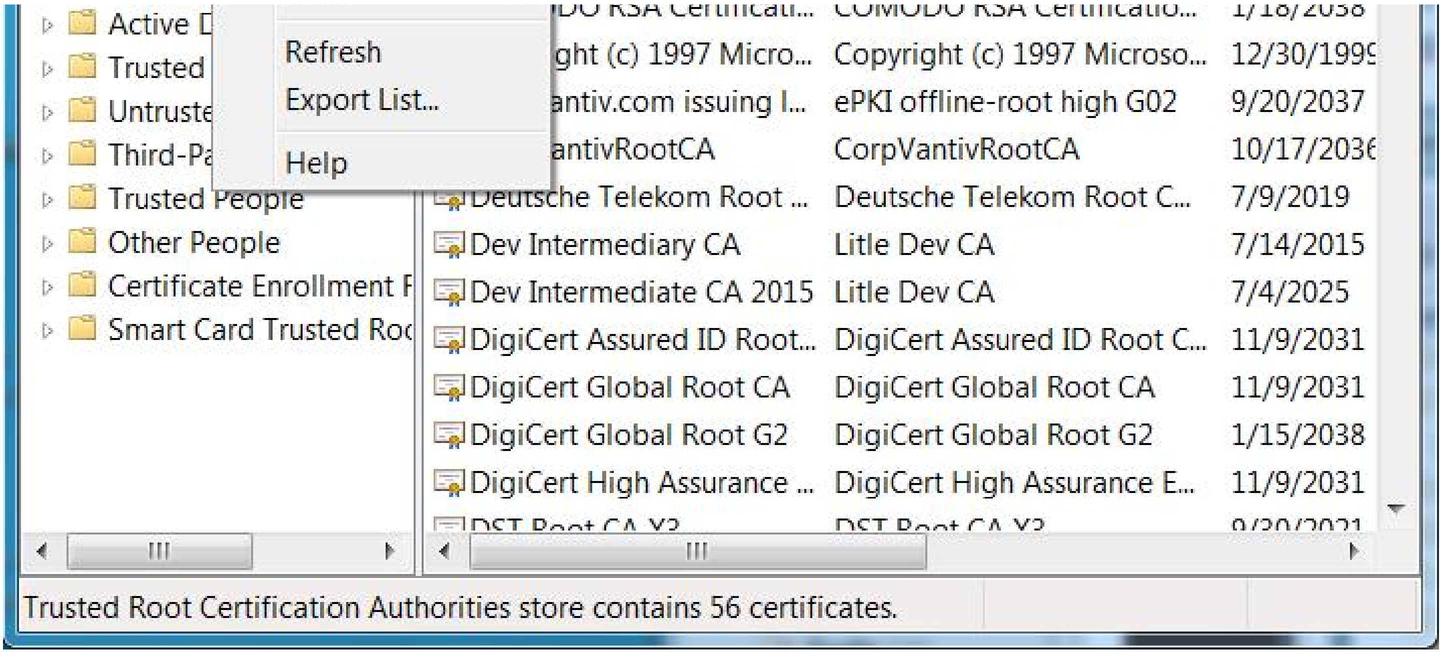
Figure O



certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certific...
File
Action
View
Help
All Tasks
Import...
View

Certificates - Current User
- Personal
- Trusted Root Certificati
  - Certificates

Issued To	Issued By	Expiration .
AddTrust External CA Root	AddTrust External CA Root	5/30/2020
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025
	caadmin.netskope.com	6/12/2043
Public Primary Ce...	Class 3 Public Primary Certi...	8/1/2028
DO RSA Certificati...	COMODO RSA Certificatio...	1/18/2038

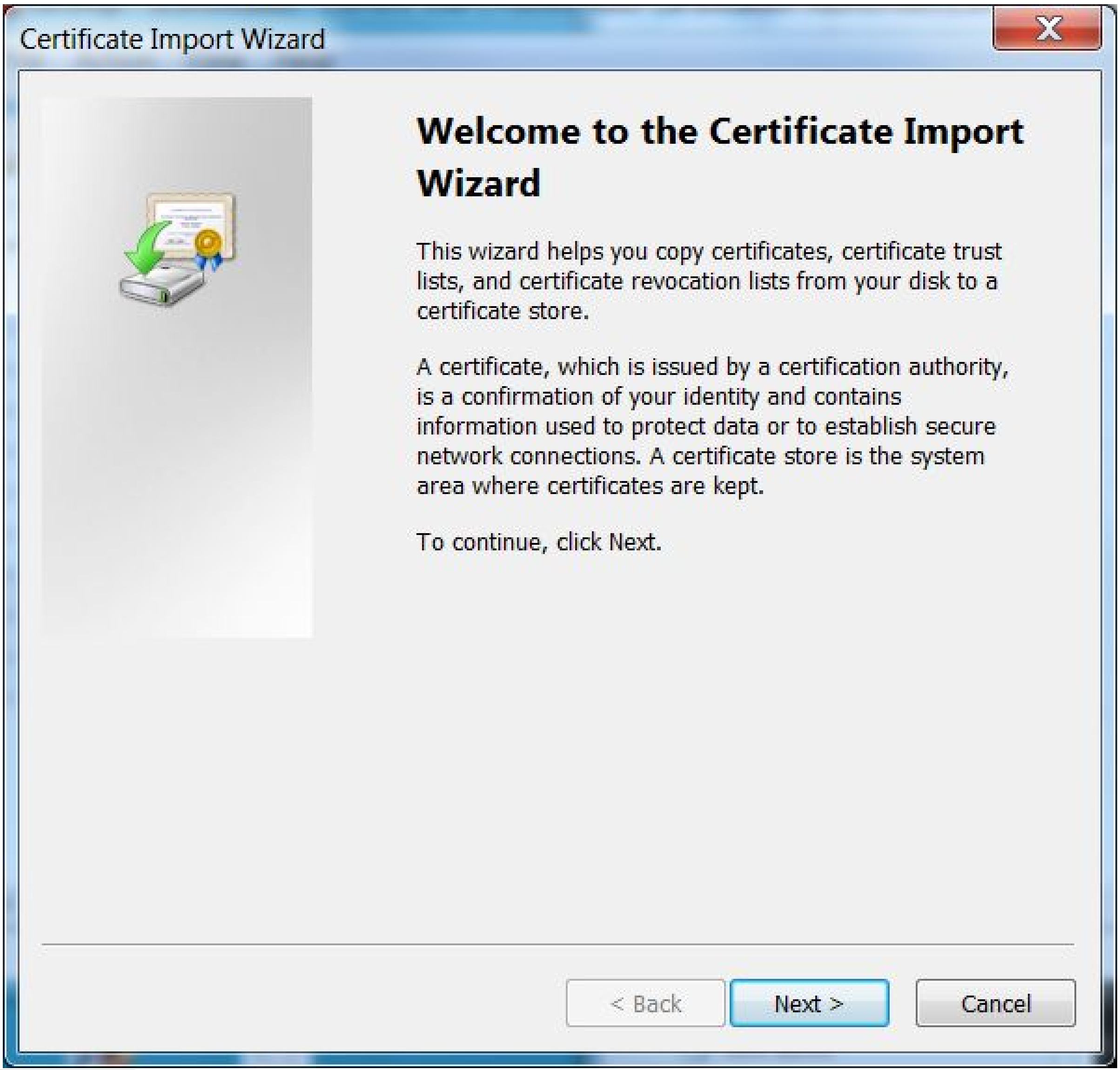


DO RSA Certificati...	COMODO RSA Certificatio...	1/18/2038
ght (c) 1997 Micro...	Copyright (c) 1997 Microso...	12/30/1999
antiv.com issuing I...	ePKI offline-root high G02	9/20/2037
antivRootCA	CorpVantivRootCA	10/17/2036
Deutsche Telekom Root ...	Deutsche Telekom Root C...	7/9/2019
Dev Intermediary CA	Litle Dev CA	7/14/2015
Dev Intermediate CA 2015	Litle Dev CA	7/4/2025
DigiCert Assured ID Root...	DigiCert Assured ID Root C...	11/9/2031
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038
DigiCert High Assurance ...	DigiCert High Assurance E...	11/9/2031
DST Root CA X3	DST Root CA X3	9/30/2021

Trusted Root Certification Authorities store contains 56 certificates.

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

Figure P



Welcome to the Certificate Import Wizard

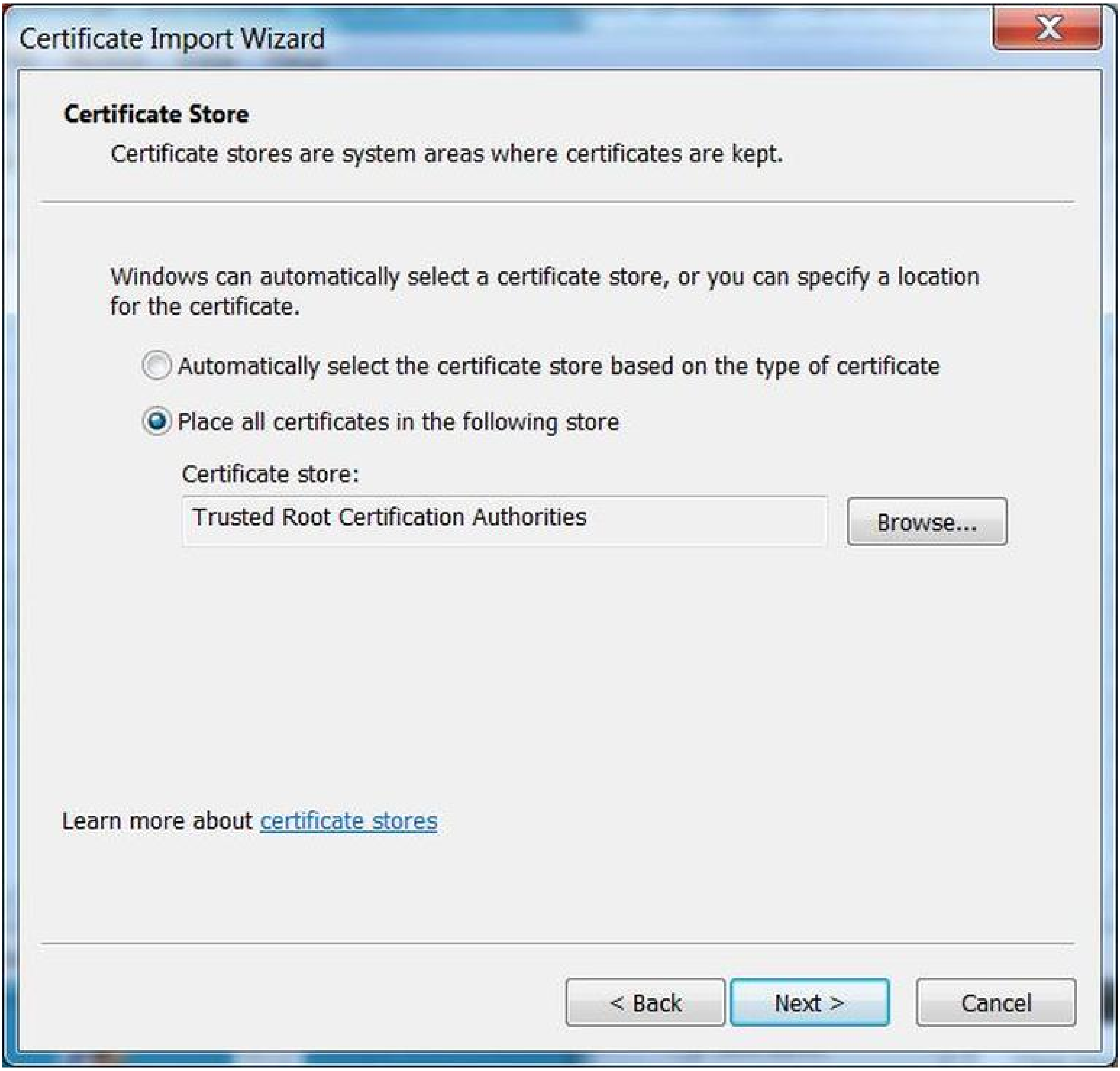
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Click Next, then click Browse, then browse to and select the CA certificate you copied to this computer (**Figure Q**).

Figure Q



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

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

Click Next, then click Finish.

Click Yes to any final prompt.

Adding the CA certificates as a Trusted Root Authority to Firefox

Manage Cookies

Unfortunately, Firefox does not trust the CA certificates that Windows does by default, so the instructions in the section above will work only if you perform this setting change in Firefox:

In Firefox, type *about:config* in the address bar.

If prompted, accept any warnings.

Scroll down to the security.enterprise_roots.enabled entry, which should be set to False.

Double-click the value to change it to True.

Firefox should enact the setting immediately.

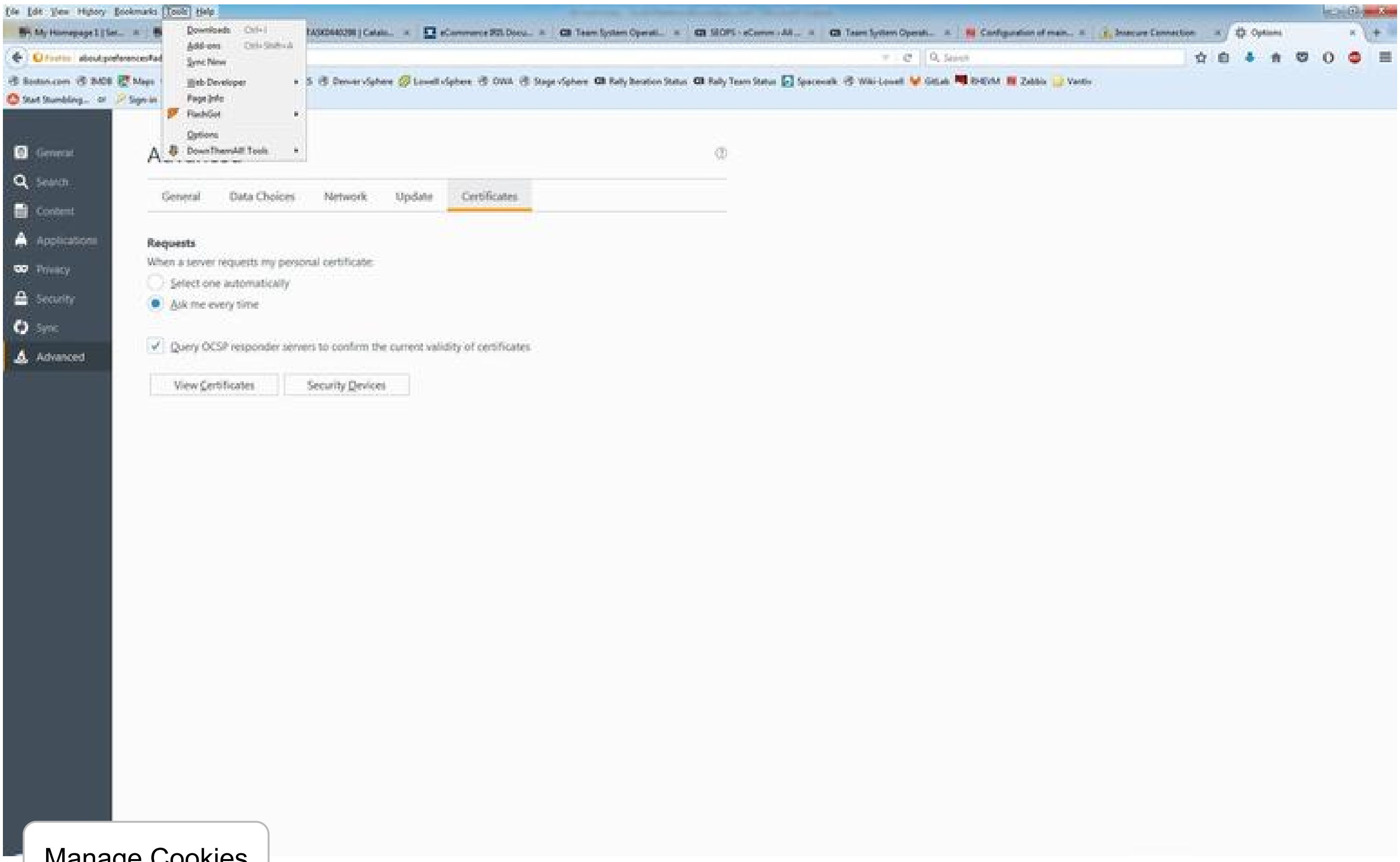
If you aren't using Active Directory/Group Policy, you can still configure Firefox to trust your CA.

Manually configuring Firefox to trust your CA

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

Click Tools (**Figure R**).

Figure R



General | Data Choices | Network | Update | Certificates

Requests

When a server requests my personal certificate:

○ Select one automatically

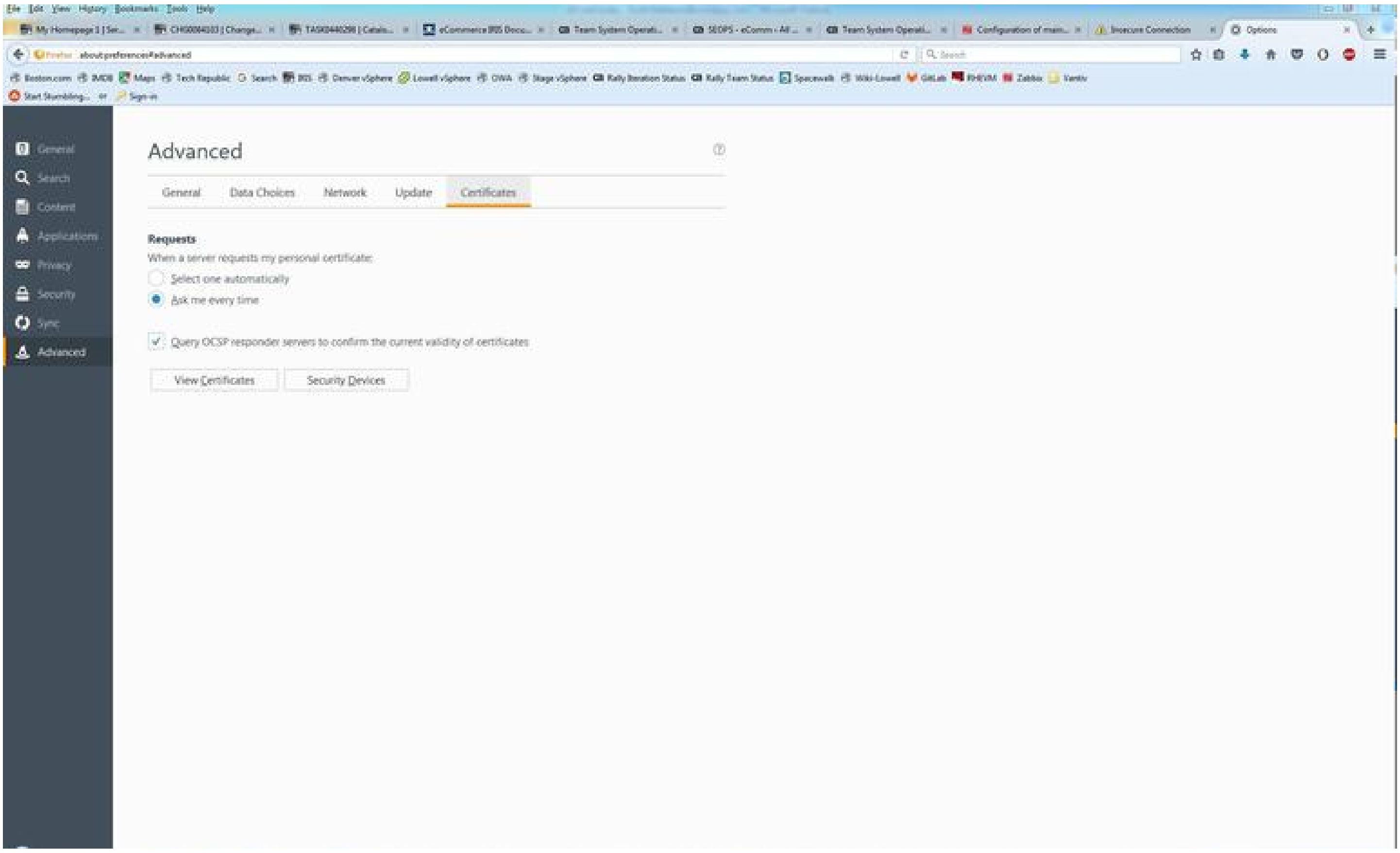
● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

View Certificates | Security Devices

Choose Options and click Advanced, then select the Certificates tab (**Figure S**).

Figure S



Advanced

Requests

When a server requests my personal certificate:

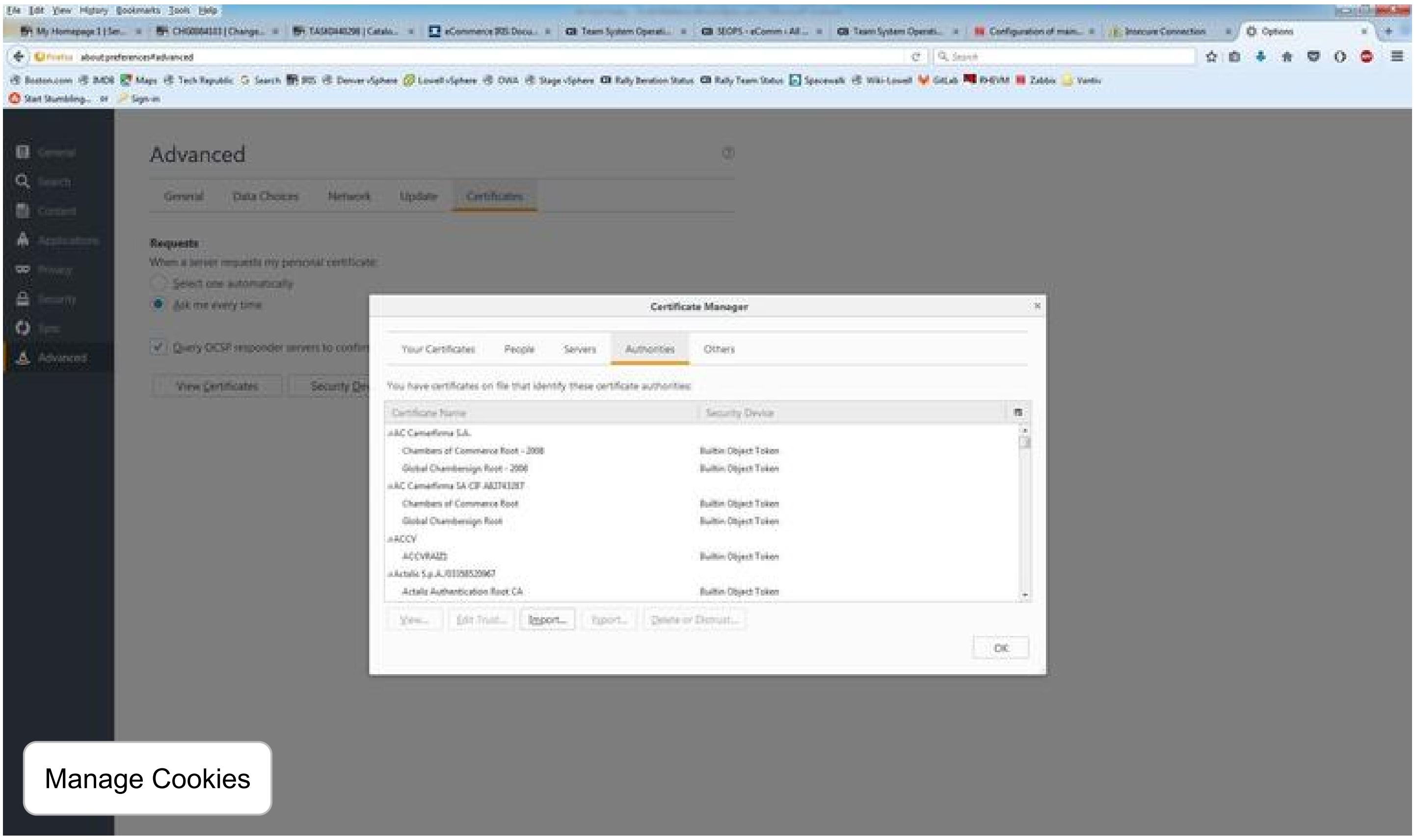
○ Select one automatically

● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

Click View Certificates, then select Authorities (**Figure T**).

Figure T

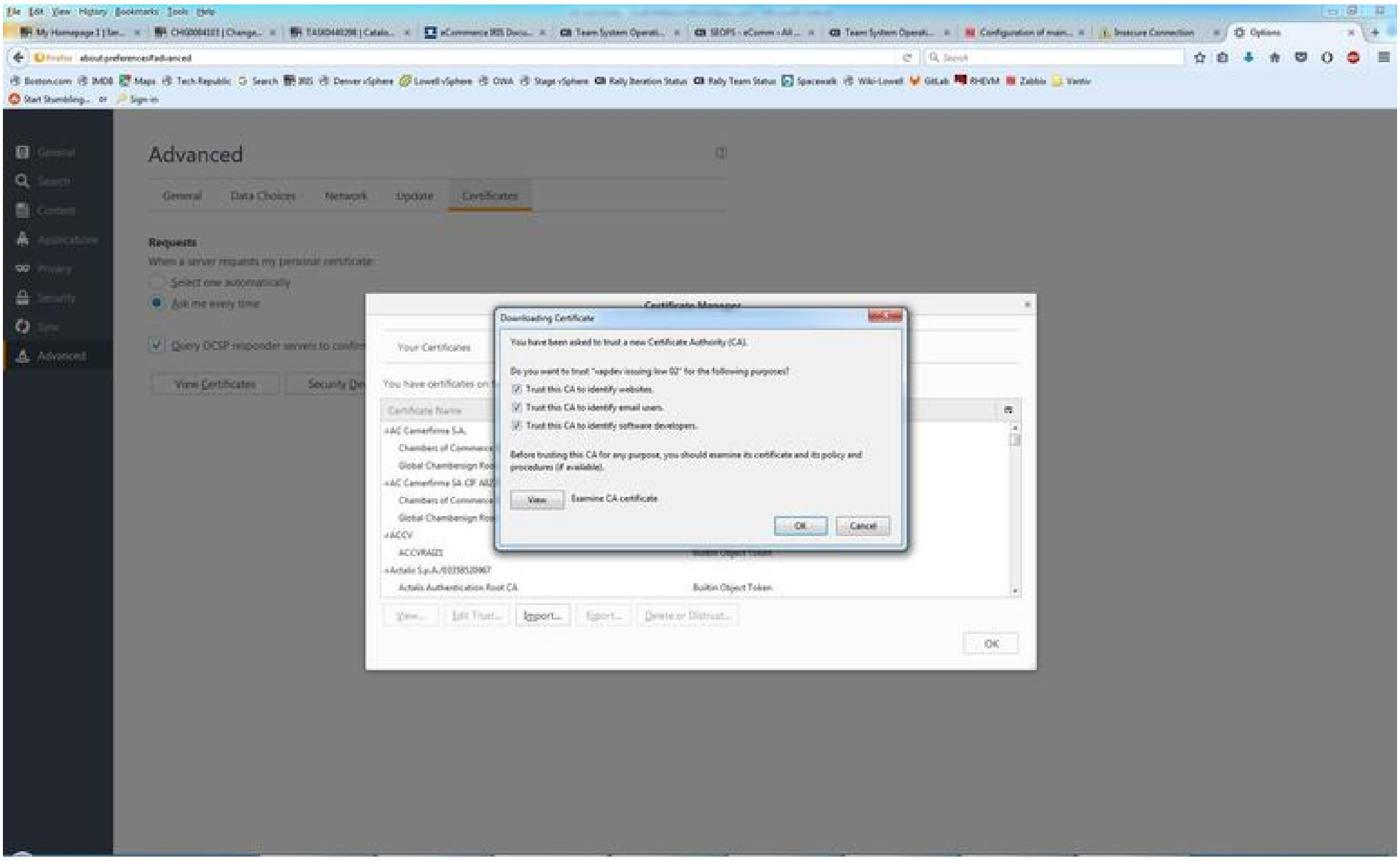


You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
⌄AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⌄AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
⌄ACCV	
ACCVRAIZ1	Builtin Object Token
⌄Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token

Click Import, then browse to your CA file and select it (**Figure U**).

Figure U



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "vapdev issuing low 02" for the following purposes?

☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

☑ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

Check off all the Trust This CA options as shown above, then click OK.

Firefox should now trust the certificate authorities and stop providing security warnings.

Also read....

- Why Google Chrome will label thousands of websites as "unsafe" in the next few months (https://www.techrepublic.com/article/why-google-chrome-will-label-thousands-of-websites-as-unsafe-in-the-next-few-months/)(TechRepublic)
- Why your company should consider implementing DNS security extensions (https://www.techrepublic.com/article/why-your-company-should-consider-implementing-dns-security-extensions/) (TechRepublic)
- Let's Encrypt brings free wildcard certificates to the web (http://www.zdnet.com/article/lets-
Manage Cookies
dcard-certificates-to-the-web/) (ZDNet)

- Rampant spam, falling registrations show new gTLDs have limited business value (https://www.techrepublic.com/article/rampant-spam-falling-registrations-show-new-gtlds-have-limited-business-value/) (TechRepublic)

Your thoughts

Have you applied any of these techniques to add a trusted CA to Chrome and Firefox? Share your advice and experiences with fellow TechRepublic members.

EDITOR'S PICKS

Transgender employees in tech: Why this "progressive" industry has more work to do

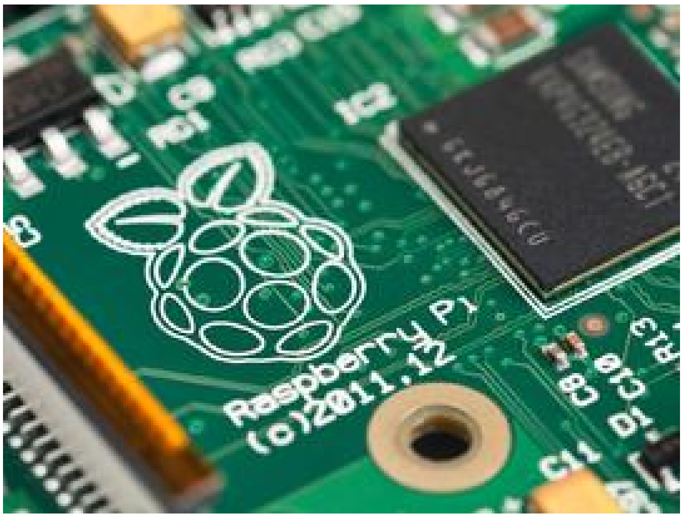
Python is eating the world: How one developer's side project became the hottest programming language on the planet

Manage Cookies

How iRobot used data science, cloud, and DevOps to design its next-gen smart home robots

Beyond the PC: Lenovo's ambitious plan for the future of computing

Straight up: How the Kentucky bourbon industry is going high tech



Inside the Raspberry Pi: The story of the $35 computer that changed the world

By Scott Matteson

Scott Matteson is a senior systems administrator and freelance technical writer who also performs consulting work for small organizations. He resides in the Greater Boston area with his wife and three children.

SECURITY SOFTWARE CXO HARDWARE MOBILITY DATA CENTERS CLOUD

SECURITY ON ZDNET

How to use God Mode in Windows 10

11 popular IT certifications that make the most money

Python: Where to learn it and why you should do it now

SHOW COMMENTS

EDITOR'S PICKS

Manage Cookies

Transgender employees in tech: Why this "progressive" industry has more work to do

Python is eating the world: How one developer's side project became the hottest programming language on the planet

How iRobot used data science, cloud, and DevOps to design its next-gen smart home robots

Beyond the PC: Lenovo's ambitious plan for the future of computing