March 11, 2024

Updating List of Trusted Root Certificates in Windows

All Windows versions have a built-in feature for automatically updating root certificates from the Microsoft websites. MSFT, as part of the **Microsoft Trusted Root Certificate Program**, maintains and publishes a list of trusted certificates for clients and Windows devices in its online repository. If the verified certificate in its certification chain refers to the root CA that participates in this program, the system will automatically download this root certificate from the Windows Update servers and add it to the trusted ones.

> Windows updates a trusted root certificate list (CTL) once a week. If Windows doesn't have direct access to the Windows Update, the system won't be able to update the root certificates. So a user may have some troubles when browsing websites (which SSL certificates are signed by an untrusted CA – see the article about the "Chrome SSL error: This site can't provide a secure connection"), or with installing/running signed scripts and apps.

In this article, we'll try to find out how to manually update the list of root certificates in TrustedRootCA in disconnected (isolated) networks or computers/servers without direct Internet access.

Contents:

> **Note.** If your computers access the Internet through a proxy server, Microsoft recommends that you open direct access (bypass) to Microsoft Web sites to automatically renew root certificates. However, it isn't always possible or applicable due to corporate restrictions.

Managing Trusted Root Certificates in Windows 10 and 11

1. To open the root certificate store of a computer running Windows 11, 10, 8.1, or Windows Server 2022, 2019, 2016, run the **mmc.exe** console;
2. Select **File** -> **Add/Remove Snap-in**, select **Certificates** (certmgr) in the list of snap-ins -> **Add**;
3. Select that you want to manage certificates of local **Computer account**;
4. Next -> OK -> OK;
5. Expand the **Certificates** node -> **Trusted Root Certification Authorities Store.** This section contains the list of trusted root certificates on your computer.

In the mmc console, you can view information about any certificate or remove it from trusted ones.

You can also get a list of trusted root certificates with their expiration dates using PowerShell:

```
Get-Childitem cert:\LocalMachine\root |format-list
```

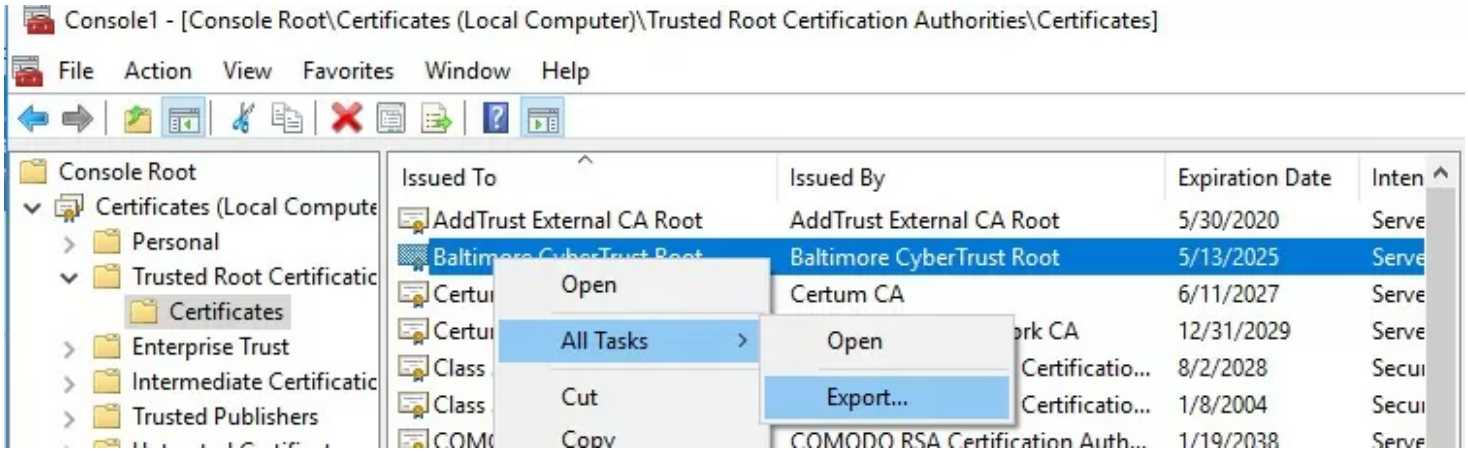
You can list the expired certificates, or which expire in the next 60 days:

```
Get-ChildItem cert:\LocalMachine\root|Where {$_.NotAfter -lt  (Get-Date).AddDays(60)}|select NotAfter, Subject
```

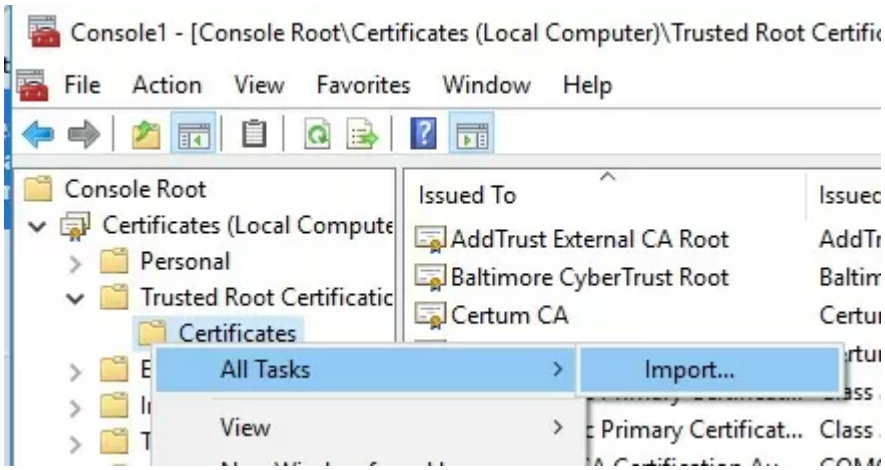
> For security reasons, it's recommended that you periodically check the certificate trust store on your computer for suspicious and revoked certificates using the **Sigcheck** tool. This tool allows you to compare the list of certificates installed on the computer with the list of root certificates on the Microsoft website (you can download an offline file with up-to-date certificates authrootstl.cab).

You can manually transfer the root certificate file between Windows computers using the Export/Import options.

1. You can export any certificate to a .CER file by clicking on it and selecting All Tasks -> Export;



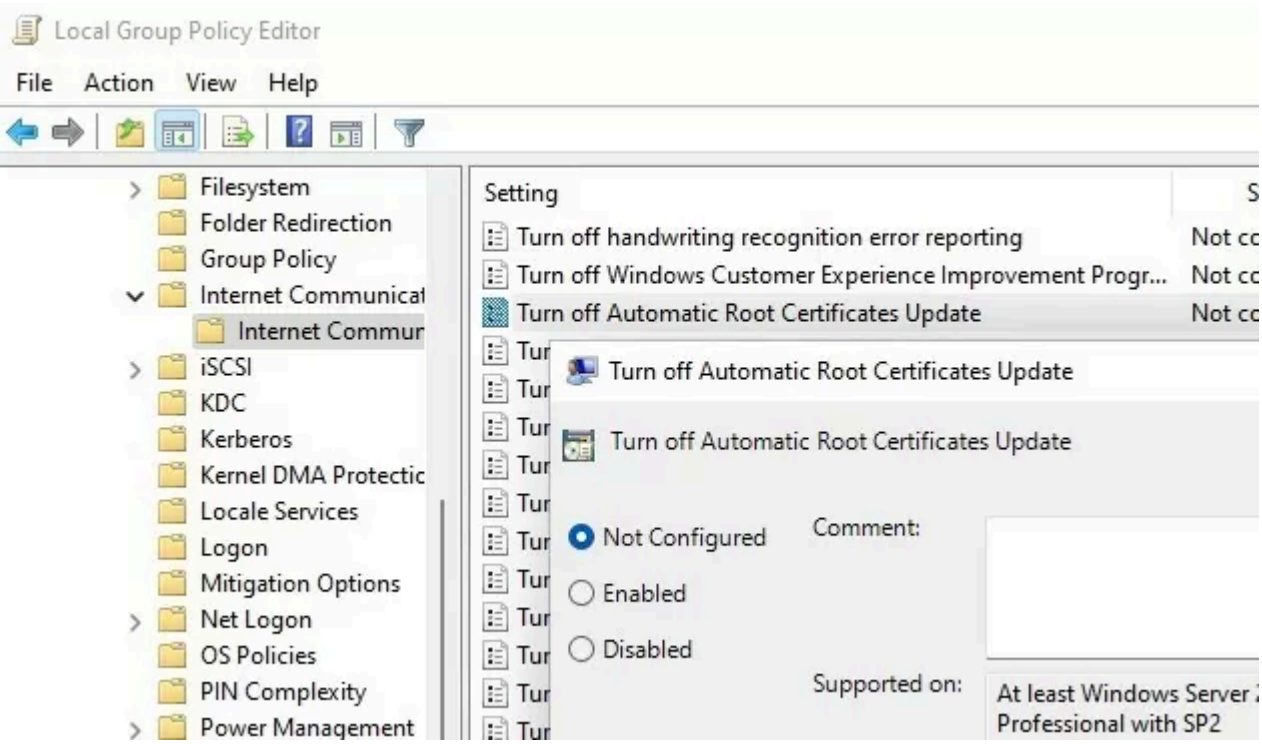
2. You can import this certificate on another computer using the option All Tasks -> Import.



How to Disable/Enable Automatic Root Certificates Update in Windows?

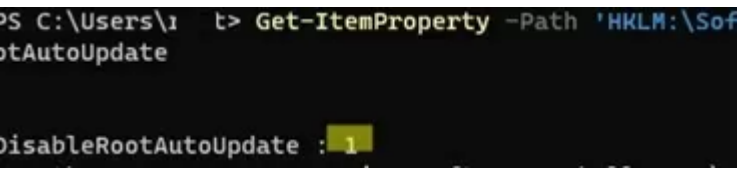
As we mentioned, Windows automatically updates root certificates. You can enable or disable certificate renewal in Windows through a GPO or the registry.

The **Turn off Automatic Root Certificates Update** option in this section allows you to disable automatic updating of root certificates through the Windows Update sites. By default, this policy is not configured and Windows always tries to automatically renew root certificates.



If this GPO option is not configured and the root certificates are not automatically renewed, check if this setting is manually enabled in the registry. Check the value of the registry parameter using PowerShell:

```
Get-ItemProperty -Path 'HKLM:\Software\Policies\Microsoft\SystemCertificates\AuthRoot' -Name DisableRootAutoUpdate
```



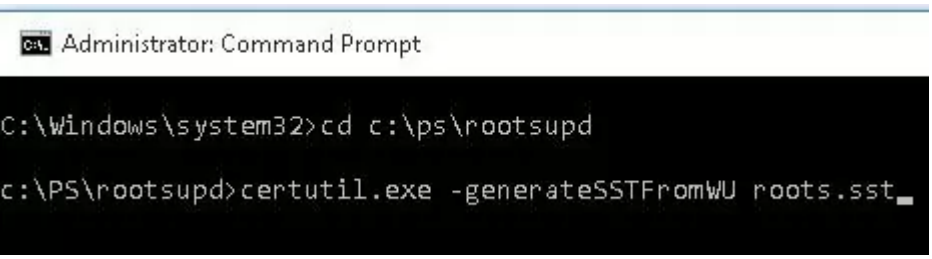
If the command returns that the value of the **DisableRootAutoUpdate** registry parameter is **1**, then the updating of root certificates is disabled on your computer. To enable it, change the parameter value to 0.

Certutil: Download Trusted Root Certificates from Windows Update

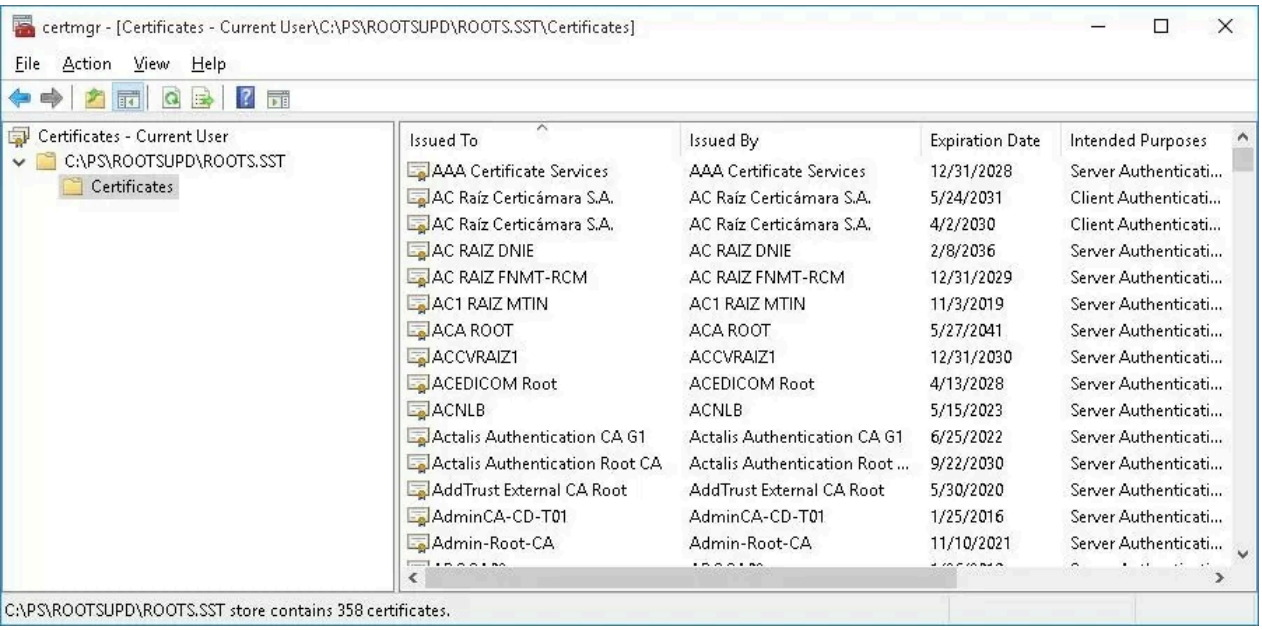
Certutil.exe CLI tool can be used to manage certificates (introduced in Windows 10, for Windows 7 is available as a separate update). It can be used to download an up-to-date list of root certificates from Windows Update and save it to an SST file.

To generate an SST file on a computer running Windows 10 or 11 and having direct access to the Internet, open the elevated command prompt and run the command:

```
certutil.exe -generateSSTFromWU C:\PS\roots.sst
```



As a result, an SST file containing an up-to-date list of root certificates will appear in the target directory. Double-click to open it. This file is a container containing trusted root certificates.



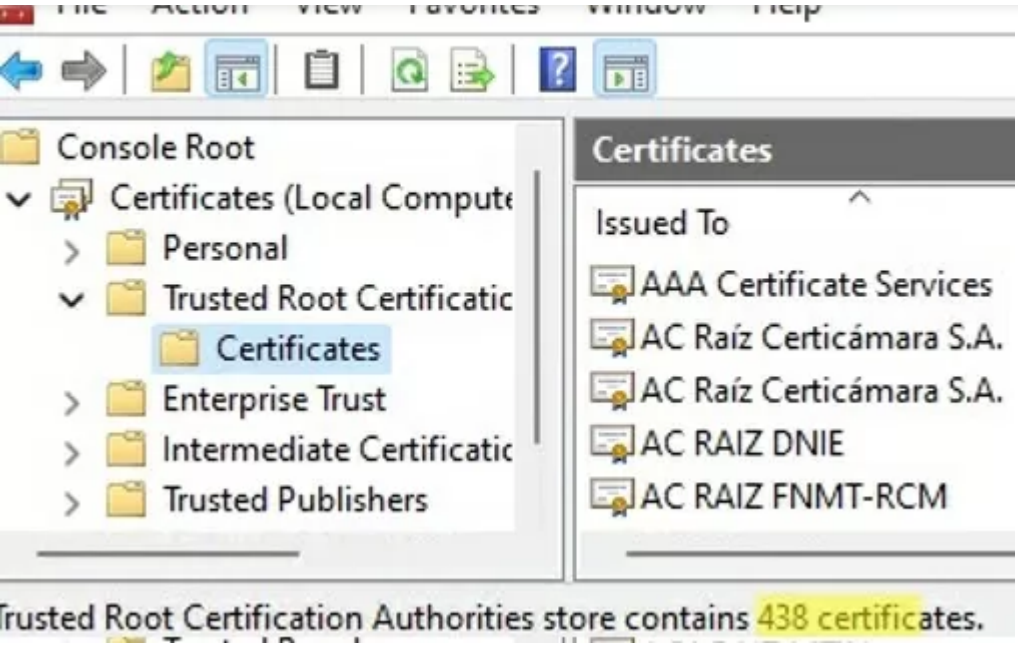
As you can see, a familiar Certificate Management snap-in opens, from which you can export any of the certificates you have got. In my case, there have been 358 items in the list of certificates. Obviously, it is not rational to export the certificates and install them one by one.

> **Tip**. The `certutil -syncWithWU` command can be used to generate individual certificate files. The certificates obtained in this way can be deployed to Windows devices using GPO.

You can use PowerShell script to install all certificates from the SST file and add them to the list of trusted root certificates on a computer:

```
$sstStore = ( Get-ChildItem -Path C:\ps\rootsupd\roots.sst )
$sstStore | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root
```

Run the **certmgr.msc** snap-in and make sure that all certificates have been added to the **Trusted Root Certification Authority**. In my example on Windows 11, the number of root certificates increased from 34 to 438.



> A clean copy of Windows after installation contains only a small number of certificates in the root store. If the computer is connected to the Internet, the rest of the root certificates will be installed automatically (on demand) if your device access an HTTPS site or SSL certificate that has a fingerprint from Microsoft CTL in its trust chain. Therefore, as a rule, there is no need to immediately add all certificates that Microsoft trusts to the local certification store.

Certificate Trust List (STL) in Windows

A **Certificate Trust List** (**CTL**) is simply a list of data (such as certificate hashes) that is signed by a trusted party (by Microsoft in this case). The Windows client periodically downloads from Windows Update this CTL, which stores the hashes of all trusted root CAs. It should be understood that this CTL doesn't contain the certificates themselves, only their hashes and attributes (for example, Friendly Name). Windows devices can download a trusted certificate from Certificate Trust List on demand.

You can manually download and install the CTL file. To do it, download the file http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab (updated twice a month). Using any archiver (or even Windows Explorer), unpack the contents of the **authrootstl.cab** archive. It contains a single **authroot.stl** file.

The Authroot.stl file is a container with a list of trusted certificate thumbprints in Certificate Trust List format.

You can install this CTL file to a Trusted Root Certificate Authority using the certutil command:

```
certutil -enterprise -f -v -AddStore "Root" "C:\PS\authroot.stl"
```

```
root "Trusted Root Certification Authorities"
CTL 0 added to store.
CertUtil: -addstore command completed successfully.
```

You can also import certificates using the certificate management console (**Trust Root Certification Authorities** -> **Certificates** -> **All Tasks** -> **Import**). Specify the path to your STL file with certificate thumbprints.

After you have run the command, a new section Certificate Trust List appears in **Trusted Root Certification Authorities** container of the Certificate Manager console (`certmgr.msc`).

In the same way, you can download and install the list of the revoked (disallowed) certificates that have been removed from the Root Certificate Program. To do it, download the **disallowedcertstl.cab** file (http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab), extract it, and add it to the Untrusted Certificates store with the command:

```
certutil -enterprise -f -v -AddStore disallowed "C:\PS\disallowedcert.stl"
```

Updating Trusted Root Certificates via GPO in an Isolated Environment

If you have the task of regularly updating root certificates in an Internet-isolated Active Directory domain, there is a slightly more complicated scheme for updating local certificate stores on domain-joined computers using Group Policies. You can configure root certificate updates on user computers in the disconnected Windows networks in several ways.

The first way assumes that you regularly manually download and copy a file with root certificates to your isolated network. You can download the file with current Microsoft root certificates as follows:

```
$sstStore = (Get-ChildItem -Path \\fr-dc01\SYSVOL\woshub.com\rootcert\roots.sst )
$sstStore | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root
```

The second way is to download the actual Microsoft root certificates using the command:

```
Certutil -syncWithWU -f \\fr-dc01\SYSVOL\woshub.com\rootcert\
```

A number of root certificate files (CRT file format) will appear in the specified shared network folder (including files authrootstl.cab, disallowedcertstl.cab, disallowedcert.sst, thumbprint.crt).

Then use the Group Policy Preferences to change the value of the registry parameter **RootDirURL** under **HKLM\Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate**. This parameter should point to the shared network folder from which your Windows computers will receive new root certificates. Run the domain GPMC.msc console, create a new GPO, switch to the edit policy mode, and expand the section **Computer Configuration -> Preferences -> Windows Settings -> Registry**. Create a new registry property with the following settings:

- **Action**: Update
- **Hive**: HKLM
- **Key path**: Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate
- **Value name**: RootDirURL
- **Type**: REG_SZ
- **Value data**: file://\\fr-dc01\SYSVOL\woshub.com\rootcert\

It remains to link this policy on a computer`s OU and after updating GPO settings on the client, check for new root certificates in the certstore.

> The GPO parameter **Turn off Automatic Root Certificates Update** under Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings should be disabled or not configured.

How to Update Trusted Root Certificates in Windows 7?

Despite the fact that Windows 7 is now is at the End of Support phase, many users and companies still use it.

After installing a clean Windows 7 image, you may find that many modern programs and tools do not work on it as they are signed with new certificates. In particular, there have been complaints that .Net Framework 4.8 or Microsoft Visual Studio (vs_Community.exe) cannot be installed on Windows 7 SP1 x64 without updating root certificates.

```
The installer manifest failed signature validation.
```

Or

```
NET Framework has not been installed because a certificate chain could not be built to a trusted root authority.
```

To update root certificates in Windows 7, you must first download and install MSU update **KB2813430** (https://support.microsoft.com/en-us/topic/an-update-is-available-that-enables-administrators-to-update-trusted-and-disallowed-ctls-in-disconnected-environments-in-windows-0c51c702-fdcc-f6be-7089-4585fad729d6)

After that, you can use the certutil to generate an SST file with root certificates (on current or another computer):

```
certutil.exe -generateSSTFromWU c:\ps\roots.sst
```

Now you can import certificates into trusted ones:

Run **MMC** -> add snap-in -> certificates -> computer account > local computer. Right click Trusted root certification authority, All Tasks -> Import, find your SST file (in the file type select **Microsoft Serialized Certificate Store — *.sst**) -> Open -> Place all certificates in the following store -> Trusted Root Certification Authorities.

Updating Root Certificates on Windows XP Using the Rootsupd.exe Tool

In Windows XP, the **rootsupd.exe** utility was used to update the computer`s root certificates. The list of root and revoked certificates in it was regularly updated. The tool was distributed as a separate update **KB931125** (Update for Root Certificates). Let's see if we can use it now.

1. Download the **rootsupd.exe** utility using the following link ~~http://download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/rootsupd.exe~~. At the moment (January 2021) the link doesn't work, Microsoft decided to remove it from the public. Today you can download the rootsupd.exe from the Kaspersky website — http://media.kaspersky.com/utilities/CorporateUtilities/rootsupd.zip;
2. To install the Windows root certificates, just run the **rootsupd.exe** file. But we will try to examine its contents more carefully. Extract the certificates from the executable file with the command: `rootsupd.exe /c /t: C:\PS\rootsupd`

```
updroots.exe authroots.sst
updroots.exe -d delroots.sst
```

However, as you can see, these certificate files were created on April 4, 2013 (almost a year before the end of official support for Windows XP). Thus, since then the tool has not been updated and cannot be used to install up-to-date certificates.

But you can use cerutil tool in Windows 10/11 to download root.sst, copy that file in Windows XP and install the certificate using updroots.exe:

```
updroots.exe c:\temp\roots.sst
```

> There is information that the updroots.exe tool is not recommended for use in modern builds of Windows 10 1803+ and Windows 11, as it can break the Microsoft root CA on a device.

In this article, we looked at several ways to update trusted root certificates on Windows network computers that are isolated from the Internet (disconnected environment).

Group Policies Windows 10 Windows 11 Windows Server 2019

previous post
How to Extend Office 2021/2019/2016 & Office 365 Trial Period

next post
Forwarding Emails to an External Address in Microsoft 365 (Exchange Online)

RELATED READING

How to Repair EFI/GPT Bootloader on Windows 10...
March 16, 2024

How to Restore Deleted EFI System Partition in...
March 11, 2024

Wi-Fi (Internet) Disconnects After Sleep or Hibernation on...
March 15, 2024

46 COMMENTS

YUE YAO

Reply

August 22, 2017 - 3:26 pm

thanks for the very good article. And further what about using Powershell Import/Export-certificate ?

ADMIN

Reply

August 30, 2017 - 4:55 am

PoSh PKI module is available only since Windows Server 2012/ Win 8. To export all certs from trusted root certificate authorities on Windows machine on Windows 2008 r2/ Win 7 to the files you can use this script:

```
$type = [System.Security.Cryptography.X509Certificates.X509ContentType]::Cert
$certs = get-childitem -path cert:\LocalMachine\AuthRoot
foreach($cert in $certs)
{
$hsh = $cert.GetCertHashString()
$path = "c:\certs\" + $hsh + ".der"
[System.IO.File]::WriteAllBytes($path, $cert.export($type) )
}
```

SEBUS

Reply

November 14, 2017 - 11:45 am

1. Install CTL does not exist as Context menu in Windows 10
2. certutil -addstore -f root authroot.stl

works OK, but then Microsoft Certificate Trust List Publisher shows error: "This certificate trust list is not valid. The certificate that signed the list is not valid

---

ADMIN

Reply

November 17, 2017 - 5:26 am

Apparently in your case, it's easiest way to download the certificates from WU using the command:

```
certutil.exe -generateSSTFromWU roots.sst
```

Then you can import them using Import-Certificate cmdlet:

```
$sst = ( Get-ChildItem -Path C:\certs\roots.sst )
$sst| Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root
```

SEBUS

R

Still would like to understand where the error comes from & why…

STEVE Reply

December 10, 2018 - 6:45 pm

Thank you! Reading how to do this on the MS site was pure obfuscation. Your method is so simple and 1/30th the size of MS completly useless article on doing the same.

COWLINATOR Reply

January 24, 2019 - 11:26 pm

Why would you post a url for root certificates from Microsoft over standard insecure http?

WALT Reply

August 23, 2019 - 5:07 pm

I was having trouble with this one as well until I realized that if you're downloading certificates you might not get the HTTPS to establish without the certificates you need to download…
Would be nice if it was available via both HTTP and HTTPS though. My end user devices are behind a firewall that disallows HTTP but they can get to any HTTPS.

TIM DE VRIES Reply

November 13, 2019 - 5:41 am

A lot of it is the redistribution licenses are tougher to get through than just hosting a verified file by https. But yeah, doesn't make tons of sense.

THOUGHTS Reply

April 10, 2019 - 3:36 pm

Do you need disallowedcert.sst if you have disallowedcert.stl? Are they the same?

ADMIN Reply

April 15, 2019 - 11:42 am

Sst and stl are two different file formats for transferring root certificates between computers. It is better to use disallowedcert.sst.

WALT Reply

August 23, 2019 - 5:08 pm

GLNZ

Reply

May 2, 2019 - 11:46 pm

THREE things:
FIRST, on my Win 10 Pro 64-bit machine (version 1803), the ONLY .sst file I have is
Connected Devices Platform certificates.sst
in
C:\Users\[My Name]\AppData\Local\ConnectedDevicesPlatform
►Is that correct?
SECOND, after running certmgr.msc, I see a few lists of certificates, in which the two certificates that are issue BY my own computer TO my own computer are actually expired. What are they?
THIRD, which is how I found this excellent website, I am getting two to four AUDIT FAILURES on every reboot, Event 5061, for Cryptographic Operation, and they sometimes mention the same Microsoft Connected Devices Platform.
I have posted about these AUDIT FAILURES in detail at the following thread in technet – please go there to suggest answers:
https://social.technet.microsoft.com/Forums/windows/en-US/48425e2a-54c2-480d-8957-383415be2381/audit-failures-every-reboot-event-5061-cryptographic-operation-win-10-pro-64bit?forum=win10itprosetup

I have also received a possibly good hint at this link ABOUT CERTIFICATES POSSIBLY BEING RELATED but need more info:
https://social.technet.microsoft.com/Forums/windows/en-US/3e88df37-d718-4b1f-ac90-e06b597c0359/event-5061-audit-failures-every-reboot-cryptography-win-10-pro-64bit?forum=win10itprogeneral

WOuld appreciate your help – thanks.

A HAPPY VISITOR

Reply

August 5, 2019 - 4:23 pm

Steam wasn't working properly for me. Impossible to connect to the friend list. I had to run it in no-browser mode.
Then a video game (BDO) was failing at start: the DRM system couldn't connect to endpoint.
Then another game was failing with no reason. No meaningful error message, no log.
And then I've check my certificates, noticed some were outdated, and found your post about how to do it. Guess what? Everything is fixed now. From Steam itself to other application issues. Thanks a lot!

WALT

Reply

October 1, 2019 - 6:29 pm

This is very helpful, but it's also a bit confusing about the authroot.stl file.

You need to get the actual certificates onto your device, which there seem to be many ways of accomplishing (and none that I've settled on yet.)
Anyhow, thanks for the info, and you might want to add some clarity around that.

TZATZ Reply

November 29, 2019 - 2:43 pm

Warning quote
"The rootsupd.exe (and the updroots.exe inside of it) are outdated and should not be used. In fact, they break the "Microsoft Root Certificate Authority" root certificate on modern systems (at least Windows 10 1803+). – Koraktor Jan 9 at 12:34"
Src: https://serverfault.com/questions/760874/get-the-latest-ctl-or-list-of-trusted-root-certificates#

LOHMAR ASHAR Reply

February 26, 2020 - 10:15 pm

I've used the "`certutil.exe -generateSSTFromWU d:\roots.sst"` command to get what I was thinking to be an updated list of ROOT CA certificates, but when I've loaded the file and checked I can still see some expired ROOT CAs … should it be that way ? is it safe to keep them ? is it safe to delete them ?

MIKI Reply

March 29, 2020 - 7:35 am

I've windows 7 but when i use the -generateSSTFromWU command, the certutil utility return an error and say that the command doesn't exist. Guess is valied only for win 10.
Can you please add the correct command to retrieve the certificates but for windows 7 x64?
Downloading the cab with the etl certificates and add them manually have no effect, my system said that the operation was succesfull executed but if i open the mmc console i still have the old one and nothing is added.
Thank you.
ps: Without updated certificates i can't install net frameworks and some utilities that use SSL don't work properly (like gpu-z that return a certificate error).

MIKI Reply

March 29, 2020 - 10:47 am

Update:
was able to update certificates, importing them individually in mmc, however i got several capi2 errors doing so, to solve this i execute the "certutil -urlcache * delete" to clean the cache.
However, is very annoying that every now and then i'm force to manually update the certificates, some tools never told me why they have issue working, like the .net Framework, the installation fail and only after several hours later i realized that issue was certificate not up to date.

into my clean system, so maybe this is the root cause and work as intended, aka force the users to abandon win 7 for win 10.
I wont do it since i have many tools and hardware pre 2000 that works only on XP and win 7 since they are old, this is a very bad move from MS, and my system is 100% genuine with a oem valid key.
If only Linux was more mainstream and more compatible, and more software and hardware manufacturer support it i could finally abandon this damn mess.

PETER

Reply

April 7, 2020 - 10:18 pm

You guys are awesome ©
Actually, I had a problem which I even asked for both Microsoft Community and Support Center, I just wanted to know WHY the KB4014984 update couldn't install on Vista Business (after 3 no-problem years). There was 0x800B0109 error (lack of trusted certificate), and I really didn't know what to do until I followed your advice and downloaded [that magic utility] from Kaspersky store.
Now that's fine, the only thing is that I did Run/MMC/Snap-in…etc. and had a look at the amount of trusted certificates which I have now. It is…I suppose 5 times bigger, and there are namigs like Big Daddy or Santa Luis Cruz…they can be hardly related to what we used to call Windows area 🙂
So I'm really glad that with your help the 0x800B0109 problem has been overcome, and hope that increased amount of certificates will go only right. Thank you. Peter.

ADMIN

Reply

April 14, 2020 - 8:07 am

Hi,
If you want, you can check all certificates in your trusted cert ctore using the Sigcheck tool. See the article https://woshub.com/how-to-check-trusted-root-certification-authorities-for-suspicious-certs/

MIKI

Reply

April 16, 2020 - 1:19 pm

Update 2:
Finally updated correctly the certificates under Win 7 x64 and i was able to flawlessy install Netframework 4.8 and have some tools that use SSL to work properly. Now i understand the issues i had i do not need to import registry files from another pc.
In a fresh Win 7 installation, if you do not allow windows auto updates, like i do since i do not want to install tons of useless and bugged crap , you have to indeed update manually some of your system files since they are old and miss some functions.
The certutil.exe tool need to be upgraded to use new commands, to do so you have to install the KB2813430 update:

Once you do this your certutil.exe file is updated and you can use the -GenerateSSTFromWU command.
Then go to the dos window (cmd) and type command "certutil.exe -generateSSTFromWU x:\roots.sst" where x is the drive where you want the file sst to be created.
The operation need 1-2 minutes, after the file is created load the MMC console.
MMC -> add snap-in -> certificates -> computer account > local computer.
Then expand the +Trusted root certifaction authory folder, select certificates, right click all task -> import, choose the SST file create before, press the browse button and chose the Trusted root certification authority from the list. Finish.
Then you have succesfully update the certificates.
For some reasons, probably i miss some other updated files, the file STL extracted from authrootstl.cab refuse to install directly, so this method is the only alternative possible along export/import certificates from others up to date pc with already updated certificates.
On a side note, you do not need to install this KB update in all your pc, once you have created the file.SST, you can do the same procedure in all your pc without the update, since the KB just update certutill.exe file and add auto certificates updates in the registry (that i disabled since i prefer to manually update the certificates).
Once you have updated the certificates you do not need to update them again since the expiration update is something like 2038 or more. Just keep the file SST you created in a safe place and load it if you need to install a fresh win 7 installation again in future.
That's all.

USER Reply

April 10, 2021 - 10:24 am

thank you man you helped me a lot

MAN Reply

April 10, 2021 - 10:30 am

miki i was having certificates problems for a year only your solution that worked thank you MIKI for shearing

KRAUTERSUPPE Reply

September 27, 2021 - 2:28 pm

Congrats MIKI, your solution has worked for many people who want to install different software products.
I wrote down your guidelines in a forum post and it has gotten on the first page in google search : https://forum.planetchili.net/viewtopic.php?f=3&t=5738

GROSS OUT R

certificates? No one should trust that! Explain why it is safe?

HOTSHOT

Reply

June 5, 2020 - 4:55 pm

Wonderful, very helpful. Thanks a lot.

TAB

Reply

September 7, 2020 - 9:02 pm

Pretty, pretty GOOD! (pardons to Larry David)

NIKOLAI

Reply

September 16, 2020 - 11:56 pm

Wonderful. Perfect

ZEBO

Reply

February 18, 2021 - 11:45 pm

This was HUGE. Had issues with Windows Update and some apps not working for a couple of years now, and it was due to out of date certs– this fixed me right up…

EM

Reply

April 19, 2021 - 1:33 pm

Many thanks! Downloading http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab and installing helped on Win7 right after reboot.

YURIY

Reply

May 13, 2021 - 5:22 pm

Thank you very much !!!

ERIC

Reply

October 6, 2021 - 12:09 pm

Good information here, thanks. One of the things I find a bit odd is that when Windows (10 in my case) has internet connection and can access the MS updates URL(s) that provide the updated trusted root info, that is

this because the Windows OS will install/update the trusted-root-cert on demand when you as a user (or the system-account in case of some app/service) access an https-website and that https-certificate issuer root cert is not in your store but trusted by MS that some trusted-installer process then only installs that particular trusted-root-cert? I couldn't find any useful information about this exact process.
We have systems in networks that do not have internet access and thus require an automated approach to update the trusted-roots to be able to connect to some internal webservers with an external issued certificate. Importing that full roots.sst does work of course.

SCHAPPY

Reply

May 5, 2022 - 9:36 pm

Should the "second way" under the "Updating Trusted Root Certificates via GPO in an Isolated Environment" section actually import the certificates into the Trusted Root Certification Authorities folder? I've used the second way and see the registry keys getting dropped on the client (and some of the others created like DisallowedCertEncodedCtl, DisallowedCertLastSyncTime and PinRulesEncodedCtl and PinRulesLastSyncTime), but no new certificates show up in the certlm.mmc. I verified the computer in question can access the file share containing the Certificates by manually importing one from the network share I created for this GPO. This "second way" is actually fixing a problem I had with apps not downloading from the Microsoft Store because of the download attempt the Store makes for the the disallowedcertstl.cab file before the download begins (our network team is blocking the msdownload site). So the client is obviously finding the dissallowedcertstl.cab file on my RootDirURL network share, so my only question is why does it not import the root certificates with this process?

MOEJO

Reply

May 27, 2022 - 3:44 pm

I'm having the same issue as well. I have a disconnected domain and although I have a mechanism to get the certs into a directory in my SYSVOL folder on the DCs weekly (which is working fine), the domain members aren't importing them automatically. Registry entries are present on the domain members (RootDirURL and TUrn of Automatic Root Certificates Update is Disabled).

BRIAN A SEKLECKI

Reply

August 11, 2022 - 8:00 am

It would be nice to hear from someone who has it working to get details and clue (logs file entries, etc.) about how to check if it is working and what the behavior is supposed to be. What happens if you trigger WU client manually on domain client?

ANDYU

Reply

December 7, 2022 - 4:33 pm

Did anybody get this working ?

BRETT R

Reply

September 20, 2024 - 6:04 pm

Facing the same exact issue here.

BRIAN A SEKLECKI

Reply

August 11, 2022 - 9:58 am

Regarding Testing/Validating the updates process: As of 11th August 2022, there are 20 Certs in the Disallowed.sst. They are listed by Thumbprint/Fingerprint (SHA1?) only.
Has anyone got a cross reference point?
Presumably there are non-Microsoft Root CA such as Symantec/Verisign compromised CAs that DigiCert has worked with -Mozilla-Firefox/Microsoft to revoke through their programs.
For example, at the top of the list is: "25 fb 7a 5d 86 f7 2f 5e 67 28 8f 79 73 05 fe 94"
Unless we can come up with a way to validate that Compromised/Publicly Revoked certificates are contained in the Disallowed cert list, and verify Code Signing Cert and/or Root CA Validity validation is denied, then I suppose technically (not cynically) it is more secure to have the default/empty root CA as opposed to potentially trusting RootCA that has a compromised Sub/Intermediate signing CA

BRIAN A SEKLECKI

Reply

August 11, 2022 - 10:00 am

I meant to add, "For Air gapped/offline environments, In the absence of access to OCSP and CRL distribution points, then it is more secure to… ^^^"

CHRIS

Reply

March 13, 2023 - 9:39 am

One option that was not described here is to use a GPO to distribute Root CA certs without using the RootDirURL and Auto Update.
I did not test but it sounds to be as if then the existing root CA certs would be gone as everything is pointing to the file share. If you then have prev installed root CA certs that are not in the new file share location you could lose those.
Hence, the other option would be to use the Windows Settings->public key settings to distribute root CA certs.

AX

Reply

July 17, 2023 - 5:55 am

download times out

MAX

Reply

July 17, 2023 - 6:00 am

new-item hklm:\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot -ItemType Container
set-itemproperty HKLM:\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot -Name DisableRootAutoUpdate -Value 1

LINDA

Reply

October 24, 2024 - 1:59 am

Certutil was part of Win2K server, Win2K3 server, and 2K3 admin tools for WinXP Pro. Dunno about NT 3.5. For some reason, 2K3 admin tool pack is still available for download from MS, (and although the admin pack shouldn't install on XP home, certutil can be extracted from it). New certutil options may be missing

SHBM MIR

Reply

November 29, 2024 - 9:14 am

Thanks for the informative post.
Is there a non-manual approach in case we have created our own CA as root CA and then want to update the TLS certificates of devices in an isolated network?

ADMIN

Reply

December 3, 2024 - 7:38 am

Do you have an isolated network with on-premises Active Directory domain?
The root CA can be published in AD with the command:

```
certutil –dspublish -f rootca.cer RootCA
```

This will deploy the root certificate to the Trusted Root store on all domain clients via autoenrollment.
Publish intermediate CA certificates in AD:

```
certutil –dspublish -f ca.cer SubCA
```

LEAVE A COMMENT

Name*

Email*

Website

NOTIFY ME OF FOLLOWUP COMMENTS VIA E-MAIL. YOU CAN ALSO SUBSCRIBE WITHOUT COMMENTING.

POST COMMENT

FACEBOOK TWITTER TELEGRAM

Fix: Remote De
How to Delete
Configure Goo
Allow Non-adm
Configuring FS
How to Backup
How to Disable

BACK TO TOP