Required trusted root certificates

Article • 03/24/2022 • 2 minutes to read • 4 contributors

In this article

This article lists the trusted root certificates that are required by Windows operating systems. These trusted root certificates are required for the operating system to run correctly.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 293781

Summary

As part of a public key infrastructure (PKI) trust management procedure, some administrators may decide to remove trusted root certificates from a Windows-based domain, server, or client. However, the root certificates that are listed in the Necessary and trusted root certificates section in this article are required for the operating system to operate correctly. Removal of the following certificates may limit functionality of the operating system, or may cause the computer to fail. Don't remove them.

Necessary and trusted root certificates

The following certificates are necessary and trusted in:

- Windows 7
- Windows Vista
- Windows Server 2008 R2
- Windows Server 2008

Issued to	Issued by	Serial number	Expiration	Intended	Fr

Issued to	Issued by	Serial number	Expiration date	Intended purposes	Fr na
Microsoft Root Authority	Microsoft Root Authority	00c1008b3c3c8811d13ef663ecdf40	12/31/2020	All	M Ro Au
Thawte Timestamping CA	Thawte Timestamping CA	00	12/31/2020	Time Stamping	Th Ti CA
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	79ad16a14aa0a5ad4c7358f407132e65	5/9/2021	All	M Ro Ce Au

The follow certificates are necessary and trusted in Windows XP and in Windows Server 2003:

Issued to	Issued by	Serial number	Expiration date	Intend purpos
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	01	12/30/1999	Time Stampi
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	01	12/31/1999	Secure mail, Code Signing
Microsoft Root Authority	Microsoft Root Authority	00c1008b3c3c8811d13ef663ecdf40	12/31/2020	All
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	4a19d2388c82591ca55d735f155ddca3	1/7/2004	Time Stampi

Issued to	Issued by	Serial number	Expiration date	Intende purpos
VeriSign Commercial Software Publishers CA	VeriSign Commercial Software Publishers CA	03c78f37db9228df3cbb1aad82fa6710	1/7/2004	Secure mail, Code Signing
Thawte Timestamping CA	Thawte Timestamping CA	00	12/31/2020	Time Stampi
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	79ad16a14aa0a5ad4c7358f407132e65	5/9/2021	All

The follow certificates are necessary and trusted in Microsoft Windows 2000:

Issued to	Issued by	Serial number	Expiration date	Intende purpos
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	01	12/30/1999	Time Stampi
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	01	12/31/1999	Secure mail, Code Signing
Microsoft Root Authority	Microsoft Root Authority	00c1008b3c3c8811d13ef663ecdf40	12/31/2020	All
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	4a19d2388c82591ca55d735f155ddca3	1/7/2004	Time Stampi
VeriSign Commercial Software Publishers CA	VeriSign Commercial Software Publishers CA	03c78f37db9228df3cbb1aad82fa6710	1/7/2004	Secure mail, Code Signing
Thawte Timestamping	Thawte Timestamping	00	12/31/2020	Time Stampi

Issued to	Issued by	Serial number	Expiration	Intend
CA	CA			

Some certificates that are listed in the previous tables have expired. However, these certificates are necessary for backward compatibility. Even if there's an expired trusted root certificate, anything that was signed by using that certificate *before* the expiration date requires that the trusted root certificate is validated. As long as expired certificates aren't revoked, they can be used to validate anything that was signed before their expiration.

Recommended content

Valid root CA certificates are untrusted - Windows Server

Root CA certificates distributed using GPO might appear sporadically as untrusted. This article provides a workaround for this issue.

Distribute Certificates to Client Computers by Using Group Policy

Learn more about: Distribute Certificates to Client Computers by Using Group Policy

Import third-party certification authorities (CAs) into Enterprise NTAuth store - Windows Server

Describes two methods you can use to import the certificates of third-party CAs into the Enterprise NTAuth store. You can use the public key infrastructure (PKI) Health Tool, or Certutil.exe.

Confirm That Certificates Are Deployed Correctly (Windows) - Windows security

Learn how to confirm that a Group Policy is being applied as expected and that the certificates are being properly installed on the workstations.

Change expiration date of certificates - Windows Server

Describes how to change the validity period of a certificate that is issued by Certificate Authority (CA).

Security certificate validation fails - Windows Server

Works around an issue where security certificate that's presented by a website isn't issued when it has multiple trusted certification paths to root CAs.

Export Root Certification Authority Certificate - Windows Server

describes how to export Root Certification Authority Certificate.

Find the name of Enterprise Root CA server - Windows Server

Helps you to find name of the Enterprise Root Certificate Authority (CA) server.

Show more