Required trusted root certificates

Article • 02/26/2024

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: Supported versions of Windows Server and Windows Client
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

Expand table

Issued to	Issued by	Serial number	Expiration date	Intended purposes	Friendly name	Status
Microsoft Root Authority	Microsoft Root Authority	00c1008b3c3c8811d13ef663ecdf40	12/31/2020	All	Microsoft Root Authority	R
Thawte Timestamping CA	Thawte Timestamping CA	00	12/31/2020	Time Stamping	Thawte Timestamping CA	R
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	79ad16a14aa0a5ad4c7358f407132e65	5/9/2021	All	Microsoft Root Certificate Authority	R

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

Expand table

Issued to	Issued by	Serial number	Expiration date	Intended purposes	Friendly name	Status
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	01	12/30/1999	Time Stamping	Microsoft Timestamp Root	R
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	01	12/31/1999	Secure E-mail, Code Signing	Microsoft Authenticode(tm) Root	R
Microsoft Root Authority	Microsoft Root Authority	00c1008b3c3c8811d13ef663ecdf40	12/31/2020	All	Microsoft Root Authority	R
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	4a19d2388c82591ca55d735f155ddca3	1/7/2004	Time Stamping	VeriSign Time Stamping CA	R
VeriSign Commercial Software Publishers CA	VeriSign Commercial Software Publishers CA	03c78f37db9228df3cbb1aad82fa6710	1/7/2004	Secure E-mail, Code Signing	VeriSign Commercial Software Publishers CA	R
Thawte Timestamping CA	Thawte Timestamping CA	00	12/31/2020	Time Stamping	Thawte Timestamping CA	R
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	79ad16a14aa0a5ad4c7358f407132e65	5/9/2021	All	Microsoft Root Certificate Authority	R

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

Expand table

Issued to	Issued by	Serial number	Expiration date	Intended purposes	Friendly name	Status
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	01	12/30/1999	Time Stamping	Microsoft Timestamp Root	R
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	01	12/31/1999	Secure E-mail, Code Signing	Microsoft Authenticode(tm) Root	R
Microsoft Root Authority	Microsoft Root Authority	00c1008b3c3c8811d13ef663ecdf40	12/31/2020	All	Microsoft Root Authority	R
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	4a19d2388c82591ca55d735f155ddca3	1/7/2004	Time Stamping	VeriSign Time Stamping CA	R
VeriSign Commercial	VeriSign Commercial	03c78f37db9228df3cbb1aad82fa6710	1/7/2004	Secure E-mail,	VeriSign Commercial	R

Issued to	Issued by	Serial number	Expiration date	Intended purposes	Friendly name	Status
Software Publishers CA	Software Publishers CA			Code Signing	Software Publishers CA	
Thawte Timestamping CA	Thawte Timestamping CA	00	12/31/2020	Time Stamping	Thawte Timestamping CA	R

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.

Feedback