Guidance to SHA-1 Hashing Algorithm Deprecation for the Microsoft Trusted Root Certificate Program
(For IT Administrators)

Microsoft Co., Ltd.

Versions

Version	Release Date	Revision Note
1.0	July 6, 2016	Original version released Documentation of contents released in Security Advisories and official blog.
2.0	July 29, 2016	Updated section 4 to reflect the changes of the lock icon on Edge and Internet Explorer 11
3.0	May 9, 2017	Updated section 3 and 4 to reflect the changes of the SHA-1 certificate block

Note
The latest information can be found at the web site shown below.

Official information on this topic:
http://aka.ms/sha1

Table of Contents

1. Overview

For Microsoft Trusted Root Certificate Program, Microsoft will gradually regulate the issue of certificates that use SHA-1 hashing algorithm and restrict the usage of the certificates on Windows.

Accompanied by the compromise of SHA-1 hashing algorithm, public agencies and the whole industry is making a recommendation to migrate to a more secure algorithm. To promote a safer environment and prevent the damage that might occur from the threats to SHA-1, Microsoft is enforcing a deprecation policy to gradually stop the usage of SHA-1 hashing algorithm.

2. Targets of the Policy

2.1. Target Root Certification Authority and Certificate

The SHA-1 deprecation policy applies to Root Certification Authorities that are part of Microsoft Trusted Root Certificate Program, and certificates issued by such authorities.

A list of Root Certification Authorities that are members of the Program can be found at:

"Windows and Windows Phone 8 TLS Root Certificate Program (Member CAs)"

Note: This policy does not apply to Root Certification Authorities that are not part of the Microsoft Trusted Root Certificate Program. For example:

- Private authority within an organization
- Authority within an organization that is built using Windows Server Certificate Service

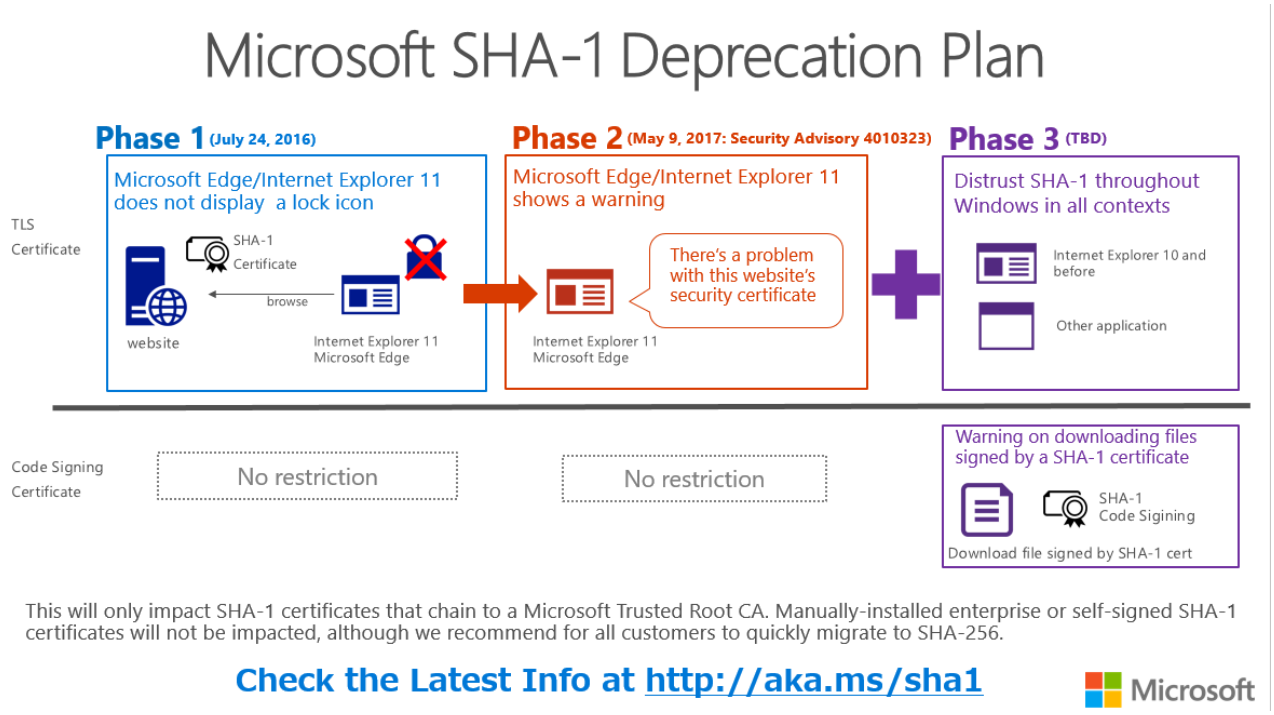
Note: The Microsoft Trusted Root Certificate Program is an approach initiated by Microsoft in cooperation with Root Certification Authorities, to build a safe infrastructure for certificates. In this program, Microsoft qualifies the authorities on behalf of the users, and distributes the trusted CA certificates that are automatically installed to Windows machines.

2.2. Target Environment

After the date of deprecation, certificates issued by the target Certification Authority used in the environment shown below will no longer be trusted.

Windows 7 and later, Windows Server 2008 and later, and Internet Explorer or Edge installed on these Operating Systems.

3. Enforcement Schedule



This will only impact SHA-1 certificates that chain to a Microsoft Trusted Root CA. Manually-installed enterprise or self-signed SHA-1 certificates will not be impacted, although we recommend for all customers to quickly migrate to SHA-256.

Check the Latest Info at http://aka.ms/sha1

Microsoft

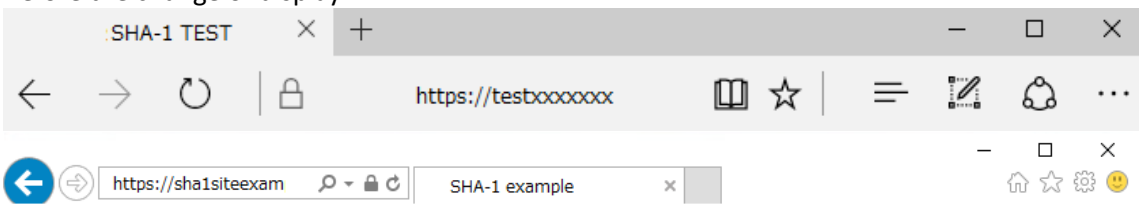
4. Enforcements Details

4.1 Phase 1

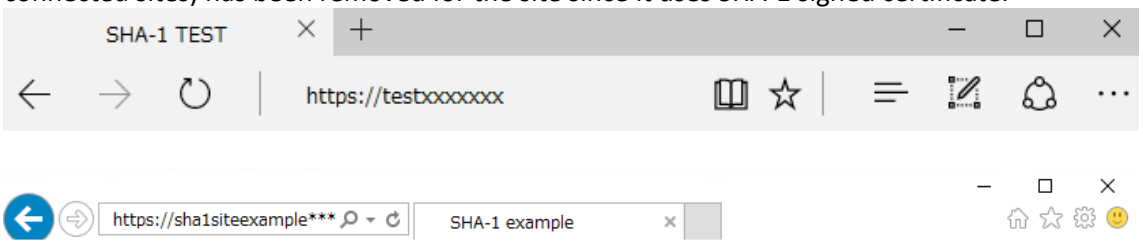
The first phase of our plan is to indicate to users that browse to TLS-secured websites that SHA-1 is less secure than SHA-2. Starting with the Windows 10 Anniversary Update or the monthly security update release of July 2016, Microsoft Edge and Internet Explorer will no longer consider websites protected with a SHA-1 certificate as secure and will remove the address bar lock icon for these sites. These sites will continue to work, but will not be considered secure.

The change of icon display applies to the Certification Authorities, certificates and environment (Microsoft Edge on Windows 10 and Internet Explorer 11 on Windows 7, Windows 8.1 and Windows 10) that are targeted by the SHA-1 deprecation policy.

Before the change of display:



After the change of display: Below is an example of the address bar of a web site using SHA-1 signed certificate. The lock icon that is usually shown next to the address bar for HTTPS sites (TLS connected sites) has been removed for the site since it uses SHA-1 signed certificate.



The above changes to the lock icon for SHA-1 protected sites are included in the following updates:

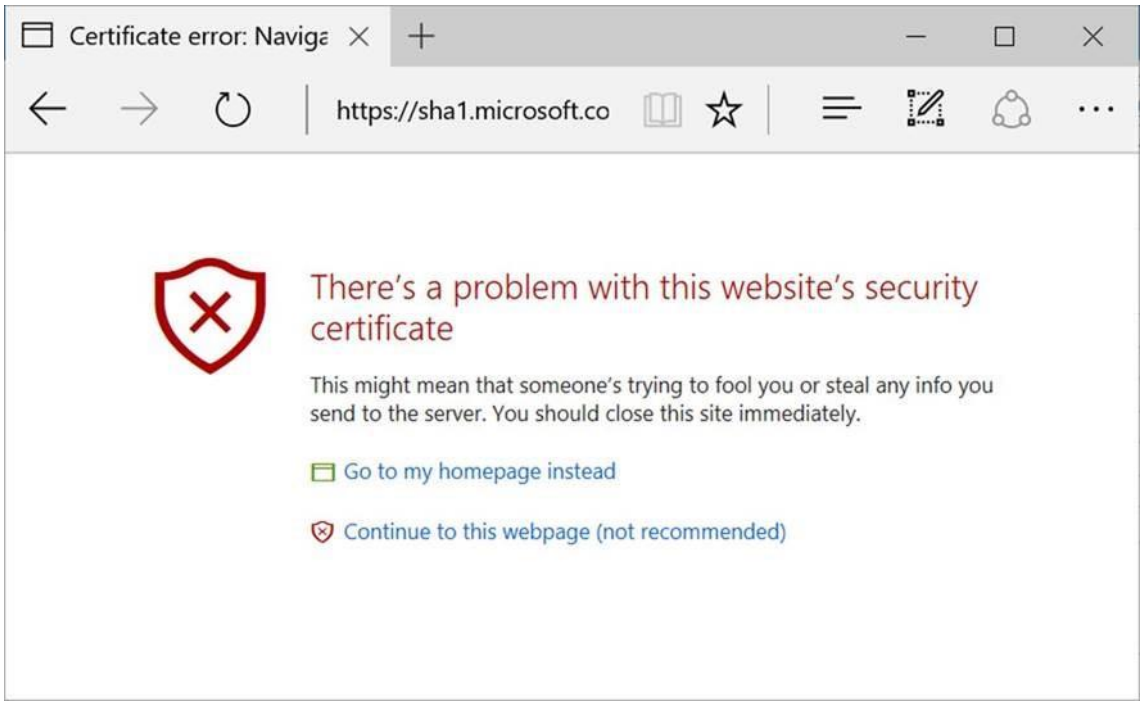
- Windows 10: KB3163912
- Windows 10 Version 1511: KB3172985
- Windows 7 and Server 2008 R2: KB3170106 and KB3172605
- Windows 8.1 and Server 2012 R2: KB3170106 and KB3172614

Read more at https://blogs.windows.com/msedgedev/2016/04/29/sha1-deprecation-roadmap

4.2 Phase 2

On May 9, 2017, Microsoft released an update to Microsoft Edge and Internet Explorer that will prevent sites that are protected with a SHA-1 certificate from loading and will display an invalid certificate warning. Additionally, the Windows 10 Creators Update blocks SHA-1 by-default in the browser.

Read more at Security Advisory 4010323: https://technet.microsoft.com/library/security/4010323 and Knowledge Base Article 4010323: https://support.microsoft.com/kb/4010323



4.3 Phase 3

Today, we intend to do more to warn consumers about the risk of downloading software that is signed using a SHA-1 certificate. Our goal is to develop a common, OS-level experience that all

applications can use to warn users about weak cryptography like SHA-1. Long-term, Microsoft intends to distrust SHA-1 throughout Windows in all contexts. Microsoft is closely monitoring the latest research on the feasibility of SHA-1 attacks and will use this to determine complete deprecation timelines.

5. Impact that is Likely To Occur

SHA-1 signed certificates used after the date of deprecation will no longer be trusted by Windows. Thus, impact shown below is likely to occur.

5.1. Impact of TLS Certificate Deprecation

SHA-1 signed certificates used after the date of deprecation will no longer be trusted by Windows, and TLS connection will fail. Thus, an error message will be displayed, or applications that require TLS may not work. TLS connection includes HTTPS (HTTP over TLS) used for safe communication on web sites, and FTPS, SMTPS, etc.

Example of Impact

If the web site that is published on the Internet is providing safe communication via HTTPS using SHA-1 signed certificates, users will not be able to access the web site after the deprecation date. In particular, the browser (Internet Explorer, Microsoft Edge, etc) will display an error message, and the user cannot browse the web site.

5.2. Code Signing Certificates

Today, we intend to do more to warn consumers about the risk of downloading software that is signed using a SHA-1 certificate. Our goal is to develop a common, OS-level experience that all applications can use to warn users about weak cryptography like SHA-1. Long-term, Microsoft intends to distrust SHA-1 throughout Windows in all contexts. Microsoft is closely monitoring the latest research on the feasibility of SHA-1 attacks and will use this to determine complete deprecation timelines.

6. FAQs

6.1. FAQ on Overview

Q. What is SHA-1?

A. SHA-1 is one type of algorithm that generates hash, and was standardized in 1995 by NIST (National Institute of Standards and Technology). A hash is a value (hash value) that is generated from the original data according to a certain rule (hash function). A hash value is mainly used for verification of data integrity, and ensures security by the features given below.

1. Cannot compute or reconstruct the original data from the hash value (irreversibility)
2. Different hash value will be generated from different input data (collision-resistant)

For example, using digital signature which is an encrypted hash value, can avoid tampering and spoofing of certificates.

Q. Why will SHA-1 be deprecated?

A. In spite of the difference in original data, there is a risk that same hash value might be generated by the hashing algorithm (this is called hash collision). If this happens, spoofing and

data tampering is possible, because the hash value remains the same even if the original data is changed. New algorithms are discovered as research proceed, and mathematics or calculation that are used in hash algorithm to ensure safety can be realize in a short time because of faster computing speed. These factors cause hash collision. There is a research report that by using a certain cloud service, it is possible to make an effective SHA-1 collision attack for only 75K U.S. dollars.

Q. Why is action for SHA-1 necessary now?
A. Not only Microsoft is recommending the migration from SHA-1, it is an industry-wide (and governmental guided) movement. It is estimated from research that criminal syndicates will exploit SHA-1 two years earlier than previously expected, and one year before SHA-1 will be deprecated in modern Internet browsers. Public agencies have already stopped using SHA-1, and migration to a safer algorithm is recommended.
Microsoft is gradually regulating the usage of SHA-1, and promoting migration to SHA-2.

Q. I want to know how other products on the market (e.g. Chrome、Safari、Firefox) are responding.
A. Each company has announced their policy and measures on SHA-1 deprecation.

Q. I am a system administrator. What should I do to deal with SHA-1 deprecation and migration to SHA-2?
A. Refer to Recommended Action.

Q. How do know if I am using SHA-1?
A. Refer to STEP 4: Verify if the certificate is using SHA-1 hashing algorithm.
Microsoft Customer Service & Support will support migration.

Q. Is there a possibility of change in schedule? How can I know about changes, and get latest information on this topic?
A. Refer to the web site for latest information.
Official information about SHA-1 deprecation:
http://aka.ms/sha1

Q. How can I know about changes, and get latest information on this topic?
A. Refer to the web site for latest information.
Official information about SHA-1 deprecation:
http://aka.ms/sha1

6.2. FAQ on Targets of the Policy

Q. Does the policy only apply to certificates that are issued by CAs that are part of the Microsoft Root Certificate Program?
A. Yes. The targets of this policy for Microsoft products are certificates issued by CAs participating in the Microsoft Root Certificate Program. The policy does not apply to Root CAs that are not part of the Program. For example, private authority within an organization (such as root authority within an organization that is built using Windows Server Certificate Service) is not the target of this policy.

Q. My understanding is that the targets of the policy are certificates issued by public CAs, not private CAs. Is this correct?
A. This policy applies to usage of certificates issued by CAs that are part of Microsoft Root Certificate Program.

Q. I understand that the policy applies to certificates issued by CAs that are participating in the Microsoft Root Certificate Program. Which level in the CA hierarchy is the policy being enforced on? For example, does the policy apply to root certificate itself?
A. The policy does not apply to root certificates of CAs that are part of the Microsoft Root Certificate Program. All certificates (i.e. the leaf certificates and intermediate certificates) issued by CAs that are participating in the Microsoft Root Certificate Program are "certificates issued under the root certificate" so the policy will be enforced on them. Note that deprecation of SHA-1 for root certificates are ongoing in another timeline.

Q. Does the SHA-1 deprecation policy apply only to TLS certificates and code signing certificates regarding Windows?
A. At this point of time, the policy applies to TLS certificates.

Q. How are TLS certificates used?
A. TLS certificates are often used for HTTPS on web servers that are made public to the internet.

Q. Who will mainly be affected by this policy?
A. This policy affects users when connecting to a secure site on the Internet. Companies can continue to use SHA-1 internally, but there will be a bigger risk than SHA-2. Companies that own web servers connected to the Internet should migrate from SHA-1.

6.3. FAQ on Warnings

Q. Do you have any plans to provide a function in Internet Explorer to display warning messages?
A. Starting with the Windows 10 Anniversary Update, Microsoft Edge and Internet Explorer will no longer consider websites protected with a SHA-1 certificate as secure and will **remove the address bar lock icon** for these sites. These sites will continue to work, but will not be considered secure. This change will be in upcoming Windows Insider Preview builds, and will be deployed broadly this summer. For more information, refer to "An update to our SHA-1 deprecation roadmap".

6.4. FAQ on Policy Deployment

Q. How will the policy actually be deployed? Will it be activated automatically on January 1, 2016? Are security updates delivered via Microsoft Update for activation?
A. This policy will only apply to systems with updates described in "An update is available that improves management of weak certificate cryptographic algorithms in Windows (Knowledge Base Article 2862966)" installed. This Knowledge Base was introduced in Security Advisory 2854544 on August 13, 2013 and is updated automatically. Security update 2862966 is for Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, and Windows RT (For Windows 8.1/Windows Server 2012 R2 and later, the function is already included in the OS by default). There is a plan to deploy security update via Windows Update to enforce the configuration of SHA-1 hashing algorithm deprecation to target OSs.

Q. I want to know about SHA-2. support My understanding is that SHA-2 root certificates were not included in the initial installation of Windows 7. From which update was it provided?
A. Updates to add SHA-2 hashing algorithm function for Windows7/Windows Server 2008 R2 are released in Security Advisory 2949927 or Security Advisory 3033929 (For Windows 8.1/Windows Server 2012 R2 and later, the function is already included in the OS by default). Update 3033929 replaces update 2949927. Customers who are planning to apply this update, please install update 3033929 (Update 3033929 was released to address issues that some customers experienced after installation of update 2949927. Customers who did not experience any issues after applying update 2949927 do not need to install update 3033929).

Q. Regarding Security Advisory "Availability of SHA-2 Code Signing Support for Windows 7 and Windows Server 2008 R2" (2949927 or 3033929), do you have plans to release updates for Windows Vista and Windows Server 2008?
A. No. There are no plans to release updates for Windows Vista and Windows Server 2008.

Q. Will SHA-1 become invalid and not authenticated after the application of Advisory 3033929?
A. No. The updates add SHA-2 hashing algorithm signing and verification support to affected operating systems, which includes the following:

- Support for multiple signatures on Cabinet files
- Support for multiple signatures on Windows PE files
- UI changes that enable the viewing of multiple digital signatures
- The ability to verify RFC3161 timestamps to the Code Integrity component that verifies signatures in the kernel
- Support for various APIs (CertIsStrongHashToSign, CryptCATAdminAcquireContext2, and CryptCATAdminCalcHashFromFileHandle2, etc.)

7. Recommended Action

7.1. Recommended Actions for TLS Certificates

If there are any SHA-1 signed certificates used in the system, they must be replaced.

STEP 1: Verify the servers to be inspected

Servers using TLS such as HTTPS, SMTPS, FTPS should be inspected (if it is a web site, IIS installed servers are targets). Among these servers, mainly the ones providing services used on the Internet, such as web sites published on the Internet, should be verified.

STEP 2: Verify the certificate used by the server

Verify the TLS certificate by using any of the following methods:

- The TLS certificate used in a web site that is published on the Internet can actually be viewed by opening the web site from the browser that runs on the client machine.
- When using IIS, view the certificate that is used for TLS connection (Reference: View a Server Certificate (IIS 7))
- For others, open mmc.exe file on the server that uses TLS, and check the certificate in the certificate store, personal folder of the computer account. Check the certificates which purpose of usage is server authentication (Reference: Add the Certificates Snap-in to an MMC)

STEP 3: Verify the issuer of the certificate

First open the certificate, and then open the tab of the certification path. Displayed on the top is the root certification authority (You can open the certificate of the root CA by double-clicking the icon). Check if the root CA is participating in the Microsoft Root Certificate Program.

If it is not on the list, the deprecation policy does not apply to the certificate. For example, certificates that are issued internally within a company or organization's system using Windows Server Certificate Services are not targets of the policy.

STEP 4: Verify if the certificate is using SHA-1 hashing algorithm

Open the certificate, and then open the [Advanced] tab. Check if the "Signature hashing algorithm" is SHA-1. If it is SHA-1, this policy applies to it. Migration of the certificate is required.

STEP 5: Contact the issuer of the certificate and renew the certificate

If the server is using SHA-1 signed certificate, you must replace it with a certificate with new hashing algorithm, such as SHA-2. Contact the CA that issued the certificate, and renew the certificate.

STEP 6: Verify the impact of the policy using a test client

Prepare a client to connect to a server that provides TLS connection, set it up as deprecation policy applied, and check if there is no trouble in TLS connection.

1. On the test client, type the following commands into an Administrator Command Prompt:

certutil -setreg chain¥Default¥WeakSha1ThirdPartyFlags 0x80100000
TLS certificates will be considered untrusted according to this setting. This will enable the client to be in a state of deprecation policy applied. (Reference: Protecting Against Weak Cryptographic Algorithms)
Use the following command to remove the settings after you have completed your testing:
certutil -delreg chain¥Default¥WeakSha1ThirdPartyFlags
Note: This configuration includes registry change. Validate on the test client, and backup data before configuration to prepare for unexpected problems.
Note: There are cases when the verification does not work because of other settings and configurations. Check for related settings and change the value of the flags as needed. Refer to the web site below for details on flag value and related settings. Protecting Against Weak Cryptographic Algorithms

2. Verify if there is no trouble in web sites, application, system that use TLS
Using the test client for daily operation for a while can reveal hidden impacts.
If there is any impact, verify the certificate used on the target server.

Note: You can enable logging your use of SHA1 certificates by typing the following commands into an Administrator Command Prompt. The following command does not block the use of SHA-1 TLS certificates; however, it will log the certificate to the provided directory.

First create a logging directory and grant universal access:

```
set LogDir=C:¥Log
  mkdir %LogDir%
  icacls %LogDir% /grant *S-1-15-2-1:(OI)(CI)(F)
  icacls %LogDir% /grant *S-1-1-0:(OI)(CI)(F)
  icacls %LogDir% /grant *S-1-5-12:(OI)(CI)(F)
  icacls %LogDir% /setintegritylevel L
```

Enable certificate logging.

```
Certutil -setreg chain¥WeakSignatureLogDir %LogDir%
  Certutil -setreg chain¥WeakSha1ThirdPartyFlags 0x80900008
```

Use the following command to remove the settings after you have completed your testing.

```
Certutil -delreg chain¥WeakSha1ThirdPartyFlags
  Certutil -delreg chain¥WeakSignatureLogDir
```

8. Public Information

8.1. The latest information on this topic

https://aka.ms/sha1

8.2. Security Advisory

Deprecation of SHA-1 Hashing Algorithm for Microsoft Root Certificate Program

8.3. Updates for deprecation of SHA-1 hashing algorithm

Updates to Improve Cryptography and Digital Certificate Handling in Windows
Deprecation of SHA-1 Hashing Algorithm for Microsoft Root Certificate Program

8.4. Advisories and updates for SHA-2 support

Availability of SHA-2 Hashing Algorithm for Windows 7 and Windows Server 2008 R2
Availability of SHA-2 Code Signing Support for Windows 7 and Windows Server 2008 R2
* A known issue has been reported for 2949927, so customers who are planning to apply this update, please install 3033929 (3033929 replaces 2949927).