KB5014754: Certificate-based authentication changes on Windows domain controllers

▶ *Applies To*

Change log

Summary

CVE-2022-34691, CVE-2022-26931 and CVE-2022-26923 address an elevation of privilege vulnerability that can occur when the Kerberos Key Distribution Center (KDC) is servicing a certificate-based authentication request. Before the May 10, 2022 security update, certificate-based authentication would not account for a dollar sign ($) at the end of a machine name. This allowed related certificates to be emulated (spoofed) in various ways. Additionally, conflicts between User Principal Names (UPN) and **sAMAccountName** introduced other emulation (spoofing) vulnerabilities that we also address with this security update.

Take action

To protect your environment, complete the following steps for certificate-based authentication:

1. Update all servers that run Active Directory Certificate Services and Windows domain controllers that service certificate-based authentication with the May 10, 2022 update (see Compatibility mode). The May 10, 2022 update will provide audit events that identify certificates that are not compatible with Full Enforcement mode.

2. If no audit event logs are created on domain controllers for one month after installing the update, proceed with enabling Full Enforcement mode on all domain controllers. By **February 2025**, if the **StrongCertificateBindingEnforcement** registry key is not configured, domain controllers will move to Full Enforcement mode. Otherwise, the registry keys Compatibility mode setting will continue to be honored. In Full Enforcement mode, if a certificate fails the strong (secure) mapping criteria (see Certificate mappings), authentication

will be denied. However, the option to move back to Compatibility mode will remain until September 2025.

Audit events

The May 10, 2022 Windows update adds the following event logs.

No strong mapping

Certificate predates account

The certificate was issued to the user before the user existed in Active Directory and no strong mapping could be found. This event is only logged when the KDC is in Compatibility mode.

Event Log	System
Event Type	Error
Event Source	Kdcsvc
Event ID	40 48 (For Windows Server 2008 R2 SP1 and Windows Server 2008 SP2
Event Text	The Key Distribution Center (KDC) encountered a user certificate that was valid but could not be mapped to a user in a strong way (such as via explicit mapping, key trust mapping, or a SID). The certificate also predated the user it mapped to, so it was rejected. See https://go.microsoft.com/fwlink/?linkid=2189925 to learn more. User: <principal name> Certificate Subject: <Subject name in Certificate> Certificate Issuer: <Issuer FQDN> Certificate Serial Number: <Serial Number of Certificate> Certificate Thumbprint: <Thumbprint of Certificate> Certificate Issuance Time: <FILETIME of certificate> Account Creation Time: <FILETIME of principal object in AD>

Users SID does not match Certificate SID

The SID contained in the new extension of the users certificate does not match the users SID, implying that the certificate was issued to another user.

Event Log	System
Event Type	Error
Event Source	Kdcsvc
Event ID	41 49 (For Windows Server 2008 R2 SP1 and Windows Server 2008 SP2)
Event Text	The Key Distribution Center (KDC) encountered a user certificate that was valid but contained a different SID than the user to which it mapped. As a result, the request involving the certificate failed. See https://go.microsoft.com/fwlink/?linkid=2189925 to learn more. User: <principal name> User SID: <SID of the authenticating principal> Certificate Subject: <Subject name in Certificate> Certificate Issuer: <Issuer FQDN> Certificate Serial Number: <Serial Number of Certificate> Certificate Thumbprint: <Thumbprint of Certificate> Certificate SID: <SID found in the new Certificate Extension>

Certificate mappings

Domain administrators can manually map certificates to a user in Active Directory using the **altSecurityIdentities** attribute of the users Object. There are six supported values for this attribute, with three mappings considered weak (insecure) and the other three considered strong. In general, mapping types are considered strong if they are based on identifiers that you cannot reuse. Therefore, all mapping types based on usernames and email addresses are considered weak.

Mapping	Example	Type	Remarks
X509IssuerSubject	“X509:<I>IssuerName<S>SubjectName”	Weak	
X509SubjectOnly	“X509:<S>SubjectName”	Weak	
X509RFC822	“X509:<RFC822>user@contoso.com”	Weak	Email Address
X509IssuerSerialNumber	“X509:<I>IssuerName<SR>1234567890”	Strong	Recommended
X509SKI	“X509:<SKI>123456789abcdef”	Strong	
X509SHA1PublicKey	“X509:<SHA1-PUKEY>123456789abcdef”	Strong	

If customers cannot reissue certificates with the new SID extension, we recommend that you create a manual mapping by using one of the strong mappings described above. You can do this by adding the appropriate mapping string to a users **altSecurityIdentities** attribute in Active Directory.

Manually map certificates

Timeline for Windows updates

Important The Enablement Phase starts with the April 11, 2023 updates for Windows, which will ignore the Disabled mode registry key setting.

Compatibility mode

Full Enforcement mode

Disabled mode

Strong Mapping default changes

Troubleshooting

Failure to sign in after installing CVE-2022-26931 and CVE-2022-26923 protections

Failure to authenticate using Transport Layer Security (TLS) certificate mapping

Registry key information

After you install CVE-2022-26931 and CVE-2022-26923 protections in the Windows updates released between May 10, 2022 and September 10, 2025, or later, the following registry keys are available.

Key Distribution Center (KDC) registry key

This registry key will be unsupported after installing updates for Windows released on or after September 2025.

Important

Using this registry key is a temporary workaround for environments that require it and must be done with caution. Using this registry key means the following for your environment:

- This registry key only works in Compatibility mode starting with updates released May 10, 2022.
- This registry key will be unsupported after installing updates for Windows released on September 10, 2025.
- The SID Extension detection and validation used by the Strong Certificate Binding Enforcement has a dependency on the KDC registry key **UseSubjectAltName** value. The SID extension will be used if the registry value does not exist or if the value is set to a value of **0x1**. The SID extension will not be used if **UseSubjectAltName** exists, and the value is set to **0x0**.

Registry Subkey	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc
Value	StrongCertificateBindingEnforcement
Data Type	REG_DWORD
Data	1 – Checks if there is a strong certificate mapping. If yes, authentication is allowed. Otherwise, the KDC will check if the certificate has the new SID extension and validate it. If this extension is not present, authentication is allowed if the user account predates the certificate.

2 – Checks if there's a strong certificate mapping. If yes, authentication is allowed. Otherwise, the KDC will check if the certificate has the new SID extension and validate it. If this extension is not present, authentication is denied.

0 – Disables strong certificate mapping check. Not recommended because this will disable all security enhancements.

If you set this to 0, you must also set **CertificateMappingMethods** to 0x1F as described in the Schannel registry key section below for computer certificate-based authentication to succeed..

Restart Required?	No

SChannel registry key

When a server application requires client authentication, Schannel automatically attempts to map the certificate that the TLS client supplies to a user account. You can authenticate users who sign in with a client certificate by creating mappings that relate the certificate information to a Windows user account. After you create and enable a certificate mapping, each time a client presents a client certificate, your server application automatically associates that user with the appropriate Windows user account.

Schannel will try to map each certificate mapping method you have enabled until one succeeds. Schannel tries to map the Service-For-User-To-Self (S4U2Self) mappings first. The Subject/Issuer, Issuer, and UPN certificate mappings are now considered weak and have been disabled by default. The bitmasked sum of the selected options determines the list of certificate mapping methods that are available.

The SChannel registry key default was 0x1F and is now 0x18. If you experience authentication failures with Schannel-based server applications, we suggest that you perform a test. Add or modify the **CertificateMappingMethods** registry key value on the domain controller and set it to 0x1F and see if that addresses the issue. Look in the System event logs on the domain controller for any errors listed in this article for more information. Keep in mind that changing the SChannel registry key value back to the previous default (0x1F) will revert to using weak certificate mapping methods.

Registry Subkey	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\Schannel
Value	CertificateMappingMethods
Data Type	DWORD
Data	0x0001 - Subject/Issuer certificate mapping (weak – Disabled by default) 0x0002 - Issuer certificate mapping (weak – Disabled by default) 0x0004 - UPN certificate mapping (weak – Disabled by default)

0x0008 - S4U2Self certificate mapping (strong)

0x0010 - S4U2Self explicit certificate mapping (strong)

Restart Required?	No

For additional resources and support, see the "Additional resources" section.

Certificate Backdating registry key

Enterprise Certificate Authorities

Enterprise Certificate Authorities (CA) will start adding a new non-critical extension with Object Identifier (OID) (1.3.6.1.4.1.311.25.2) by default in all the certificates issued against online templates after you install the May 10, 2022 Windows update. You can stop the addition of this extension by setting the 0x00080000 bit in the **msPKI-Enrollment-Flag** value of the corresponding template.

Example

Frequently asked questions

Once the CA is updated, must all client authentication certificates be renewed?

How will Full Enforcement mode affect my environment?

Additional resources

For more information about TLS client certificate mapping, see the following articles:

- Transport Layer Security (TLS) registry settings
- IIS Client Certificate Mapping Authentication <iisClientCertificateMappingAuthentication>
- Configuring One-to-One Client Certificate Mappings
- Many-To-One Mappings <manyToOneMappings>
- Securing Public Key Infrastructure (PKI)

- Active Directory Certificate Services: Enterprise CA Architecture

SUBSCRIBE RSS FEEDS

Need more help?

How can we help you?

Want more options?

Discover **Community**

Explore subscription benefits, browse training courses, learn how to secure your device, and more.

Microsoft 365 subscription benefits

Microsoft 365 training

Microsoft security

Accessibility center

Surface Laptop Go 3

Microsoft Copilot

AI in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

AI for education

Microsoft Power Platform

Microsoft Teams

Microsoft 365 Copilot

Small Business

Microsoft Learn

Support for AI marketplace apps

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap

Contact Microsoft

Privacy

Terms of use

Trademarks

Safety & eco

Recycling

About our ads