⬚ ⌕   **Microsoft**   Sign in

Support ⌄

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.
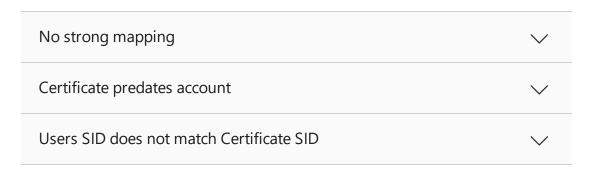
Take action

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 **StrongCertificateBindingEnforcemen**t 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	∨
Users SID does not match Certificate SID	∨

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.
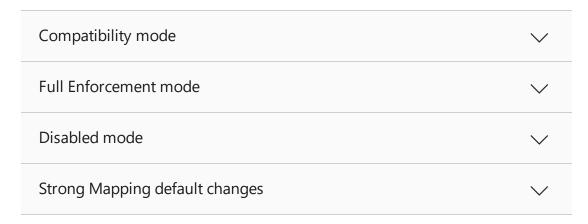
Mapping	Example	Type	Remarks
X509IssuerSubject	"X509: <I>IssuerName<S>SubjectName"	Weak	
X509SubjectOnly	"X509:<S>SubjectName"	Weak	
X509RFC822	"X509: <RFC822>user@contoso.com"	Weak	Email Address
X509IssuerSerialNumber	"X509: <I>IssuerName<SR>1234567890"	Strong	Recommended
X509SKI	"X509:<SKI>123456789abcdef"	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	⌄
SChannel registry key	⌄
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

Was this information helpful?   **Yes**   **No**

What's new

Surface Pro

Surface Laptop

Microsoft Store

Account profile

Download Center

Education

Microsoft in education

Devices for education