




Open in app ↗

Sign up Sign in

Medium

 Search

 Write



Certipy 4.0: ESC9 & ESC10, BloodHound GUI, New Authentication and Request

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 \$/month

The BloodHound team has delivered many impressive updates, and according to their [release post on version 4.1](#) and [version 4.2](#), Active Directory Certificate Services (AD CS) abuse primitives are on their road map and coming soon. However, it's been 6 months since the release of version 4.1, so I decided to implement it myself into the BloodHound GUI. This also means that if you want to use the original version of the BloodHound GUI with Certipy, you'll have to pass the `-old-bloodhound` option to Certipy's `find` command, as the new BloodHound data output from Certipy is only compatible with the forked GUI. The forked version is based on the latest [version of BloodHound \(4.2.0 - August 3, 2022\)](#) and requires `neo4j > 4.4.0`

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

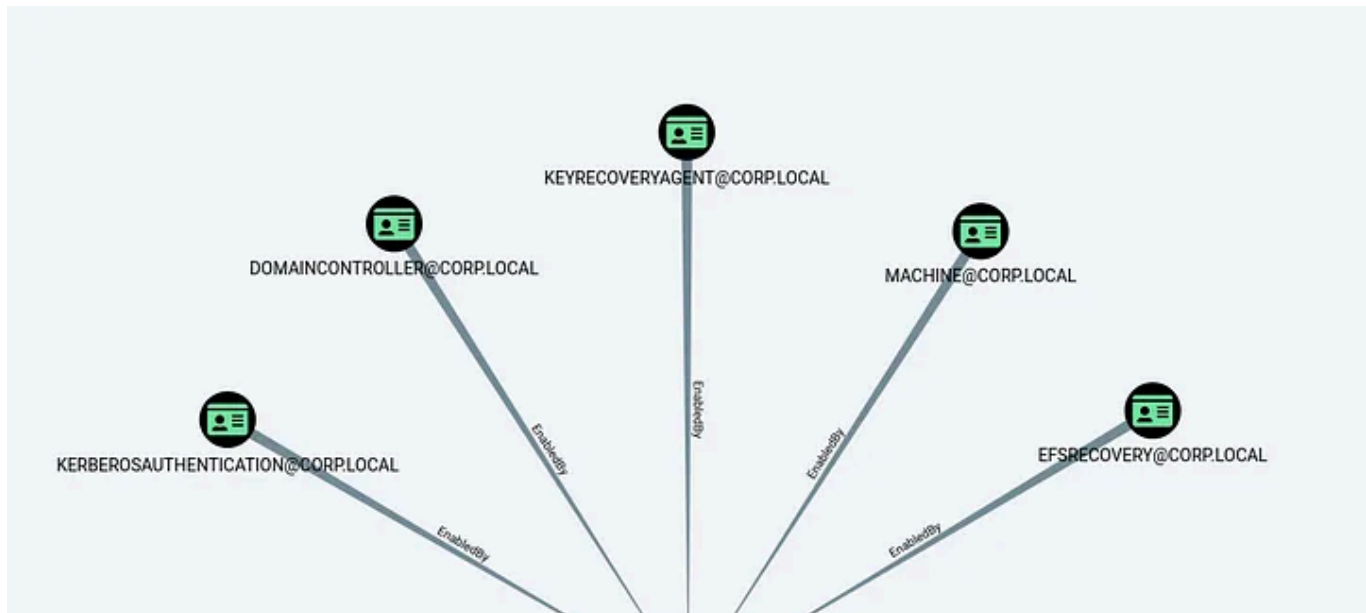
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

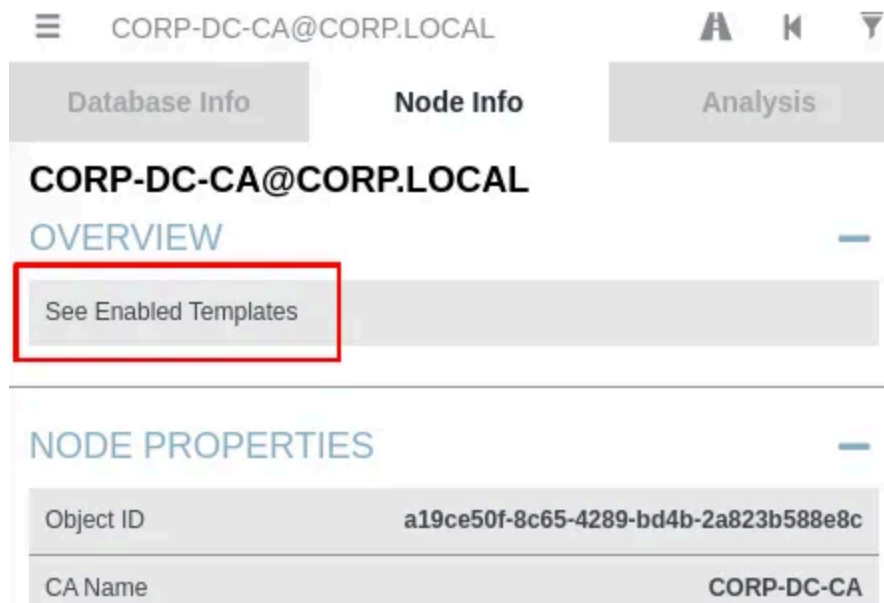
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

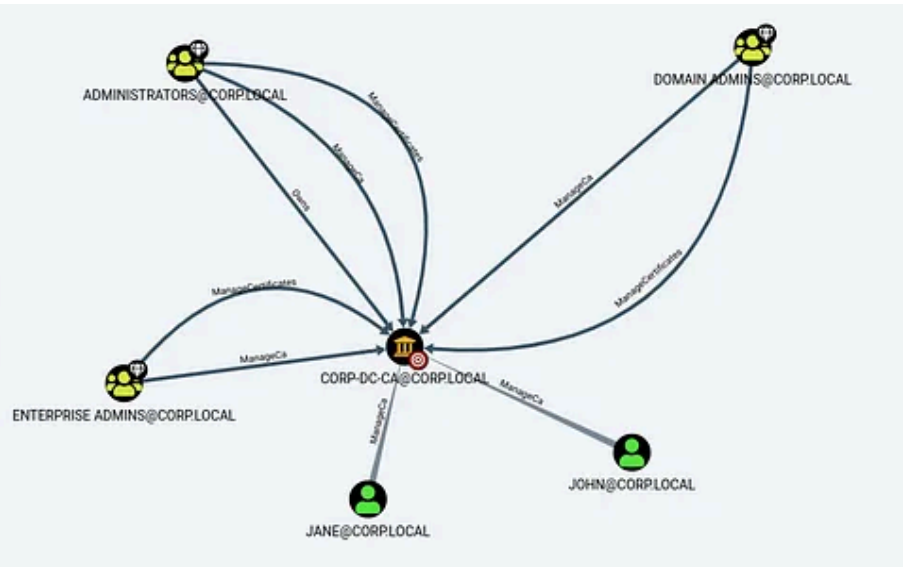
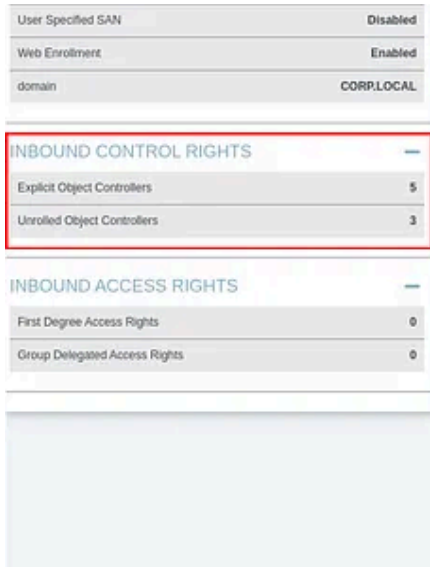
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

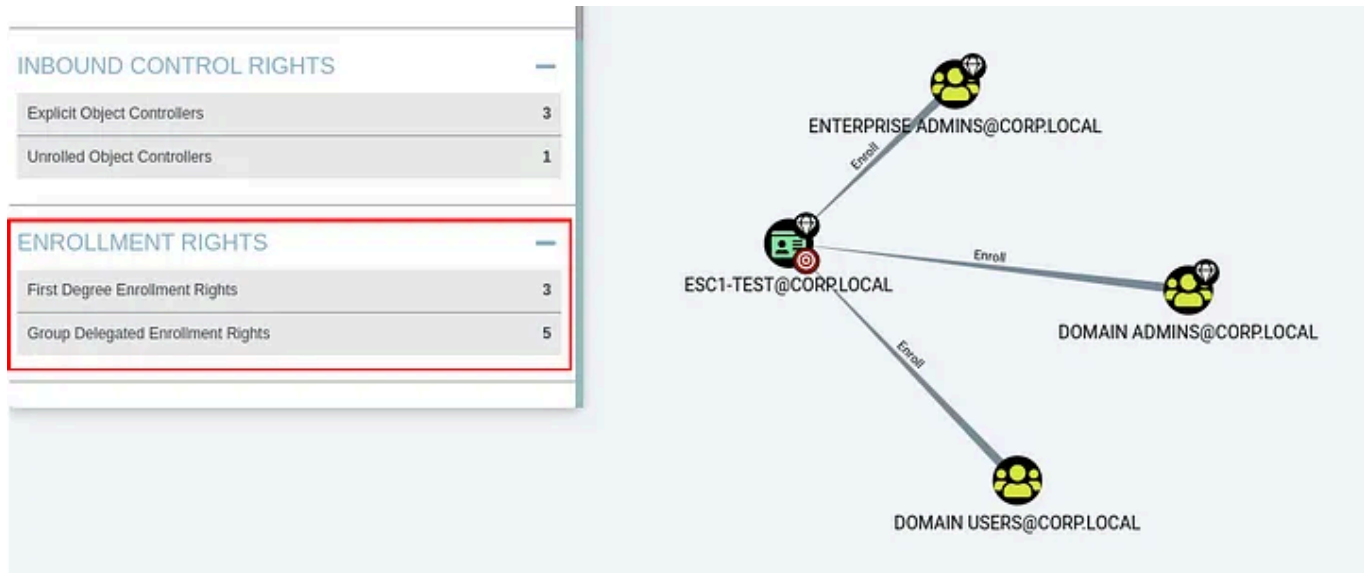
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

instance, you can now hover your mouse over a query and click the little “Copy” button to copy the query to your clipboard.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

These are just some small features I personally enjoy, and I might add new ones. The source code can be found at <https://github.com/ly4k/BloodHound/> and prebuilt binary releases can be found [here](#). I'll regularly pull commits from the upstream version so you don't miss out on those features. If you have any additions, feel free to open an issue or create a pull request.

Old Is New Again

Now, back to Certipy. I have reintroduced and improved some old features of Certipy that I previously removed related to Certipy's `find` command. For

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

an interactive LDAP shell with a limited set of commands that should be enough to aid you in the right direction, for instance configuring Resource-based Constrained Delegation, adding a user to a group, reading LAPS, and more.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

credentials of your current user context. This has happened to me a few times. Instead, let me introduce Certipy's new SSPI integration.

The first step is to get Certipy on your target machine. You could install Python and then Certipy, or you could just use something like PyInstaller (`pyinstaller ./Certipy.spec`) to pack it into an executable. Once you've done that, you can run all your usual commands, but instead of specifying username, password, and domain, you can just pass the `-sspi` option. This will make Certipy use your current user's domain context for authentication by using Windows APIs to retrieve Kerberos tickets.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

On top of this, if you would just like to inject your newly acquired domain administrator ticket into your current logon session, you can do that with the `-ptt` flag.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

ticket option. The Base64 ticket can also be used for Rubeus.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

The new `ptt` command can be used to inject tickets from a file or command line, but it can also be used to request a new TGT using credentials and inject the ticket into your logon session. This is useful if you're not in a domain context and you don't want to write the username, password, and domain for each command.

Change of Parameters

Certipy has also received a minor change on how a username, domain, password and target are specified. The username and domain is now specified in `-username user@domain` and the password is specified in `-`

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Double SAN

A feature request was sent to me to allow specifying a DNS host name

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Well, Certipy will now ask you which identification you wish to use. So can we have one certificate with identification for multiple users?

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

While this was rather trivial to implement, another user reported that a certificate template was configured to require key archival. This is specified as `CT_FLAG_REQUIRE_PRIVATE_KEY_ARCHIVAL` in the `msPKI-Private-Key-Flag` of the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Nonetheless, I wouldn't want this single flag to stand in my (or your) way to becoming domain administrator during an engagement.

Other Features

You might also encounter some other unmentioned features — which might not seem that useful — that is merely a result of my own research. For instance, it's possible to renew a certificate using an old certificate with the `-renew` parameter. Since I had already implemented all the structures and functionality, I thought I'd just add it to Certipy.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

- Overwrite `userPrincipalName` of user to be `<sAMAccountName>@<domain>` of target to hijack machine account since machine accounts don't have a UPN
- Delete `userPrincipalName` of user and overwrite `sAMAccountName` to be `<sAMAccountName>` without a trailing `$` to hijack a machine account

These three cases are all related to how a certificate is mapped to an account during authentication. First of all, a missing domain part of the UPN doesn't matter. Secondly, if the KDC can't find an account where the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

This was tested against a fully patched domain controller where `john` only had `GenericWrite` over `johnpc$`.

On top of this, Microsoft implemented the new `szOID_NTDS_CA_SECURITY_EXT` security extension for issued certificates, which will embed the `objectSid` property of the requester. Furthermore, Microsoft created the new registry key values

(`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\Schannel`) `CertificateMappingMethods` and

(`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kds`)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

`CertificateMappingMethods` correspond to Kerberos and Schannel, respectively.

Certificates can either be mapped via implicit or explicit mappings. For explicit mappings, the `altSecurityIdentities` property on an account object is configured to contain identifiers for a certificate, for instance the issuer and serial number. This way, when a certificate is used for authentication via explicit mapping, it must be signed by a trusted CA and then match the values specified in the `altSecurityIdentities`. On the other hand, when a certificate is used for authentication via implicit mapping, then the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

certificate mapping in Kerberos is exactly as before the patch. Setting this value to 0 is not recommended by Microsoft, but according to BleepingComputer, this value fixed the authentication issues for a Windows admin.

If this value is 1 (default value after patch), the KDC checks if there is a strong certificate mapping (explicit). 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.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

If the certificate contains a UPN with the value `john@corp.local`, the KDC will first try to see if there exists a user with a `userPrincipalName` property value that matches. If not, it checks if the domain part `corp.local` matches the Active Directory domain. If there is no domain part in the UPN SAN, i.e. the UPN is just `john`, then no validation is performed. Next, it will try to map the user part `john` to an account where the `sAMAccountName` property matches. If this also fails, it will try to add a `$` to the end of the user part, i.e. `john$`, and try the previous step again (`sAMAccountName`). This means that a certificate with a UPN value can actually be mapped to a machine account.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Schannel will map the certificate a little bit differently than the KDC would. Let's take a look at the possible values for the `CertificateMappingMethods` registry key value. This value is a DWORD that supports multiple values as a bit set. The new default value is `0x18` (`0x8` and `0x10`), whereas the old value was `0x1f` (all of the below values).

- `0x0001` — Subject/Issuer certificate mapping (explicit)
- `0x0002` — Issuer certificate mapping (explicit)
- `0x0004` — SAN certificate mapping (implicit)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

or modify the `CertificateMappingMethods` registry key value on the domain controller and set it to 0x1F and see if that addresses the issue.”

Now that we understand the patch for CVE-2022-26923, let’s look at the new ESCs and some examples.

ESC9 — No Security Extension

Description

ESCs are used to extend the lifetime of a certificate. ESC9 is a security extension that is used to extend the lifetime of a certificate.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Please see the “Examples” section for a practical example. To abuse this misconfiguration, the attacker needs `GenericWrite` over any account A that is allowed to enroll in the certificate template to compromise account B (target).

ESC10 — Weak Certificate Mappings

Description

ESC10 refers to two registry key values on the domain controller.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

account A that is allowed to enroll in a certificate with client authentication to compromise account B (target).

Unfortunately, these registry keys cannot be read by a low-privileged user remotely. However, if you ever find yourself in a scenario, where you have `GenericWrite` over any account, it might be worth trying each abuse case nonetheless.

Examples

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

First, we obtain the hash of `Jane` with for instance Shadow Credentials (using our `GenericWrite`).

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Notice that the `userPrincipalName` in the certificate is `Administrator` and that the issued certificate contains no “object SID”.

Then, we change back the `userPrincipalName` of `Jane` to be something else,

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

And voilà.

ESC10(Case 1)

Conditions:

- StrongCertificateBindingEnforcement set to 0

Requisites:

- Generate a new account A to compromise any account B

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Next, we change the `userPrincipalName` of `Jane` to be `Administrator`. Notice that we're leaving out the `@corp.local` part.

This is not a constraint violation, since the `Administrator` user's `userPrincipalName` is `Administrator@corp.local` and not `Administrator`.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Now, if we try to authenticate with the certificate, we will receive the NT hash of the Administrator@corp.local user. You will need to add -domain <domain> to your command line since there is no domain specified in the certificate.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Next, we change the `userPrincipalName` of `Jane` to be `DC$@corp.local`.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Then, we change back the `userPrincipalName` of `Jane` to be something else, like her original `userPrincipalName` (`Jane@corp.local`).

Now, since this registry key applies to Schannel, we must use the certificate for authentication via Schannel. This is where Certipy's new `-ldap-shell`

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Conclusion

In this blog post, we looked at some new features of Certipy and the forked BloodHound GUI that I changed to have full PKI support. Furthermore, we looked at the new ESCs — which are not as juicy as ESC1 or ESC8 — but I have seen many environments where everyone or a specific group had `GenericWrite` over a single user or computer. On top of this, we might see more and more admins change these registry key values or enabling the vulnerable flag on a template — simply because it makes thing work — just like ESC6.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Written by Oliver Lyak

319 Followers · Editor for IFCR

Twitter: <https://twitter.com/ly4k> Github: <https://github.com/ly4k/>

Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month