What is ESC5?

ESC5 is an AD CS abuse where a low-privileged account has control over an AD object the PKI relies on rather than over a template: the CA's computer account, the CA configuration containers under the Configuration partition, or related objects. Compromising one of these can let an attacker alter CA behaviour, reach the CA host, or enable other ESC paths. It is a reminder that certificate security depends on the access control of the objects around the CA, not just templates.

HOW IT WORKS

01 The abuse and payload

ESC5 is less a single command and more a pivot: the attacker uses control of a PKI-adjacent object to reach the CA or enable another path.

- Enumerate PKI object permissions: `certipy find -u user@corp.local -p pass -dc-ip <ip>` (reports CA and object security)
- If the attacker controls the CA host computer account, they can pursue RBCD or host takeover, then issue or forge certificates directly.
- If they control a configuration object, they may enable ESC6-style behaviour or add trusted certificates.

The specifics depend on which object is exposed.

> **WIDEN THE AUDIT**
>
> *Do not stop at templates. Check who can write the CA computer object and the Configuration-partition PKI containers. ESC5 lives in those object ACLs.*

HOW TO DEFEND

- Audit ACLs on every PKI object, not just templates: the CA host account, Enrollment Services, NTAuthCertificates, and the certificate-templates container.
- Treat the CA host as Tier 0 and protect its computer account like a Domain Controller.
- Remove write or owner rights from non-administrative principals on these objects.
- Run BloodHound to find paths to PKI objects and the CA host.

SOURCES

[1] Microsoft: Active Directory Certificate Services

[2] MITRE ATT&CK Enterprise Matrix

[3] NIST SP 800-115 Technical Guide to Security Testing

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-esc5

Open online