

# Edit misconfigured certificate templates ACL (ESC4) - Microsoft Defender for Identity

 [learn.microsoft.com/en-us/defender-for-identity/security-assessment-edit-misconfigured-acl](https://learn.microsoft.com/en-us/defender-for-identity/security-assessment-edit-misconfigured-acl)

AbbyMSFT

 Screenshot of the Edit misconfigured certificate templates ACL (ESC4) recommendation.

This article describes Microsoft Defender for Identity's **Misconfigured certificate template ACL** security posture assessment report.

Certificate templates are Active Directory objects with an ACL controlling the access to the object. Besides determining enrollment permissions, the ACL also determines permissions for editing the object itself.

If for any reason, there's an entry in the ACL that grants a built-in, unprivileged group with permissions that allow for template setting changes, an adversary can introduce a template misconfiguration, escalate privileges, and compromise the entire domain.

Examples of built-in, unprivileged groups are *Authenticated users*, *Domain users*, or *Everyone*. Examples of permissions that allow for template setting changes are *Full control* or *Write DACL*.

1. Review the recommended action at <https://security.microsoft.com/securescore?viewid=actions> for a misconfigured certificate template ACL. For example:

 Screenshot of the Edit misconfigured certificate templates ACL (ESC4) recommendation.

2. Research why the template ACL might be misconfigured.
3. Remediate the issue by removing any entry that grants unprivileged group permissions that allow tampering with the template.
4. Remove the certificate template from being published by any CA if they're not needed.

Make sure to test your settings in a controlled environment before turning them on in production.

#### Note

While assessments are updated in near real time, scores and statuses are updated every 24 hours. While the list of impacted entities is updated within a few minutes of your implementing the recommendations, the status may still take time until it's marked as **Completed**.

- [Learn more about Microsoft Secure Score](#)
- [Check out the Defender for Identity forum!](#)