Edit misconfigured enrollment agent certificate template (ESC3) - Microsoft Defender for Identity

learn.microsoft.com/en-us/defender-for-identity/security-assessment-edit-misconfigured-enrollment-agent

AbbyMSFT

Screenshot of the Edit misconfigured enrollment agent certificate template (ESC3) recommendation.

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

Typically, users have an Enrollment Agent that enrolls their certificates for them. Under specific circumstances, Enrollment Agent certificates can enroll certificates for any eligible user, posing a risk to your organization.

When Microsoft Defender for Identity reports about Enrollment Agent certificate templates that endanger your organization, risky Enrollment Agent templates are listed on the **Exposed entities** pane.

1. Review the recommended action at https://security.microsoft.com/securescore?viewid=actions for misconfgured enrollment agent certificate templates. For example:

   Screenshot of the Edit misconfigured enrollment agent certificate template (ESC3) recommendation.

2. Remediate the issues by performing at least one of the following steps:

   - Remove the *Certificate request agent* EKU.
   - Remove overly permissive enrollment permissions, which allow any user to enroll certificates based on that certificate template. Templates marked as vulnerable by Defender for Identity have at least one access list entry that allows enrollment for a built-in unprivileged group, making this exploitable by any user. Examples of built-in, unprivileged groups are *Authenticated Users* or *Everyone*.
   - Turn on the CA certificate *Manager approval* requirement.
   - Remove the certificate template from being published by any CA. Templates that aren't published can't be requested, and therefore can't be exploited.
   - Use Enrollment Agent restrictions on the Certificate Authority level. For example, you might want to restrict which users are allowed to act as an Enrollment Agent, and which templates can be requested.

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!