# Enforce encryption for RPC certificate enrollment interface (ESC11) - Microsoft Defender for Identity

learn.microsoft.com/en-us/defender-for-identity/security-assessment-enforce-encryption-rpc

AbbyMSFT


11/27/2024

This article describes Microsoft Defender for Identity's **Enforce encryption for RPC certificate enrollment** security posture assessment report.

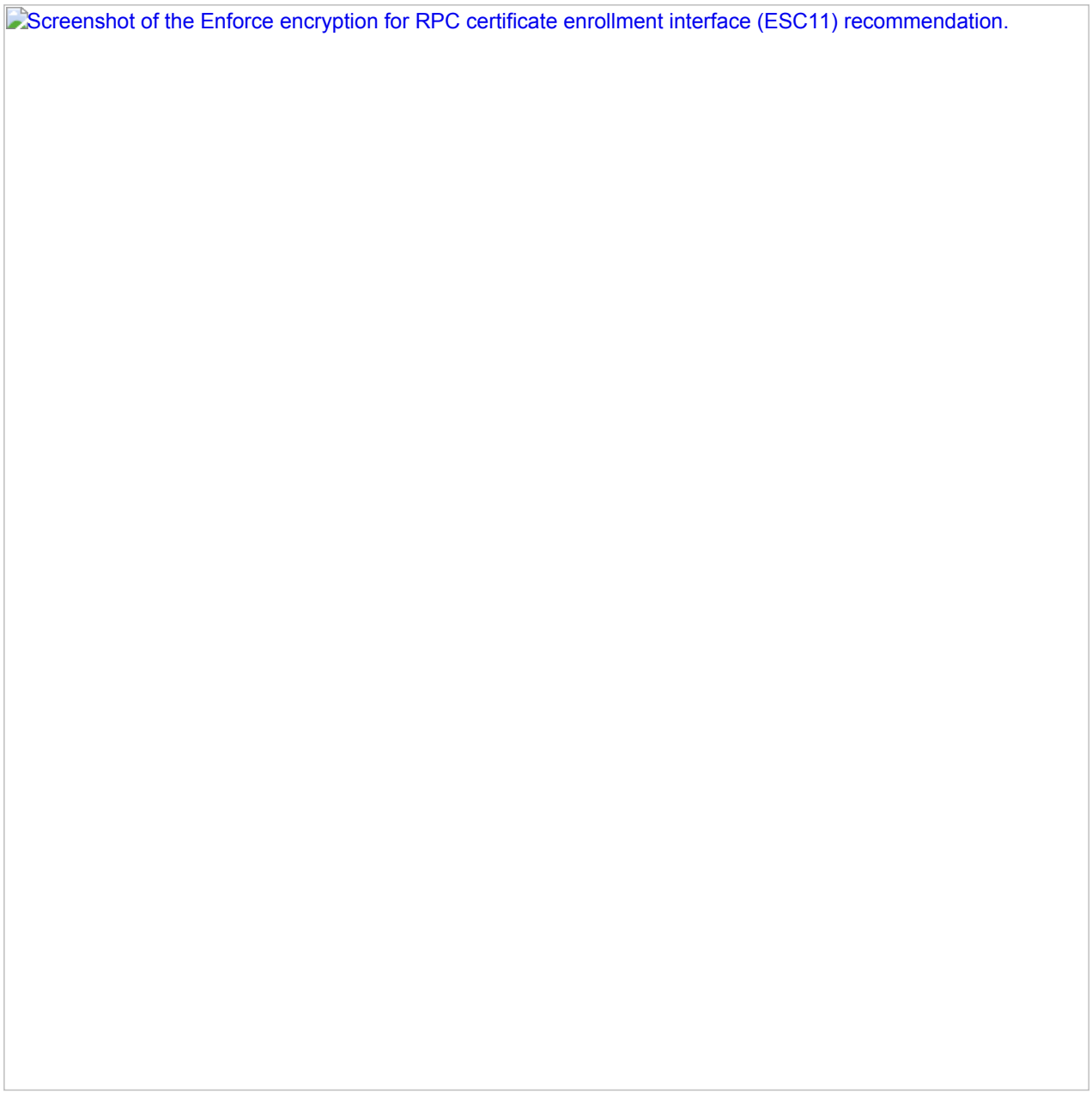
Active Directory Certificate Services (AD CS) supports certificate enrollment using the RPC protocol, specifically with the MS-ICPR interface. In such cases, the CA settings determine the security settings for the RPC interface, including the requirement for packet privacy.

If the `IF_ENFORCEENCRYPTICERTREQUEST` flag is turned on, the RPC interface only accepts connections with the `RPC_C_AUTHN_LEVEL_PKT_PRIVACY` authentication level. This is the highest authentication level, and requires each packet to be signed and encrypted so as to prevent any kind of relay attack. This is similar to `SMB Signing` in the SMB protocol.

If the RPC enrollment interface doesn't require packet privacy, it becomes vulnerable to relay attacks (ESC11). The `IF_ENFORCEENCRYPTICERTREQUEST` flag is on by default, but is often turned off to allow clients that can't support the required RPC authentication level, such as clients running Windows XP.

This assessment is available only to customers who have installed a sensor on an AD CS server. For more information, see New sensor type for Active Directory Certificate Services (AD CS).

1. Review the recommended action at https://security.microsoft.com/securescore?viewid=actions for enforcing encryption for RPC certificate enrollment. For example:

2. Research why the `IF_ENFORCEENCRYPTICERTREQUEST` flag is turned off.

3. Make sure to turn the `IF_ENFORCEENCRYPTICERTREQUEST` flag on to remove the vulnerability.

   To turn on the flag, run:

   Windows Command Prompt

   ```
   certutil -setreg CA\InterfaceFlags +IF_ENFORCEENCRYPTICERTREQUEST
   ```

   To restart the service, run:

   Windows Command Prompt

   ```
   net stop certsvc & net start certsvc
   ```

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!

Training

Module

Protect email with Microsoft Purview Message Encryption - Training

Protect email with Microsoft Purview Message Encryption

Certification

Microsoft Certified: Information Security Administrator Associate - Certifications

As an Information Security Administrator, you plan and implement information security of sensitive data by using Microsoft Purview and related services.