[MICROSOFT ACTIVE DIRECTORY]

Kerberos RC4 Retirement: Key 2026 Changes & Actions

Microsoft is retiring default RC4 use in Kerberos through a staged rollout in 2026. Organizations must update their encryption settings or risk authentication failures in legacy applications.

[WHAT'S CHANGING?]

January 2026 – Audit Only

- New logs show where RC4 is still being used
- No encryption changes applied automatically
- Purpose: inventory and understand RC4 dependencies

April 2026 – Enforcement Begins

- Windows Updates enable AES-by-default for Kerberos
- Manual rollback is possible via a new registry key if issues occur
- Apps still relying on RC4 may start failing authentication

July 2026 – Full Enforcement

- Manual rollback is no longer supported
- RC4 works only if explicitly set on an account or domain controller (not recommended)
- Any unremediated system still using RC4 will break

[WHAT YOU NEED TO DO]

Inventory RC4 Usage (Now–April 2026)

- Review System Events (201–209) and Security Events 4768/4769
- Identify service accounts and legacy systems still using RC4

Fix Root Causes (Now–Apr 2026)

- Reset passwords on service accounts with old passwords to generate AES keys
- Update account encryption settings to enable AES and remove RC4 where possible
- For legacy systems: Explicitly allow RC4 (temporary) and prioritize remediation

Prepare for April Changes (Now–Apr 2026)

- Use the `RC4DefaultDisablementPhase` setting to test Enforcement mode early
- Coordinate with app owners to update configs, keytabs, and dependencies
- Validate that authentication works with AES

Final Hardening (By July 2026)

- Verify all accounts / systems are using AES or are manually configured for RC4
- Monitor events to ensure no new RC4 tickets appear
- If RC4 is no longer required, enforce AES-only policies on domain controllers

Need help or have questions?

CONTACT US
+1 844 267 0804
info@ravenswoodtechnology.com

RAVENSWOOD TECHNOLOGY GROUP

Microsoft Solutions Partner