Silverfort

RC4 remediation readiness checklist

Are you prepared for Microsoft's July 2026 deadline?

Microsoft's enforcement of RC4 encryption deprecation in Kerberos authentication is already underway. **With the final enforcement deadline in July 2026, organizations that haven't mapped their RC4 dependencies risk authentication failures, application downtime, and permanent blind spot in their Active Directory (AD) security**. Follow this checklist to assess your readiness and share with your Identity Security team members.

---

1. Do you know which accounts have ***msDS-SupportedEncryptionTypes*** undefined?

Accounts without an explicitly defined ***msDS-SupportedEncryptionTypes*** attribute have historically defaulted to allowing RC4. Every undefined account has a potential RC4 dependency—and most environments have thousands of them.

---

2. Can you identify which service accounts have never had AES keys generated?

Service accounts whose passwords were last set before Windows Server 2008 were never issued AES keys. These accounts can only authenticate using RC4 and are the most likely to break when enforcement hits—but they're invisible without the right visibility tools.

---

3. Do you know which machine accounts are tied to legacy systems that can't support AES?

Devices running Windows versions older than Server 2008 don't support AES at all. Without a clear inventory of these systems, you risk unexpected authentication failures—and no time to act before the July deadline.

---

4. Do you know whether human user accounts in your environment are also authenticating with RC4—not just service and machine accounts?

RC4 exposure isn't limited to service and machine accounts. Human user accounts can also authenticate using RC4—particularly in environments with legacy systems or misconfigured endpoints. Without visibility across all account types, your RC4 exposure assessment is incomplete.

5. Can you see where RC4 is actively being used in your authentication traffic right now?

Configuration checks alone won't provide you with complete visibility. An account can appear correctly configured and still be using RC4 in authentication traffic due to client-side limitations or legacy application behavior. Real-time authentication visibility is the only way to know for certain.

How Silverfort provides you visibility into RC4 exposure

With **Silverfort's ISPM**, you gain continuous, real-time visibility into RC4 exposure across your AD environment—without any additional configuration or scripting.

Silverfort's ISPM automatically surfaces ***Weak Encryption (Users)*** and ***Weak Encryption (Servers)*** risk indicators when weak encryption is detected in authentication traffic in real time—giving you an immediate, actionable list of accounts where RC4 has actually been observed, across all account types.

With Silverfort's ISPM you can broaden the visibility scope with two additional categories that address the root causes of RC4 dependencies:

- **Users with Old Passwords** identifies service accounts most likely to be carrying RC4-only keys.
- **Old Operating Systems** surfaces devices that don't support AES—giving you a clear view of which machine accounts need attention before enforcement hits.

To analyze RC4 encryption usage in real time, **Silverfort's Authentication Logs** enable you filter by the ***Weakly_encrypted_reply*** and ***Weakly_encrypted_ticket risk*** indicators to get per-authentication visibility into exactly where RC4 is being used—including the account involved, source host, target service, and domain controller.

Ready to see where RC4 is hiding in your environment? Schedule a call with one of our experts.

About Silverfort

Silverfort secures every dimension of identity—humans or machines across the cloud and on-prem. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.