ExacqVision Client and Enterprise Manager LDAP SSO Login Failures After April 2026 Windows Updates

KB Number: 23996
Published: 28/04/2026

Introduction

Microsoft security updates beginning April 2026 changed Kerberos behavior so that RC4 encryption is no longer implicitly allowed (Microsoft KB ID: 5073381). On domain controllers with a defined DefaultDomainSupportedEncTypes registry value, behavior will not be functionally impacted by these changes. However, an Audit event KDCSVC Event ID: 205 will be logged in the System event log if the existing DefaultDomainSupportedEncTypes configuration is insecure (for example, when an RC4 cipher is used).

How this affects exacqVision LDAP or SSO user account authentication:

If the exacqVision LDAP/Kerberos service account in use for Enterprise Manager or exacqVision Client:

-Does not support AES encryption, or

-Is configured for RC4 only, or

-Has msDS-SupportedEncryptionTypes unset

Kerberos authentication will fail. This may result in user log-in status showing:

" Client-Side Kerberos Error" or "Server-Side Kerberos Error"

This is expected Microsoft behavior and not a defect in exacqVision.

Resolution:

Step 1 - Check Service Account Encryption Type

From an elevated PowerShell session:

Get-ADUser exacqServiceAccount -Properties msDS-SupportedEncryptionTypes |

Select Name, msDS-SupportedEncryptionTypes

Interpret the Value returned:

Not set = Legacy (RC4 only) ❌ Not supported

4 = RC4 only ❌ Not supported

24 = AES128 + AES256 ✅ Supported

Step 2 - Enable AES Encryption

If the value is unset or 4, enable AES:

```
Set-ADUser exacqServiceAccount `
 -Replace @{msDS-SupportedEncryptionTypes=24}
```

In the examples used, the accounts in use is "exacqServiceAccount". Replace this value with the desired value for your target account.

Step 3 - Reset Service Account Password (Required)

```
Set-ADAccountPassword exacqServiceAccount -Reset
```

Critical: AES Kerberos keys are not generated until the password is reset.

Verification:

Attempt LDAP SSO login again to verify successful authentication.

Secondary Verification:

On Domain Controllers, review System Event Log:

Source: KDCSVC

Event IDs: 201-209

Event ID 205 should no longer appear, as a confirmation.

On domain controllers with a defined DefaultDomainSupportedEncTypes registry value, an Audit event KDCSVC Event ID: 205 will be logged in the System event log if the existing DefaultDomainSupportedEncTypes configuration is insecure (for example, when an RC4 cipher is used).

Re-enabling RC4 after the April 2026 updates is not recommended by Microsoft due to security risk.

If AES is enabled, and password reset has been confirmed, but failures persist:

- Verify each Client and Server machine can resolve each Domain Controller

-Verify correct service account/SPN is being used.

- Remove and Re-add the DNS record for the affected server

- Try UPN vs. sAMAccountName vs. SSO log in methods

- Verify time skew (NTP)