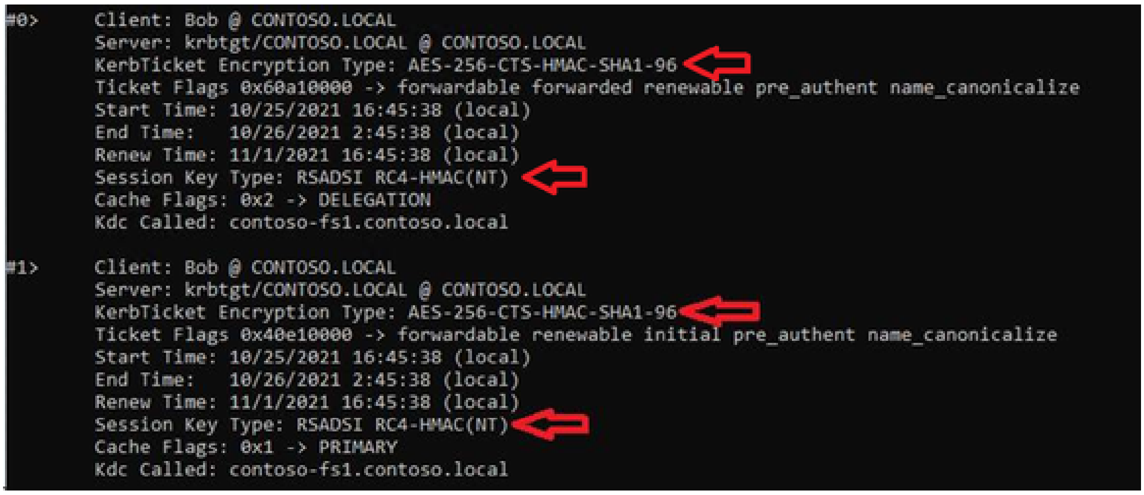
Active Directory Hardening Series - Part 4 – Enforcing AES for Kerberos

techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-directory-hardening-series---part-4-—-enforcing-aes-for-kerberos/4114965



```
#0>     Client: Bob @ CONTOSO.LOCAL
        Server: krbtgt/CONTOSO.LOCAL @ CONTOSO.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 10/25/2021 16:45:38 (local)
        End Time:   10/26/2021 2:45:38 (local)
        Renew Time: 11/1/2021 16:45:38 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x2 -> DELEGATION
        Kdc Called: contoso-fs1.contoso.local

#1>     Client: Bob @ CONTOSO.LOCAL
        Server: krbtgt/CONTOSO.LOCAL @ CONTOSO.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 10/25/2021 16:45:38 (local)
        End Time:   10/26/2021 2:45:38 (local)
        Renew Time: 11/1/2021 16:45:38 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: contoso-fs1.contoso.local
```

Blog Post

Hi everyone, Jerry Devore here again with another installment in my series on Active Directory hardening. This time I want to revisit a topic I previously wrote about in September of 2020 which is enforcing AES for Kerberos. Since I wrote that blog post a few new tips have come my way. Before we dive in here is a quick re-cap of what was previously discussed:

- RC4 encryption for Kerberos is weak and susceptible to roasting attacks.
- The msDS-SupportedEncryptionTypes attribute value of the target account will determine the ticket encryption for service ticket requests (AS-REQ). When the value is blank the KDC will default to RC4.
- By default, users accounts do not have a value for msDS-SupportedEncryptionTypes.
- Disabling RC4 support on **devices** should follow remediation of service accounts. Otherwise RC4 service tickets could be issued for devices that will not accept them.

Update - The January 2025 Cumulative update for server 2016 and newer has added new fields to 4768 and 4769 events on Domain Controllers. Details about this change have been added at the bottom of the page.

Discovering RC4 dependent devices

Identifying devices limited to RC4 is a critical step but has historically been a tricky problem to solve. However, a recently discovered "feature" in 4768 events can help you identity such devices. Previously I suggested analyzing the Ticket Encryption Type field in 4769 events (service ticket requests). At the time I was not focused on the 4768 events since a KDC will encrypt all TGTs with AES if the KRBTGT account has a key for AES. So, what is this new discovery? Drumroll please…. The **Ticket Encryption Type** field in **4768** events reflects the **session key** issued with the TGT. Why does that matter? The session key encryption selection for a TGT is dependent on what was negotiated by the device during the AS-REQ (authentication request). As a result, 4768 events can be used to identify devices that only support RC4.

To demonstrate this behavior I configured a device in my lab to only support RC4 (Network security: Configure encryption types allowed for Kerberos).   As you can see from this screenshot the session key for both the primary and delegation TGT was protected with RC4 while the TGT itself was encrypted with AES.

The 4768 event logged on the domain controller reflects the use of RC4 in the **Ticket Encryption Type** field even though RC4 was only used for the session key. That information can be more useful than reporting the actual ticket encryption since all TGTs will be AES if the KDC supports it.

In the last few years, I have worked with many large organizations as they embarked on a journey to rid their environment of RC4. So far, I have found four types of devices that you might see defaulting to using RC4 in the AS-REQ. They are:

- **Devices with Keytab files** where the only credential available is RC4 (NTLM hash). Those devices will need a new keytab file created using a different cyrpto switch.
- **Non-Windows devices that have been integrated with the domain** (e.g. NAS appliances, Linux, etc). It is possible the device is capable of using AES but is defaulting to RC4.   Check with the OS vendor if you encounter such devices.
- **Windows devices that have AES disabled** using a GPO or the registry setting. By default, 2008 and newer devices support RC4 and AES. There is no scenario where disabling AES on Windows is recommended.
- **Legacy Windows devices** that do not support AES (2003 / XP and earlier). If you have any of those, the corrective action is to decommission them immediately. If that is not possible you should triple your cyber insurance coverage and set an insanely long password on any service account that comes in contact with those devices.

Once you have identified and remediated any device defaulting to RC4 you can ramp up your efforts to enable AES on your SPN enabled service accounts. I still would not update all accounts at the same time but by all means don't be overly timid. The risk of not taking action this area is greater than the risk of hardening your environment.

To be clear, using 4768 events to detect RC4 devices depends on the devices requesting a TGT. If you have an application that uses a keytab to decrypt and read tickets but does not use the account to authenticate to Active Directory, there will be no 4768 events logged for the account. I believe that scenario is rare, but it is worth pointing out that leveraging 4768 events might not catch every last device dependent on RC4.

Even better auditing is being planned

While using 4768 events to find RC4 dependent devices can be extremely useful, more verbose logging of Kerberos tickets is being planned by the product group. What the extra logging will capture, when it will be released and how far back it will be ported is still to be determined. In the meantime, keep moving forward using the auditing currently available.

November 2022 Changes to Kerberos

In 2022 some needed changes were made which caused the KDC to start defaulting to AES session keys. Selection of encryption type for service tickets (TGS) did not change as part of that update, so it is still vitally import to define a value on msDS-SupportedEncryptionTypes for your SPN enabled service accounts. More information on those changes can be found here:

> https://support.microsoft.com/en-us/topic/kb5021131-how-to-manage-the-kerberos-protocol-changes-related-to-cve-2022-37966-fd837ac3-cdec-4e76-a6ec-86e67501407d
>
> What happened to Kerberos Authentication after installing the November 2022/OOB updates? - Microsoft Community Hub

Something that is not discussed in those articles is the change to cross domain referral tickets. Previously it was necessary to enable AES in the trust settings. Otherwise RC4 was used for the referral tickets. That is no longer necessary given referral tickets will now default to AES.   To better illustrate here are a few screenshots from my lab. Joe User resides in the contoso.local domain. When the account attempted to access a resource in the trusted fabrikam.local domain, the referral ticket was issued with AES even though the trust (Trust Domain Object) had no setting for msDS-SupportedEncryptionTypes. If your RC4 remediation project includes a task for enabling AES on your trusts, you can mark that task complete.

If you have been following my series, you know I always conclude with a list of **Do's and Don't** to make sure things go as planned. To avoid disappointing anyone, here is the list.

- **Don't** forget about the lifetime of cached tickets when testing changes. By default, tickets are valid for up to 10 hours. When you change msDS-SupportedEncryptionTypes on an account make sure cached tickets are not skewing your test results.
- **Don't** worry about manually defining msDS-SupportedEncryptionTypes on computer objects of Windows devices. They will update their own attribute automatically. If you apply a policy to manage the Network security: Configure encryption types allowed for Kerberos setting, the device will process the change locally then update the attribute in Active Directory. It is worth mentioning you may see some latency between when the GPO is applied, and the computer object is updated.
- **Do** update your service account (SPN enabled) provisioning process to include setting a value for msDS-SupportedEncryptionTypes. That will ensure RC4 will not creep back into your environment as new accounts are created.
- **Do** know that many password synchronization solutions (e.g ADMT) will only sync the NTLM hash of a user account and not the AES keys for the account. If you are using such a tool to perform a domain migration and the target domain does not support RC4, you will need to reset the account's password in the target domain in order for Kerberos to work.
- **Don't** worry about setting msDS-SupportedEncryptionTypes on user accounts that don't have a SPN. When a domain user logs onto a device, the device's configuration will determine what is used for the AS-REQ. As a result, the session key selected for the user’s tickets is determined by the device and not the user's msDS-SupportedEncryptionTypes attribute.
- **Don't** worry about setting msDS-SupportedEncryptionTypes on the KRBTGT account. As long as the account has AES keys (password reset since 2008R2) and the DFL is greater than 2003, the KDC will issues TGTs encrypted with AES.
- **Do** monitor your domain controller system logs for Event 16 and Event 27. Those will let you know if any account lacks a credential for the supported encryption type. We don't see that often, but it can happen with service accounts that have not had their passwords changed
- **Do** know that RC4 can be disabled at the domain level by creating HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\KDC\DefaultDomainSupportedEncTypes on the domain controllers and setting the value to 0x38. That would be a great way to ensure your environment remains remediated but using that approach for a big bang remediation will be too aggressive for most organizations. For more details on DefaultDomainSupportedEncTypes see this KB5021131.
- **Do** check out this blog post Chris Cartwright wrote which explains how to configure Windows Event Forwarding (WEF) to centrally hunt for RC4 use if you don’t already have a centralize event log solution.
- **Do** disable RC4 on devices using the policy Network security: Configure encryption types allowed for Kerberos **after** you have confirmed the device no longer has any RC4 dependencies.

******************************** **Update** ******************************

The January 2025 cumulative update (1B) added new and very helpful fields to 4768 and 4769 events. Below are examples of the updated events along with tables which describe key fields. The enhancements now make it possible to centrally identify:

- The session key type of both TGTs and Service Tickets.
- The eTypes the Kerberos client advertised it can support in the AS-REQ and TGS-REQ packets. Use this information to identify any device (or keytab) that is not able to support AES
- The available keys for the accounts involved. Use this information to identify accounts that require a password reset in order to support AES.

Account Information	Account Name	Account requesting the TGT
	MSDS-SupportedEncryptionTypes	If the requesting account does not have a value for MSDS-SupportedEncryptionTypes HKLM\System\CurrentControlSet\Services\KDC\DefaultDomainSupportedEncTypes of the authenticating domain controller will determine this value.
	Available Keys	If AES-SHA1 is not reported the password of the requesting account has not been changed since the domain starting supporting AES.
Service Information	Service Name	TGT requests will always list krbtgt as the service name
	MSDS-SupportedEncryptionTypes	The encryption types supported by the krbtgt is determined by the domain and not the value of MSDS-SupportedEncryptionTypes for the krbtgt account.
	Available Keys	If AES-SHA1 is not list the password of the krbtgt account has not changed since the domain began supporting AES
Network Information	Client Address	IP address of the Kerberos client that requested the TGT
	Advertized Etypes	This is the encryption type the client stated it can support in the AS-REQ.
Additional Information	Error Code	0x0 indicates no error with the request. For a list of possible values see this table.
	Ticket Encryption Type	Prior to the January 2025 update this field reported the session key encryption type. It now reports the actual ticket encryption type of the TGT. The client does not read the TGT so the encryption type only needs to be supported by the domain controllers.
	Session Encryption Type	The session key needs to be compatible with the client. Selection is dependent on the client's Adverstized Etypes.
	Pre-Authentication EncryptionType	Pre-Authentication EncryptionType is determined by the client's configuration and should be the strongest value reported in advertized Etypes. If a Windows 2008 or higher device is only reporting RC4 check the policy setting Network security: Configure encryption types allowed for Kerberos

Account Information	Account Name	Account Requesting the Service Ticket (TGS-REQ)
	MSDS-SupportedEncryptionTypes	N/A - requesting accounts MSDS-SupportedEncryptionTypes is not a factor when determine the encryption type of the ticket or session key

Service Information	Service Name	Target account of the ticket request
	MSDS-SupportedEncryptionTypes	The strongest supported value will be used by the KDC to encrypt the service ticket
	Available Keys	If AES-SHA1 is not listed the account password has not been changed since the domain began supporting AES
Network Information	Client Address	IP address of the Kerberos client that requested the Service Ticket
	Advertized Etypes	This is the encryption type the client stated it can support in the TSG-REQ.
Additional Information	Ticket Encryption Type	This is the encryption type to KDC selected for the Service Ticket. If the target account does not have a value for MSDS-SupportedEncryptionTypes the encryption type will default to RC4.
	Session Encryption Type	Encryption type of the session key for the Service Ticket. Starting with the Nov 22 update the session type will default to AES as long as the client advertised it can support AES.

Updated Jan 28, 2025

Version 7.0