
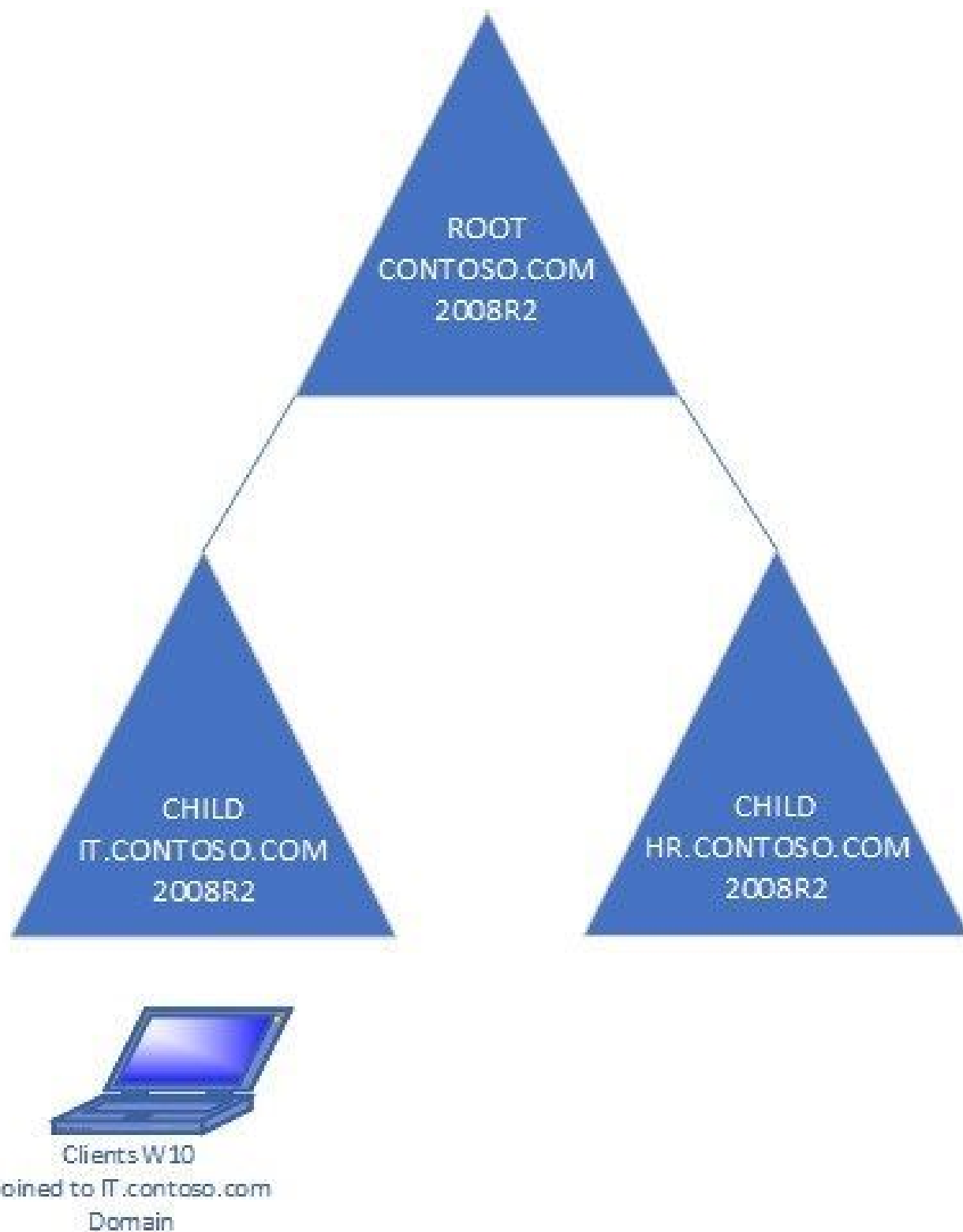


# Tough Questions Answered: Can I disable RC4 Etype for Kerberos on Windows 10?

 [techcommunity.microsoft.com/blog/itopstalkblog/tough-questions-answered-can-i-disable-rc4-etype-for-kerberos-on-windows-10/382718](https://techcommunity.microsoft.com/blog/itopstalkblog/tough-questions-answered-can-i-disable-rc4-etype-for-kerberos-on-windows-10/382718)



**Blog Post**

Today I want to share with you a direct experience from the field.

One customer received a request from their security team to disable the RC4 ETYPE (Encryption Type) for Kerberos for their Windows 10 Clients. The support team created a GPO to disable this Etype without thinking too much about the consequences.

## ENVIRONMENT

The customer have all DCs with Windows Server 2008R2 and the DFL (Domain Functional Level) and the FFL (Forest Functional Level) are set to 2008R2. All Clients are Windows 10 CB (Current Branch) Build 1803.

## THE PROBLEM

The support team created a GPO to disable the RC4 Etype on Windows 10 Clients by using this [GPO](#):

The GPO was applied in the **IT.CONTOSO.COM** domain on the OU of the Windows 10 Clients:

After that, the team responsible of the clients start opening tickets regarding the impossibility of some windows 10 clients to apply the GPOs, so we was involved for the troubleshooting.

## TROUBLESHOOTING

In one of the affected windows 10 clients we noticed this event:

=====

**Log Name: System**

Source: Microsoft-Windows-GroupPolicy

Date: 3/28/2019 11:09:25 AM

**Event ID: 1006**

Task Category: None

Level: Error

Keywords:

User: SYSTEM

Computer: CLIENT01.IT.CONTOSO.COM

Description:

**The processing of Group Policy failed. Windows could not authenticate to the Active Directory service on a domain controller. (LDAP Bind function call failed).**

Look in the details tab for error code and description.

=====

So we have enabled on the Windows 10 Client the **Group Policy Debug Logging** from regedit:

By executing on the client a **GPUPDATE /FORCE** we received the following error message:

And in the debug log (%windir%\debug\usermode\gpsvc.log) of the Group Policy Service, we found the following error message:

\*\*\*\*\*

GPSVC(1478.1d08) 11:25:22:416 SearchDSObject: **Searching**  
**<OU=WIN10\_CLIENT,DC=IT,DC=CONTOSO,DC=COM>**

.....

GPSVC(1478.1d08) 11:25:22:433 EvaluateDeferredGPOs: **Doing an ldap bind to cross-domain <HR.CONTOSO.COM>**

GPSVC(1478.1d08) 11:25:22:448 EvaluateDeferredGPOs: **ldap\_bind\_s failed with = <82>**

GPSVC(1478.1d08) 11:25:22:448 GetGPOInfo: **EvaluateDeferredGPOs failed. Exiting**

GPSVC(1478.1d08) 11:25:22:448 GetGPOInfo: Leaving with 0

\*\*\*\*\*

This kind of error show us that the client is trying to do an LDAP binding the other child Domain **HR.CONTOSO.COM** but why? The client is joined to the **IT.CONTOSO.COM** Domain!!

So we verified all the GPO applied to the Windows 10 clients from the GPMC (Group Policy Management Console) , by looking at the GPO inheritance of the OU, and we found that a GPO from **HR.CONTOSO.COM** was applied to the clients in **IT.CONTOSO.COM**:

As you can see this is my lab, and it is easy to find the GPO 😊 , but in a real production environment you need to check the **details tab** on all the GPO applied in the **inheritance tab** of the Windows 10 Clients OU.

Now we know why the client try to reach the **HR.CONTOSO.COM** Domain during the application of the GPOs, but why is not able to authenticate?

So we verified the eventlog on the DCs and we found this error message:

=====

**Log Name: System**

**Source: Microsoft-Windows-Kerberos-Key-Distribution-Center**

**Date: 3/29/2019 5:17:26 PM**

**Event ID: 14**

**Task Category: None**

**Level: Error**

**Keywords: Classic**

**User: N/A**

Description:

**While processing an AS request for target service krbtgt, the account Administrator did not have a suitable key for generating a Kerberos ticket (the missing key has an ID of 1). The requested etypes : 18 17 3. The accounts available etypes : 23 -133 -128.** Changing or resetting the password of Administrator will generate a proper key.

=====

This event show us that we have an issue related to the ETYPE for Kerberos.

## RESOLUTION

If the Windows 10 clients need to authenticate in the other child domain (HR.CONTOSO.COM), need to use the default **Parent-Child** trusts, but this trusts by default uses **RC4** as **ETYPE** for Kerberos.

So if you want to enable AES on this trusts you need to enable this flag (disabled by default) in the trusts properties:

Because the Parent-Child trust is a Two-way transitive you need to enable this flag on the parent (CONTOSO.COM) and on the child's domains (IT & HR.CONTOSO.COM).

## TO KEEP IN MIND

If you set this flag in the trusts Properties:

You are enabling only **AES 128** and **AES 256** on the Trust, the **RC4** will be **Disabled**

If you want to configure the trust to support RC4,AES 128 and AES258, you need to use the **KSETUP** command line utility.

In this example I'm connected to the **CONTOSO.COM** DC and from a command line I will enable the selected Etypes on the trust for **IT.CONTOSO.COM**:

=====

```
ksetup /setenctypeattr it.contoso.com RC4-HMAC-MD5 AES128-CTS-HMAC-SHA1-96  
AES256-CTS-HMAC-SHA1-96
```

=====

If you want to verify if you have done a good job with the **KSETUP**, you can use the **ADSIEdit**, and verify the **msDS-SupportedEncryptionTypes** attribute of the Trust if it is set to **0x1C**:

## THE FINAL ANSWER

At the end, **can I disable the RC4 as an ETYPE for Kerberos on my Windows 10 Clients?**

If you have all your DCs at least 2008R2 with DFL and FFL 2008R2, Yes you can, but remember:

1. Test always the new configuration of ETYPE in Pre-Production environment first!
2. Remember to Enable the AES ETYPE on the Trusts.
3. If all the tests in Pre-Production gone well, then you can start to apply the GPO on a small set of friendly Clients, **and prepare always a rollback plan.**
4. Test all your core business Applications on this small set of clients.
5. Apply the GPO to an increasing number of groups of clients but always step by step.

Updated Apr 27, 2021

Version 5.0

Windows Server



ViniX

Copper Contributor

Feb 20, 2025