

# Find Active Directory accounts configured for DES and RC4 Kerberos encryption

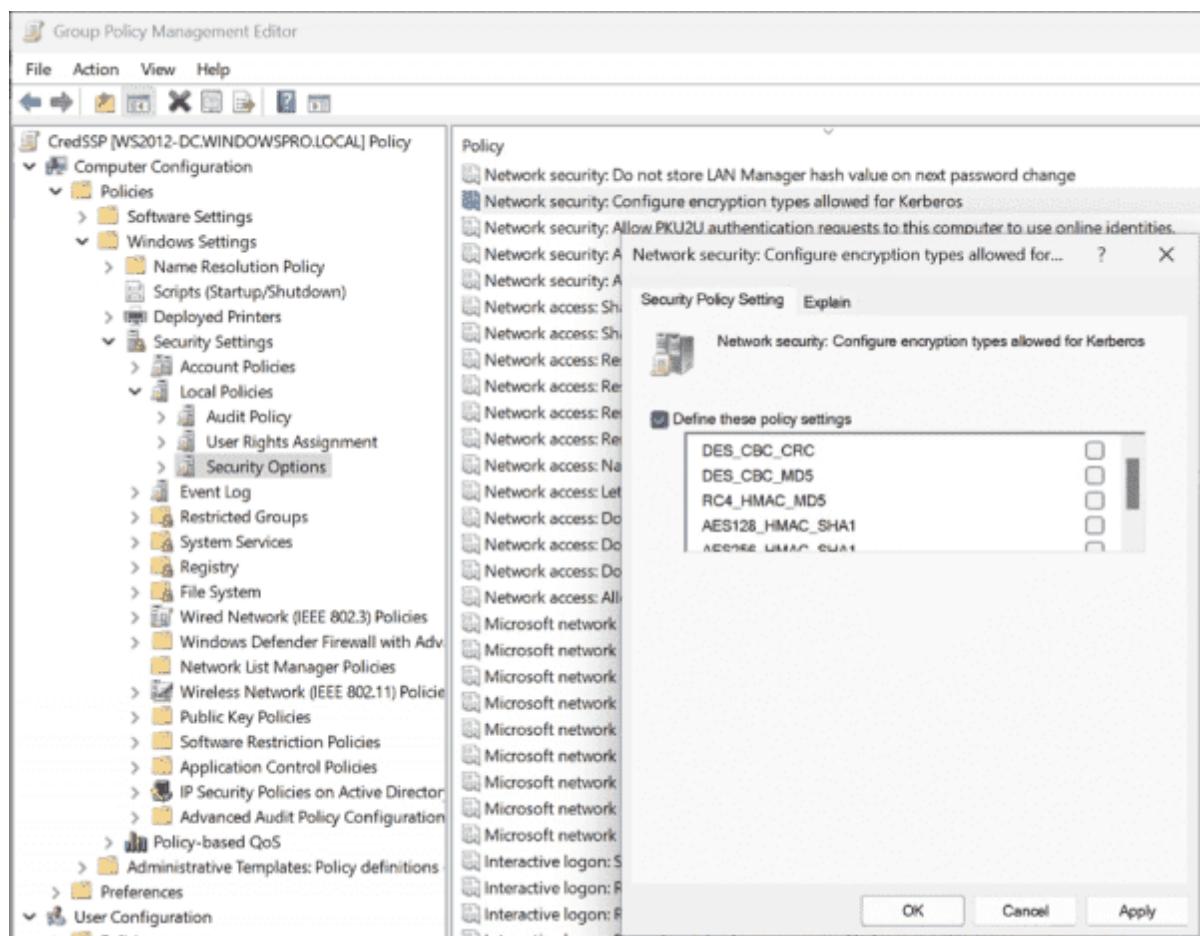
4 [4sysops.com/archives/find-active-directory-accounts-configured-for-des-and-rc4-kerberos-encryption](https://4sysops.com/archives/find-active-directory-accounts-configured-for-des-and-rc4-kerberos-encryption)

Wolfgang Sommergut Mon, Dec 19 2022 encryption, active directory, security 4

While DES has long been considered insecure, CVE-2022-37966 accelerates the departure of RC4 for the encryption of Kerberos tickets. If you have not explicitly assigned an algorithm to accounts, then AES will be used in the future. You can use PowerShell to determine which accounts are vulnerable to weak encryption.

Microsoft's automatic switch to stronger encryption may be hindered by an unfavorable configuration in some environments. This is the case if specific algorithms have been explicitly assigned to certain accounts.

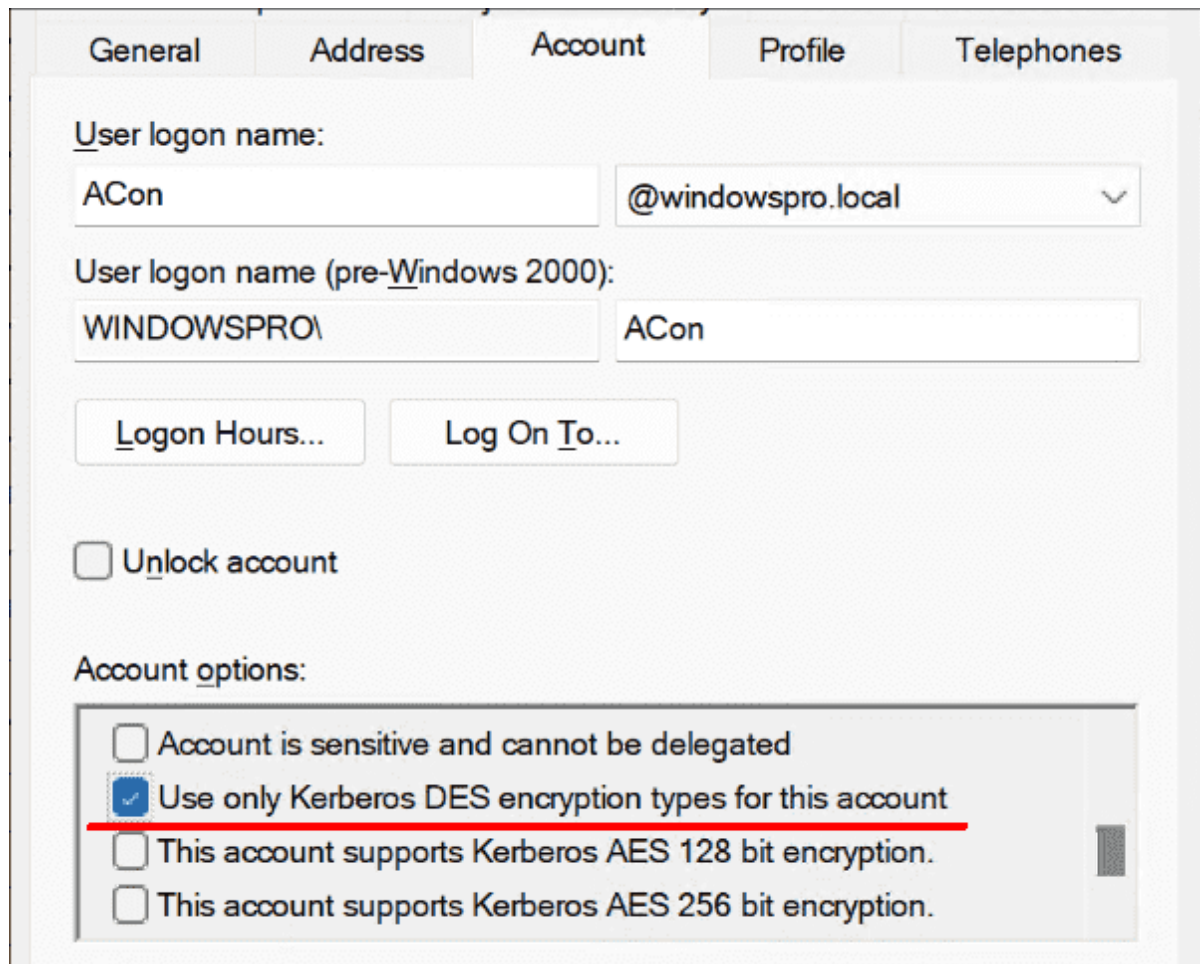
You should also check whether certain encryption methods have been configured by group policy. The setting *Network Security: Configure encryption types allowed for Kerberos* is responsible for this. It can be found under *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options*.



Algorithms that the Kerberos client may use can be defined using this Group Policy

If, among others, DES has been enabled here, which is no longer supported in Windows by default, then you should check whether the *Use only Kerberos DES encryption types for this account* flag in the *UserAccountControl* attribute is set for any accounts. If it is, the affected accounts are limited to the outdated and insecure DES algorithm, and you should disable this setting.

For individual users, you can do this in *Active Directory Users and Computers* under the *Account* tab.



DES can be set as the only algorithm using AD Users and Computers

If you want to find all users that were configured this way, the following PowerShell command will do the trick:

```
Get-ADUser -Filter 'UserAccountControl -band 0x200000'
```

The bitwise *and* of *UserAccountControl* with 0x200000 shows whether the DES encryption flag is set. If you want to remove this, you can do so as follows:

```
Get-ADUser -Filter 'UserAccountControl -band 0x200000' |  
foreach {Set-ADAccountControl -Identity $_ -UseDESKeyOnly $false}
```

## Check for RC4

---

Active Directory is inconsistent in storing the preferred algorithms for Kerberos encryption. While the *UserAccountControl* attribute is used to enforce the exclusive use of DES, the general encryption configuration is stored in *msDS-SupportedEncryptionTypes*.

This attribute, with the data type *unsigned long*, also serves as a bitmask, so you have to check the status of each flag to see which algorithms are allowed. In the case of RC4, this is the third bit. Accordingly, a query would look like this:

```
Get-ADUser -Filter 'msDS-SupportedEncryptionTypes -band 0x4' -Properties msDS-SupportedEncryptionTypes |
```

```
Select name, msDS-SupportedEncryptionTypes
```

## Remove RC4 from the attribute

---

To remove RC4 from these accounts, you can proceed as follows:

```
Get-ADUser -Filter 'msDS-SupportedEncryptionTypes -band 0x4' -Properties msDS-SupportedEncryptionTypes |
```

```
foreach{
```

```
$NewEncTyp = $_.'msDS-SupportedEncryptionTypes' - 0x4
```

```
Set-ADUser -Identity $_ -replace @{'msDS-SupportedEncryptionTypes'=$NewEncTyp}
```

```
}
```

Subtracting 4 sets the third bit to zero, but the values for all other algorithms are preserved.

On the other hand, if you want to completely rewrite the attribute, you can use the *KerberosEncryptionType* parameter for this purpose:

```
Get-ADUser -Filter 'msDS-SupportedEncryptionTypes -band 0x4' -Properties msDS-SupportedEncryptionTypes |
```

```
foreach{
```

```
Set-ADUser -Identity $_ -KerberosEncryptionType "AES128,AES256"
```

```
}
```

In the above example, we assign the two AES algorithms to all accounts that have previously configured RC4 as a permitted algorithm. If we use "none" as the value for the parameter, then the attribute is set to 0x0, and the account thus uses the default method for encryption.

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-ADUser -Filter 'msDS-SupportedEncryptionTypes -band 0x4' `
>> -Properties msDS-SupportedEncryptionTypes | foreach{
>>     Set-ADUser -Identity $_ -KerberosEncryptionType "none"
>> }
>>
PS C:\WINDOWS\system32> Get-ADUser -Filter 'msDS-SupportedEncryptionTypes -band 0x4'
PS C:\WINDOWS\system32>
```

Reset attribute msDS SupportedEncryptionTypes to 0x0 with Set ADUser

## Document encryption type for all users

---

If you want to document the status of the AD attribute for Kerberos encryption, you can do so using the [table in this blog post](#). It contains not only the values for the individual algorithms but also for all combinations of them.

The following script generates CSV output for all user accounts, which you can write to a file if needed:

```
$encTypes = @("Not defined - defaults to
RC4_HMAC_MD5","DES_CBC_CRC","DES_CBC_MD5","DES_CBC_CRC |
DES_CBC_MD5","RC4","DES_CBC_CRC | RC4","DES_CBC_MD5 |
RC4","DES_CBC_CRC | DES_CBC_MD5 | RC4","AES 128","DES_CBC_CRC | AES
128","DES_CBC_MD5 | AES 128","DES_CBC_CRC | DES_CBC_MD5 | AES 128","RC4
| AES 128","DES_CBC_CRC | RC4 | AES 128","DES_CBC_MD5 | RC4 | AES
128","DES_CBC_CRC | DES_CBC_MD5 | RC4 | AES 128","AES 256","DES_CBC_CRC
| AES 256","DES_CBC_MD5 | AES 256","DES_CBC_CRC | DES_CBC_MD5 | AES
256","RC4 | AES 256","DES_CBC_CRC | RC4 | AES 256","DES_CBC_MD5 | RC4 | AES
256","DES_CBC_CRC | DES_CBC_MD5 | RC4 | AES 256","AES 128 | AES
256","DES_CBC_CRC | AES 128 | AES 256","DES_CBC_MD5 | AES 128 | AES
256","DES_CBC_MD5 | DES_CBC_MD5 | AES 128 | AES 256","RC4 | AES 128 | AES
256","DES_CBC_CRC | RC4 | AES 128 | AES 256","DES_CBC_MD5 | RC4 | AES 128 |
AES 256","DES+A1:C33_CBC_MD5 | DES_CBC_MD5 | RC4 | AES 128 | AES 256")

$EncVal = Get-ADUser -SearchBase "OU=Finance,DC=contoso,DC=com" `
-Filter * -properties msDS-SupportedEncryptionTypes

foreach($e in $EncVal){

try {

$e.Name + "," + $encTypes[$e.'msDS-SupportedEncryptionTypes']

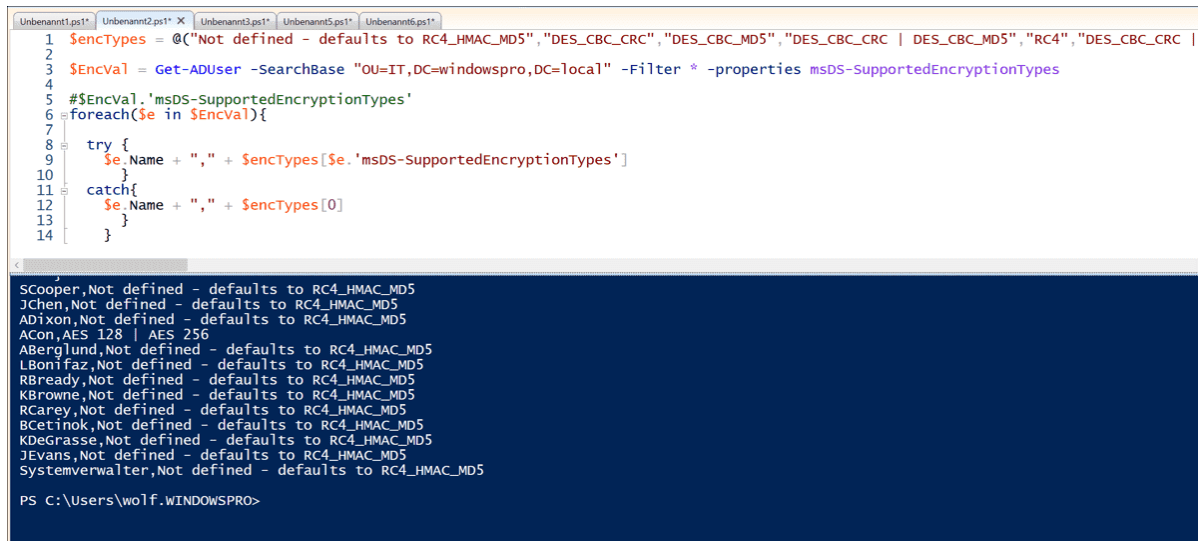
}

catch{

$e.Name + "," + $encTypes[0]
```

```
}}
```

The try/catch section catches errors caused by the attribute not containing any value if the user has never logged in.



```
1 $encTypes = @("Not defined - defaults to RC4_HMAC_MD5", "DES_CBC_CRC", "DES_CBC_MD5", "DES_CBC_CRC | DES_CBC_MD5", "RC4", "DES_CBC_CRC |  
2  
3 $encVal = Get-ADUser -SearchBase "OU=IT,DC=windowspro,DC=local" -Filter * -properties msDS-SupportedEncryptionTypes  
4  
5 # $encVal.'msDS-SupportedEncryptionTypes'  
6 foreach($e in $encVal){  
7  
8     try {  
9         $e.Name + ", " + $encTypes[$e.'msDS-SupportedEncryptionTypes']  
10    }  
11    catch{  
12        $e.Name + ", " + $encTypes[0]  
13    }  
14 }
```

```
SCooper,Not defined - defaults to RC4_HMAC_MD5  
JChen,Not defined - defaults to RC4_HMAC_MD5  
ADixon,Not defined - defaults to RC4_HMAC_MD5  
ACon,AES 128 | AES 256  
ABerglund,Not defined - defaults to RC4_HMAC_MD5  
LBonifaz,Not defined - defaults to RC4_HMAC_MD5  
RBready,Not defined - defaults to RC4_HMAC_MD5  
KBrowne,Not defined - defaults to RC4_HMAC_MD5  
RCarey,Not defined - defaults to RC4_HMAC_MD5  
BCetinok,Not defined - defaults to RC4_HMAC_MD5  
KDeGrasse,Not defined - defaults to RC4_HMAC_MD5  
JEvans,Not defined - defaults to RC4_HMAC_MD5  
Systemverwalter,Not defined - defaults to RC4_HMAC_MD5  
  
PS C:\Users\wolf.WINDOWSPRO>
```

Document status of msDS SupportedEncryptionTypes for all accounts

According to the table, a value of 0x0 corresponds to "Not defined - defaults to RC4\_HMAC\_MD5". However, this changes with [KB5019081](#) so that Microsoft will use AES as the default in the future. This should be updated accordingly in the script.

## Summary

Since Kerberos tickets are often a target for attacks to gain elevated privileges, you should make sure that Active Directory uses strong encryption for this purpose. DES and now RC4 do not meet this requirement.

## Subscribe to 4sysops newsletter!