



## Ciphersuiten managen

Mit der Powershell können wir nach Ciphersuiten suchen, unsichere deaktivieren und uns die Eigenschaften der Ciphersuiten anzeigen lassen.

### # Welche Ciphersuiten sind dem SRVFILE bekannt und wie sind die Eigenschaften?

Get-TlsCipherSuite | Format-Table Name, Exchange, Cipher, Hash, Certificate

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Ciphersuiten managen.ps1* X
1 # Welche Ciphersuiten sind dem SRVFILE bekannt?
2 Get-TlsCipherSuite | Format-Table Name, Exchange, Cipher, Hash, Certificate
3
PS C:\Windows\system32> Format-Table Name, Exchange, Cipher, Hash, Certificate
PS C:\Windows\system32> Get-TlsCipherSuite | Format-Table Name, Exchange, Cipher, Hash, Certificate

Name Exchange Cipher Hash Certificate
-----
TLS_AES_256_GCM_SHA384 AES
TLS_AES_128_GCM_SHA256 AES
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH AES ECDSA
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH AES ECDSA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH AES RSA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH AES RSA
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH AES RSA
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH AES RSA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH AES SHA256 ECDSA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH AES SHA384 RSA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH AES SHA256 RSA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH AES SHA1 ECDSA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ECDH AES SHA1 ECDSA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH AES SHA1 ECDSA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH AES SHA1 RSA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH AES SHA1 RSA
TLS_RSA_WITH_AES_256_GCM_SHA384 RSA AES RSA
TLS_RSA_WITH_AES_128_GCM_SHA256 RSA AES RSA
TLS_RSA_WITH_AES_256_CBC_SHA256 RSA AES SHA256 RSA
TLS_RSA_WITH_AES_128_CBC_SHA256 RSA AES SHA256 RSA
TLS_RSA_WITH_AES_256_CBC_SHA RSA AES SHA1 RSA
TLS_RSA_WITH_AES_128_CBC_SHA RSA AES SHA1 RSA
TLS_RSA_WITH_3DES_EDE_CBC_SHA RSA 3DES SHA1 RSA
TLS_RSA_WITH_NULL_SHA256 RSA SHA256 RSA
TLS_RSA_WITH_NULL_SHA RSA SHA1 RSA
TLS_PSK_WITH_AES_256_GCM_SHA384 PSK AES
TLS_PSK_WITH_AES_128_GCM_SHA256 PSK AES
TLS_PSK_WITH_AES_256_CBC_SHA384 PSK AES SHA384
TLS_PSK_WITH_AES_128_CBC_SHA256 PSK AES SHA256
TLS_PSK_WITH_NULL_SHA384 PSK SHA384
TLS_PSK_WITH_NULL_SHA256 PSK SHA256

PS C:\Windows\system32>
```

### # Welche der Suiten unterstützt 3DES?

Get-TlsCipherSuite -Name 3DES |

Format-Table Name, Exchange, Cipher, Hash, Certificate

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Ciphersuiten managen.ps1* X
4 # Welche der Suiten unterstützt 3DES?
5 Get-TlsCipherSuite -Name 3DES |
6 Format-Table Name, Exchange, Cipher, Hash, Certificate
7
PS C:\Windows\system32> Get-TlsCipherSuite -Name 3DES |
Format-Table Name, Exchange, Cipher, Hash, Certificate

Name Exchange Cipher Hash Certificate
-----
TLS_RSA_WITH_3DES_EDE_CBC_SHA RSA 3DES SHA1 RSA

PS C:\Windows\system32>
```



## Ciphersuiten managen

### # Deaktivieren die unsicheren 3DES-Ciphersuiten:

```
Foreach ($CSU in (Get-TlsCipherSuite -Name '3DES'))
```

```
{Disable-TlsCipherSuite -Name $CSU.Name}
```

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Ciphersuiten managen.ps1* X
8 # Deaktivieren die unsicheren 3DES-Ciphersuiten:
9 Foreach ($CSU in (Get-TlsCipherSuite -Name '3DES'))
10 {Disable-TlsCipherSuite -Name $CSU.Name}
11
12 # Gibt es noch weitere die 3DES unterstützen?:

PS C:\Windows\system32> Foreach ($CSU in (Get-TlsCipherSuite -Name '3DES'))
{Disable-TlsCipherSuite -Name $CSU.Name}

PS C:\Windows\system32> |

Abgeschlossen | Ln 112 Spalte 25 | 100%
```

### # Gibt es noch weitere die 3DES unterstützen?

```
Get-TlsCipherSuite 3DES |
```

```
Format-Table Name, Exchange, Cipher, Hash, Certificate
```

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Ciphersuiten managen.ps1* X
11
12 # Gibt es noch weitere die 3DES unterstützen?:
13 Get-TlsCipherSuite 3DES |
14 Format-Table Name, Exchange, Cipher, Hash, Certificate
15

PS C:\Windows\system32> Get-TlsCipherSuite 3DES |
Format-Table Name, Exchange, Cipher, Hash, Certificate

PS C:\Windows\system32>

Abgeschlossen | Ln 115 Spalte 25 | 100%
```

### # Aktivieren die zuvor deaktivierten Ciphersuiten wieder:

```
Enable-TlsCipherSuite -Name TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Ciphersuiten managen.ps1* X
16 # Aktivieren die zuvor deaktivierten Ciphersuiten wieder:
17 Enable-TlsCipherSuite -Name TLS_RSA_WITH_3DES_EDE_CBC_SHA
18
19 # Welche Ciphersuiten die 3DES unterstützen sind noch aktiv:
20 Get-TlsCipherSuite 3DES |

PS C:\Windows\system32> Enable-TlsCipherSuite -Name TLS_RSA_WITH_3DES_EDE_CBC_SHA

PS C:\Windows\system32> |

Abgeschlossen | Ln 117 Spalte 25 | 100%
```



## Ciphersuiten managen

# Welche Ciphersuiten die 3DES unterstützen sind noch aktiv:

Get-TlsCipherSuite 3DES | Format-Table -Property Name, Exchange, Cipher, ggeHash, Certificate

The screenshot shows the Windows PowerShell ISE interface. The command prompt is at C:\Windows\system32. The command entered is `Get-TlsCipherSuite 3DES | Format-Table -Property Name, Exchange, Cipher, ggeHash, Certificate`. The output is a table with the following data:

Name	Exchange	Cipher	ggeHash	Certificate
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES		RSA

The status bar at the bottom indicates 'Abgeschlossen' (Completed) and 'Ln 125 Spalte 25'.