



QNB eSolutions TLS Kılavuzu

İçindekiler

1. Bilgilendirme.....	2
2. Şifreleme Yöntemleri (Cipher)	4
3. Test Ortamları.....	5
4. İşletim Sistemleri Versiyonları	5
➤ Windows TLS Bilgisi (TR/ENG)	6
➤ Linux TLS Bilgisi (TR/ENG)	6
➤ MacOS TLS Bilgisi (TR/ENG)	7
5. Cipher Ayarlamaları	9
6. İstemcilerde TLS 1.2 Aktifleştirilmesi	9

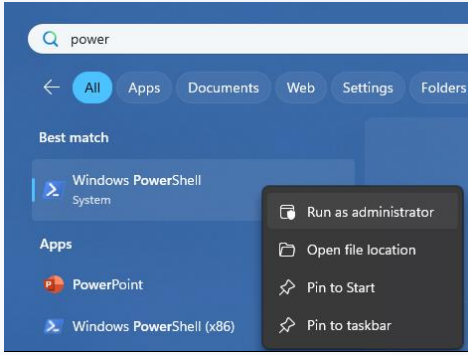
1. Bilgilendirme

25 Haziran 2025 tarihinden itibaren, eski bağlantı protokolleri (TLS 1.0 ve TLS 1.1) sistemlerimizde desteklenmeyecektir.

e-Belge işlemlerinizin kesintisiz devam etmesi için lütfen aşağıdaki adımları kontrol ediniz:

Ne Yapmanız Gerekıyor?

- **IT ekibinizden veya ERP teknik destek firmanızdan** destek alarak, sistemlerinizin **TLS 1.2 veya daha güncel bir sürümle** uyumlu çalıştığından emin olunuz.
- TLS desteğini kendiniz kontrol etmek isterseniz, [TLS 1.2 destekleyen işletim sistemleri listesine](#) ve [Windows'ta TLS 1.2 nasıl etkinleştirilir kılavuzuna](#) göz atabilirsiniz.
- **TLS 1.2 versiyonun aktifleştirilmesi için, Windows'unuzda kurulu olan "PowerShell" uygulamasını yönetici olarak çalıştırıp , aşağıdaki komutları sırası ile çalıştırabilirsiniz.**
- PowerShell uygulamasına sağ tıklayarak "Yönetici Olarak Çalıştır (Run as administrator)" tuşuna basılır.



- Aşağıdaki kodlar PowerShell ekranına yapıştırılır ve enter tuşuna basılır.

```
md "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2"  
md "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server"  
md "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client"  
# Enable TLS 1.2 for client and server SCHANNEL communications  
new-itemproperty -path  
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server" -name "Enabled" -value 1 -PropertyType "DWord"  
new-itemproperty -path  
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server" -name "DisabledByDefault" -value 0 -PropertyType "DWord"
```

```
new-itemproperty -path  
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS  
1.2\Client" -name "Enabled" -value 1 -PropertyType "DWord"  
new-itemproperty -path  
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS  
1.2\Client" -name "DisabledByDefault" -value 0 -PropertyType "DWord"
```

TLS 1.0 ve TLS 1.1'in pasifleştirilmesi için, PowerShell üzerinden aşağıdaki komutları çalıştırabilirsiniz.

TLS 1.0

```
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS  
1.0\Server' -Force | Out-Null  
New-ItemProperty -path  
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -  
name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null  
New-ItemProperty -path  
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -  
name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null  
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS  
1.0\Client' -Force | Out-Null  
New-ItemProperty -path  
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client' -  
name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null  
New-ItemProperty -path  
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client' -  
name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null
```

TLS 1.1

```
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS  
1.1\Server' -Force | Out-Null  
New-ItemProperty -path  
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -  
name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null  
New-ItemProperty -path  
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -  
name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null  
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS  
1.1\Client' -Force | Out-Null
```

Doküman No : KLVZ.48

Yayın Tarihi/Rev. : 07.05.2025/0

New-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client' - name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client' - name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null

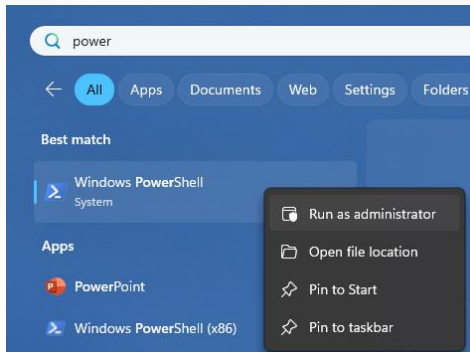
Destek ve İletişim:

Her türlü soru, destek ihtiyacı veya sistem altyapınızla ilgili daha detaylı teknik bilgiler için proje@destek.qnbolutions.com.tr adresinden bizimle iletişime geçebilirsiniz.

2. Şifreleme Yöntemleri (Cipher)

Artık sadece aşağıdaki yöntemler desteklenecektir.

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- Güvenli cipher'ların aktifleştirilmesi için, PowerShell uygulamasında aşağıdaki komutların çalıştırılması yeterli olacaktır.
- PowerShell uygulamasına sağ tıklayarak "Yönetici Olarak Çalıştır (Run as administrator)" tuşuna basılır.



- Aşağıdaki kodlar PowerShell ekranına yapıştırılır ve enter tuşuna basılır.

Set-ItemProperty `

-Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319' `

-Name 'SchUseStrongCrypto' -Value '1' -Type DWord

Set-ItemProperty `

-Path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' `

-Name 'SchUseStrongCrypto' -Value '1' -Type DWord

Doküman No : KLVZ.48

Yayın Tarihi/Rev. : 07.05.2025/0

TLS ve Cipher için paylaşılan komutlar çalıştırıldıktan sonra, işlem yaptığınız bilgisayar veya sunucunun yeniden başlatılması gerekmektedir.

3. Test Ortamları

Test ortamlarımız güncellenmiştir. Mevcut test hesaplarınızla bağlantılarınızı kontrol edebilirsiniz.

Portaltest:

1. <https://connectortest.qnbolutions.com.tr/connector/ws/userService?wsdl> (userService)
2. <https://connectortest.qnbolutions.com.tr/connector/ws/connectorService?wsdl> (connectorService)
3. <https://earsivtest.qnbolutions.com.tr/earsiv/ws/EarsivWebService?wsdl> (connectorService)
4. <https://edeftertest.qnbolutions.com.tr/edefter/ws/EDefterWS?wsdl> (connectorService)

Erpefaturatest:

1. <https://erpefaturatest1.qnbolutions.com.tr/efatura/ws/userService?wsdl> (userService)
2. <https://erpefaturatest1.qnbolutions.com.tr/efatura/ws/connectorService?wsdl> (connectorService)

4. İşletim Sistemleri Versiyonları

Aşağıdaki ekran görüntülerinde, işletim sistemleri ve sürümlerinin desteklediği TLS versiyonları belirtilmiştir.

➤ Windows TLS Bilgisi (TR/ENG)

Windows Os	TLS 1.0 İstemci	TLS 1.1 İstemci	TLS 1.2 İstemci	TLS 1.3 İstemci
Windows Vista / Windows Server 2008	Etkin	Desteklenmiyor	Desteklenmiyor	Desteklenmiyor
Windows Server 2008 With Service Pack 2 (SP2)	Etkin	Etkin Değil	Etkin Değil	Desteklenmiyor
Windows 7 / Windows Server 2008 R2	Etkin	Etkin Değil	Etkin Değil	Desteklenmiyor
Windows 8 / Windows Server 2012	Etkin	Etkin	Etkin	Desteklenmiyor
Windows 8.1 / Windows Server 2012 R2	Etkin	Etkin	Etkin	Desteklenmiyor
Windows 10, Version 1507 / 1511	Etkin	Etkin	Etkin	Desteklenmiyor
Windows 10, Version 1607 / Windows Server 2016 Standart	Etkin	Etkin	Etkin	Desteklenmiyor
Windows 10, Version 1703 / 1709 / 1803	Etkin	Etkin	Etkin	Desteklenmiyor
Windows 10, Version 1809 / Windows Server 2019	Etkin	Etkin	Etkin	Desteklenmiyor
Windows 10, Version 1903/1909/2004/20H2/20H1/21H2	Etkin	Etkin	Etkin	Desteklenmiyor
Windows Server 2022	Etkin	Etkin	Etkin	Etkin
Windows 11	Etkin	Etkin	Etkin	Etkin

Windows Os	TLS 1.0 Client	TLS 1.1 Client	TLS 1.2 Client	TLS 1.3 Client
Windows Vista / Windows Server 2008	Enabled	Not Supported	Not Supported	Not Supported
Windows Server 2008 With Service Pack 2 (SP2)	Enabled	Disabled	Disabled	Not Supported
Windows 7 / Windows Server 2008 R2	Enabled	Disabled	Disabled	Not Supported
Windows 8 / Windows Server 2012	Enabled	Enabled	Enabled	Not Supported
Windows 8.1 / Windows Server 2012 R2	Enabled	Enabled	Enabled	Not Supported
Windows 10, Version 1507 / 1511	Enabled	Enabled	Enabled	Not Supported
Windows 10, Version 1607 / Windows Server 2016 Standart	Enabled	Enabled	Enabled	Not Supported
Windows 10, Version 1703 / 1709 / 1803	Enabled	Enabled	Enabled	Not Supported
Windows 10, Version 1809 / Windows Server 2019	Enabled	Enabled	Enabled	Not Supported
Windows 10, Version 1903/1909/2004/20H2/20H1/21H2	Enabled	Enabled	Enabled	Not Supported
Windows Server 2022	Enabled	Enabled	Enabled	Enabled
Windows 11	Enabled	Enabled	Enabled	Enabled

➤ Linux TLS Bilgisi (TR/ENG)

Linux Version	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
Debian 7 Wheezy	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
Debian 8 Wheezy	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
Debian 9 Stretch	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
Debian 10 Buster	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
Ubuntu 12.04 LTS Precise Pangolin	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
Ubuntu 14.04 LTS Trusty Tahr	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
Ubuntu 16.04 LTS Xenial Xerus	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
Ubuntu 18.04 LTS Bionic Beaver	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
Ubuntu 20.04 LTS Focal Fossa	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
CentOs 6	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
CentOs 7	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
CentOs 8	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
Red Hat Enterpris Linux (RHEL) 6	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
Red Hat Enterpris Linux (RHEL) 7	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
Red Hat Enterpris Linux (RHEL) 8	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor

Linux Version	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
Debian 7 Wheezy	Supported	Supported	Supported	Not Supported
Debian 8 Wheezy	Supported	Supported	Supported	Not Supported
Debian 9 Stretch	Supported	Supported	Supported	Not Supported
Debian 10 Buster	Supported	Supported	Supported	Supported
Ubuntu 12.04 LTS Precise Pangolin	Supported	Supported	Supported	Not Supported
Ubuntu 14.04 LTS Trusty Tahr	Supported	Supported	Supported	Not Supported
Ubuntu 16.04 LTS Xenial Xerus	Supported	Supported	Supported	Not Supported
Ubuntu 18.04 LTS Bionic Beaver	Supported	Supported	Supported	Supported
Ubuntu 20.04 LTS Focal Fossa	Supported	Supported	Supported	Supported
CentOs 6	Supported	Supported	Supported	Not Supported
CentOs 7	Supported	Supported	Supported	Supported
CentOs 8	Supported	Supported	Supported	Supported
Red Hat Enterpris Linux (RHEL) 6	Supported	Supported	Supported	Not Supported
Red Hat Enterpris Linux (RHEL) 7	Supported	Supported	Supported	Supported
Red Hat Enterpris Linux (RHEL) 8	Supported	Supported	Supported	Supported

➤ MacOS TLS Bilgisi (TR/ENG)

Doküman No : KLVZ.48

Yayın Tarihi/Rev. : 07.05.2025/0

MacOs Version	MacOs Adı	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
OS X 10.0	Cheetah	Destekleniyor	Desteklenmiyor	Desteklenmiyor	Desteklenmiyor
OS X 10.1	Puma	Destekleniyor	Desteklenmiyor	Desteklenmiyor	Desteklenmiyor
OS X 10.2	Jaguar	Destekleniyor	Desteklenmiyor	Desteklenmiyor	Desteklenmiyor
OS X 10.3	Panther	Destekleniyor	Desteklenmiyor	Desteklenmiyor	Desteklenmiyor
OS X 10.4	Tiger	Destekleniyor	Destekleniyor	Desteklenmiyor	Desteklenmiyor
OS X 10.5	Leopard	Destekleniyor	Desteklenmiyor	Desteklenmiyor	Desteklenmiyor
OS X 10.6	Snow Leopard	Destekleniyor	Desteklenmiyor	Desteklenmiyor	Desteklenmiyor
OS X 10.7	Lion	Destekleniyor	Desteklenmiyor	Desteklenmiyor	Desteklenmiyor
OS X 10.8	Mountain Lion	Destekleniyor	Desteklenmiyor	Desteklenmiyor	Desteklenmiyor
OS X 10.9	Mavericks	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
OS X 10.10	Yosemite	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
OS X 10.11	El Capitan	Destekleniyor	Destekleniyor	Destekleniyor	Desteklenmiyor
MacOs 10.12	Sierra	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
MacOs 10.13	High Sierra	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
MacOs 10.14	Mojave	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
MacOs 10.15	Catalina	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
MacOs 11.0	Big Sur	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
MacOs 12.0	Monterey	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor
MacOs 13.0	Ventura	Destekleniyor	Destekleniyor	Destekleniyor	Destekleniyor

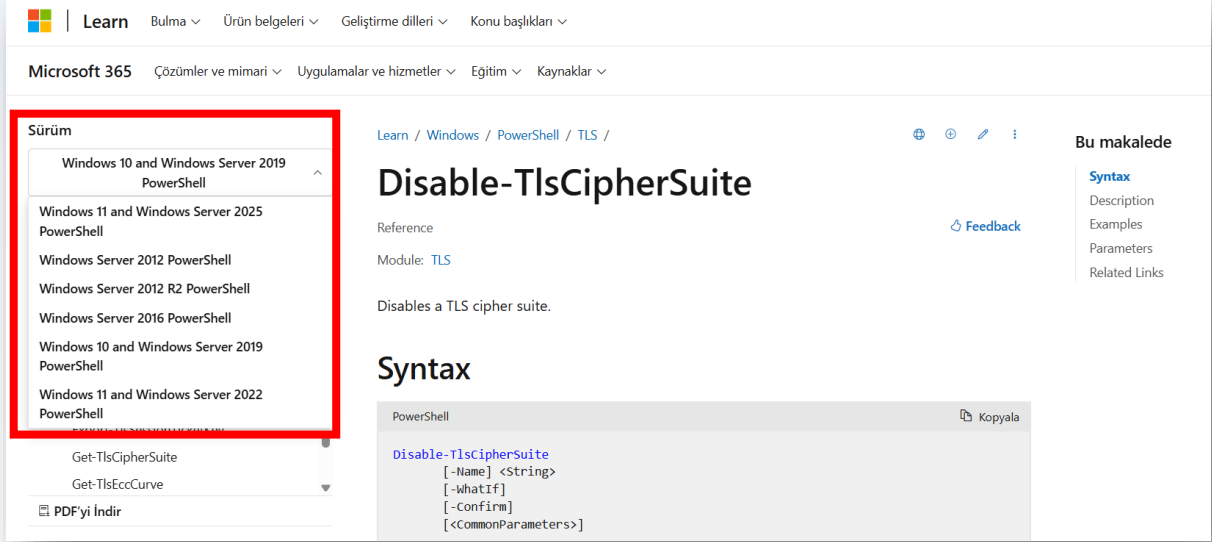
MacOs Version	MacOs Name	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
OS X 10.0	Cheetah	Supported	Not Supported	Not Supported	Not Supported
OS X 10.1	Puma	Supported	Not Supported	Not Supported	Not Supported
OS X 10.2	Jaguar	Supported	Not Supported	Not Supported	Not Supported
OS X 10.3	Panther	Supported	Not Supported	Not Supported	Not Supported
OS X 10.4	Tiger	Supported	Supported	Not Supported	Not Supported
OS X 10.5	Leopard	Supported	Not Supported	Not Supported	Not Supported
OS X 10.6	Snow Leopard	Supported	Not Supported	Not Supported	Not Supported
OS X 10.7	Lion	Supported	Not Supported	Not Supported	Not Supported
OS X 10.8	Mountain Lion	Supported	Not Supported	Not Supported	Not Supported
OS X 10.9	Mavericks	Supported	Supported	Supported	Not Supported
OS X 10.10	Yosemite	Supported	Supported	Supported	Not Supported
OS X 10.11	El Capitan	Supported	Supported	Supported	Not Supported
MacOs 10.12	Sierra	Supported	Supported	Supported	Supported
MacOs 10.13	High Sierra	Supported	Supported	Supported	Supported
MacOs 10.14	Mojave	Supported	Supported	Supported	Supported
MacOs 10.15	Catalina	Supported	Supported	Supported	Supported
MacOs 11.0	Big Sur	Supported	Supported	Supported	Supported
MacOs 12.0	Monterey	Supported	Supported	Supported	Supported
MacOs 13.0	Ventura	Supported	Supported	Supported	Supported

5. Cipher Ayarlamaları

Cipher yapılandırmalarıyla ilgili detaylı destek sağlamak amacıyla, lütfen aşağıdaki bağlantıyı inceleyerek gerekli bilgi ve yardım materyallerine ulaşabilirsiniz.

<https://learn.microsoft.com/tr-tr/powershell/module/tls/disable-tlsciphersuite?view=windowsserver2019-ps>

- İşletim sistemi sürümünüzü, aşağıda yer alan alandan tercihinize göre seçebilirsiniz.



The screenshot shows the Microsoft Learn article titled "Disable-TlsCipherSuite". On the left, a dropdown menu for "Sürüm" (Version) is open, listing various Windows and Windows Server versions with their corresponding PowerShell modules. The versions listed are: Windows 10 and Windows Server 2019 PowerShell, Windows 11 and Windows Server 2025 PowerShell, Windows Server 2012 PowerShell, Windows Server 2012 R2 PowerShell, Windows Server 2016 PowerShell, Windows 10 and Windows Server 2019 PowerShell, and Windows 11 and Windows Server 2022 PowerShell. The article content on the right includes the title "Disable-TlsCipherSuite", a reference to the TLS module, a description "Disables a TLS cipher suite.", and a syntax section for the PowerShell command "Disable-TlsCipherSuite" with parameters: [-Name] <String>, [-WhatIf], [-Confirm], and [<CommonParameters>].

6. İstemcilerde TLS 1.2 Aktifleştirilmesi

TLS 1.2 aktifleştirilmesi konusunda kapsamlı bilgiyi edinmek amacıyla, aşağıdaki bağlantıyı inceleyebilirsiniz.

<https://learn.microsoft.com/tr-tr/intune/configmgr/core/plan-design/security/enable-tls-1-2-client>

QNB eSolutions Elektronik Ticaret ve Biliřim Hizmetleri A.ř.

Esentepe Mah. Büyükdere Cad. Kristal Kule Binası

No: 215 řiřli / İstanbul

Tel: 0212 370 42 00 | Faks: 0212 212 00 35

Müşteri Hizmetleri Merkezi: 0850 250 67 50

qnbolutions