

SSL ve TLS Nedir? Sistemde Kontrolü Nasıl Sağlanır?

SSL Nedir?

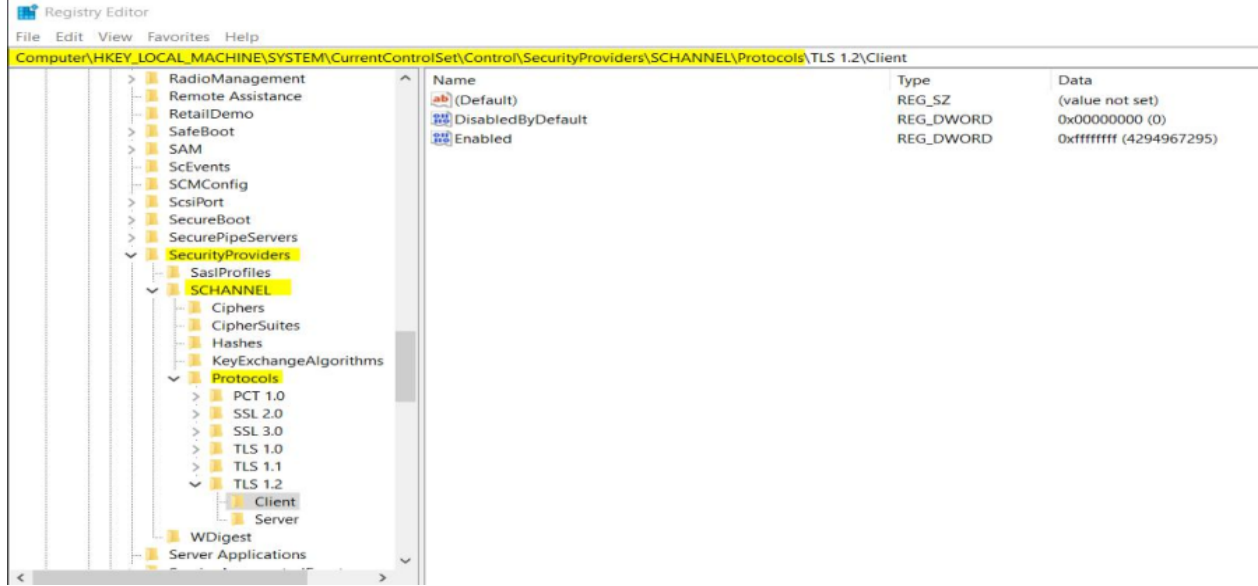
SSL, Güvenli Soket Katmanı (Secure Sockets Layer) anlamına gelmekle birlikte bir uygulama/websitesi ile sunucu arasında şifrelenmiş iletişime olanak sağlayan bir tür dijital güvenlik teknolojisidir. Kullanılan SSL tipine göre değişiklik göstermekle birlikte 40 bit veya 128 bit arasındaki bir değerde şifreleme ile veri güvenliği sağlanır. SSL üzerinden **Public Key** ve **Private Key** olarak ifade edilen anahtarlar aracılığıyla istemci ile sunucu arasındaki şifreleme ve doğrulama işlemi gerçekleşir.

TLS Nedir?

TLS, Taşıma Katmanı Güvenliği (Transport Layer Security) anlamına gelmektedir. Netscape tarafından SSL'in 1994, 1995, 1996 spesifikasyonları üzerinden geliştirilen SSL'in üst sürümü olarak nitelendirile-bilecek şekilde tanımlanabilir. TLS yapısı **TLS Record Protocol (TLS Kayıt Protokolü)** ve **TLS Handshake Protocol (TLS El Sıkışma Protokol)** şeklinde iki katmandan oluşur. Güvenliğin ön planda tutulduğu TLS yapısının kullanımına daha çok anlık mesajlaşma uygulamaları, dosya transfer uygulamaları, VPN erişim uygulamaları gibi örnek gösterilebilir.

SSL ve TLS Tanımları Nasıl Kontrol Edilir?

Firewall veya benzer güvenlik yazılımlarının kontrolü olmayan sistemlerde kayıt düzenleme defterinde Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols dizini altında her bir protokol için ayrı bir tanımlama yaparak protokolün enable/disable durumu belirtilmelidir.



Bu konuda kullanılabilecek 3rd parti uygulamalarda mevcuttur. Bu uygulamalar üzerinden gerekli tanımları kolaylıkla gerçekleştirilir.



Cryptolite



Schannel



Cipher Suites



Advanced



Templates



Site Information



Audit

Schannel

These settings enable or disable server options which offer the flexibility to group or separate settings that have specific and the default for the operating system will be used if the appropriate buttons are changed.

Server Protocols

- ☒ Multi-Protocol Unified Hello
- ☒ PCT 1.0
- ☒ SSL 2.0
- ☒ SSL 3.0
- ☒ TLS 1.0
- ☒ TLS 1.1
- ☒ TLS 1.2

Ciphers

- ☒ NULL
- ☒ DES 56/56
- ☒ RC2 40/128
- ☒ RC2 56/128
- ☒ RC2 128/128
- ☒ RC4 40/128
- ☒ RC4 56/128
- ☒ RC4 64/128
- ☒ RC4 128/128
- ☒ Triple DES 168
- ☒ AES 128/128
- ☒ AES 256/256

Hashes

- ☒ MD5
- ☒ SHA
- ☒ SHA 256
- ☒ SHA 384
- ☒ SHA 512

Key Exchanges

- ☒ Diffie-Hellman
- ☒ PKCS
- ☒ ECDH

Client Protocols

- ☒ Multi-Protocol Unified Hello
- ☒ PCT 1.0
- ☒ SSL 2.0
- ☒ SSL 3.0
- ☒ TLS 1.0
- ☒ TLS 1.1
- ☒ TLS 1.2