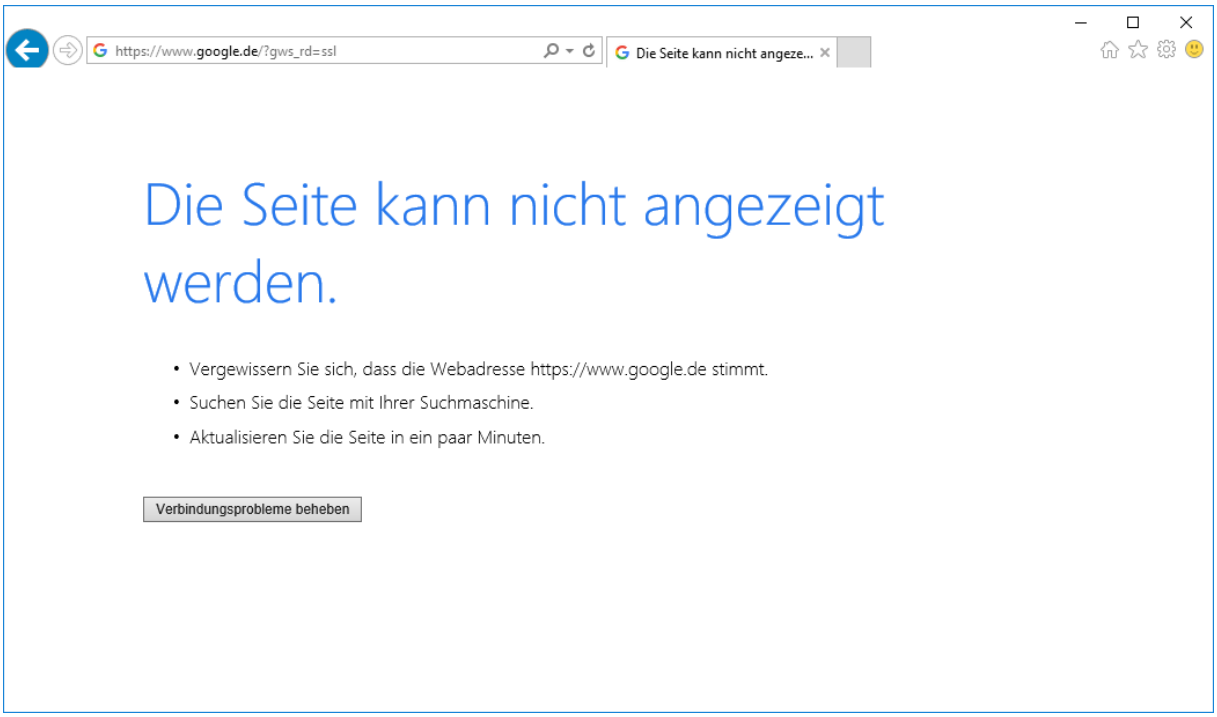
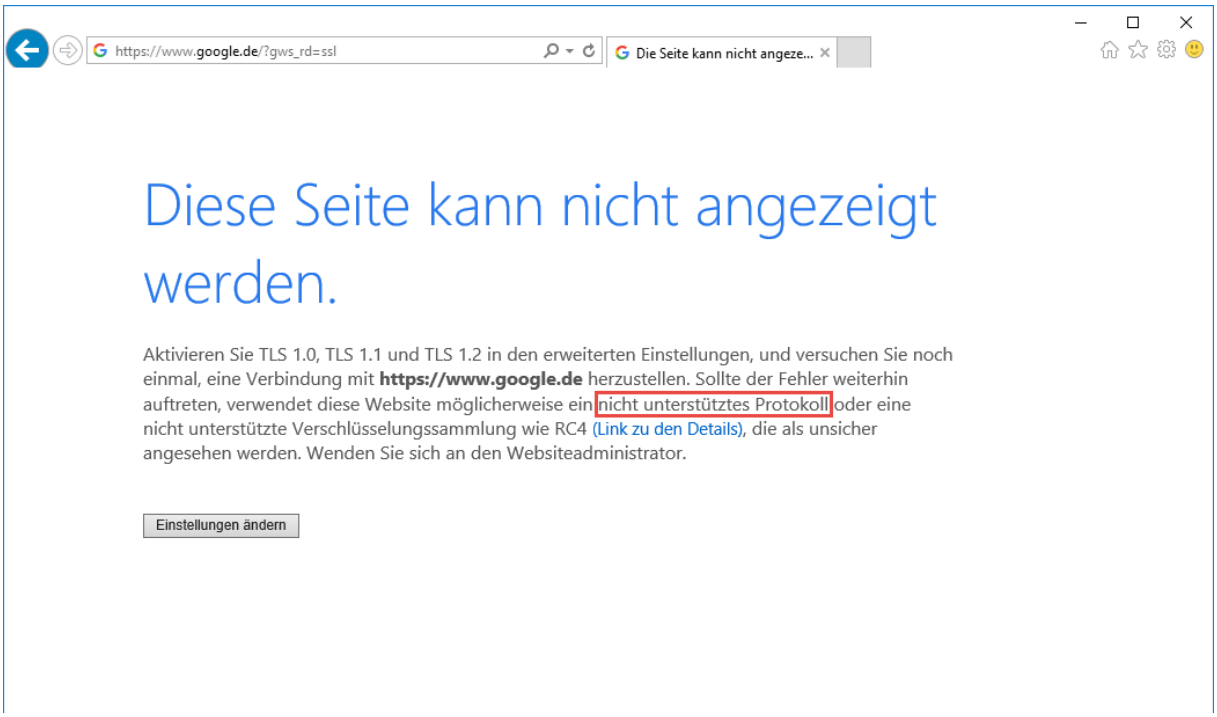
Fehlende Ciphersuiten unter TLS 1.2

Bei der Umstellung auf TLS 1.2 kann eine falsche Auswahl von Ciphersuiten zu Problemen führen. In diesem Beispiel bekomme ich beim Aufruf von https://www.google.de folgenden Hinweis angezeigt.

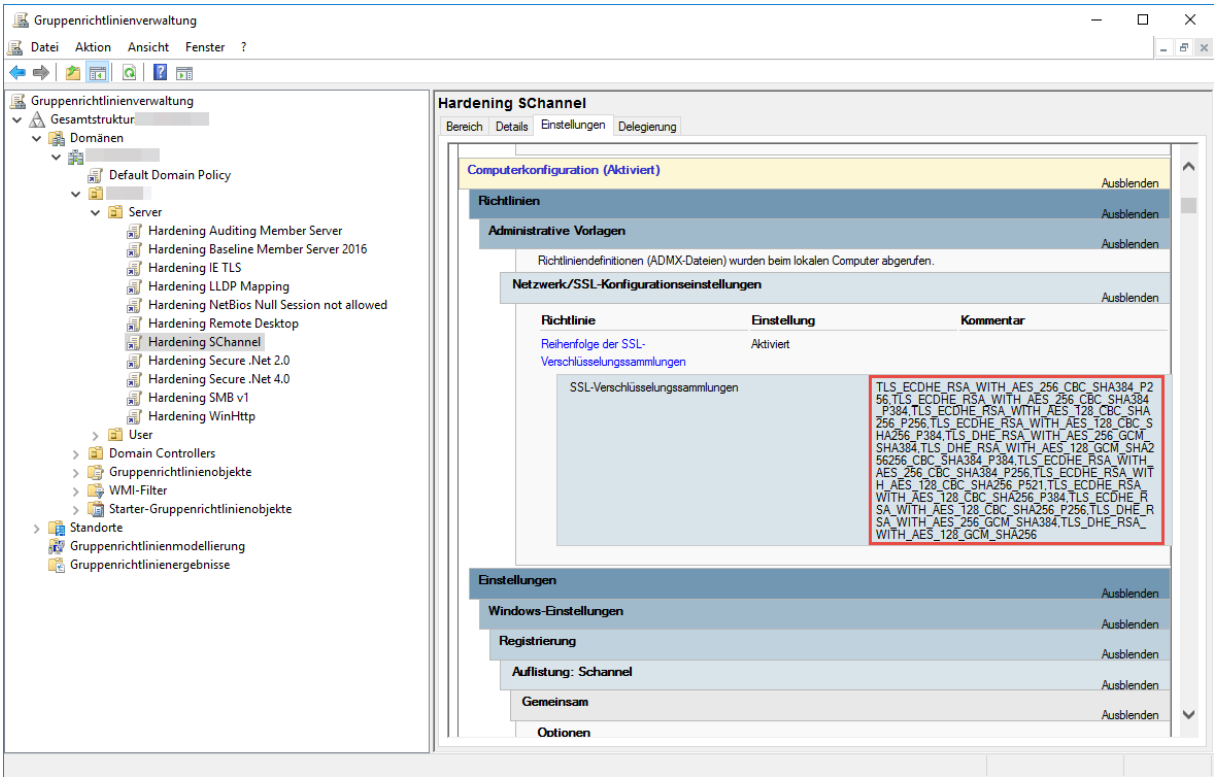


Ein Hinweis, wäre die fehlende Unterstützung eines Protokolls.

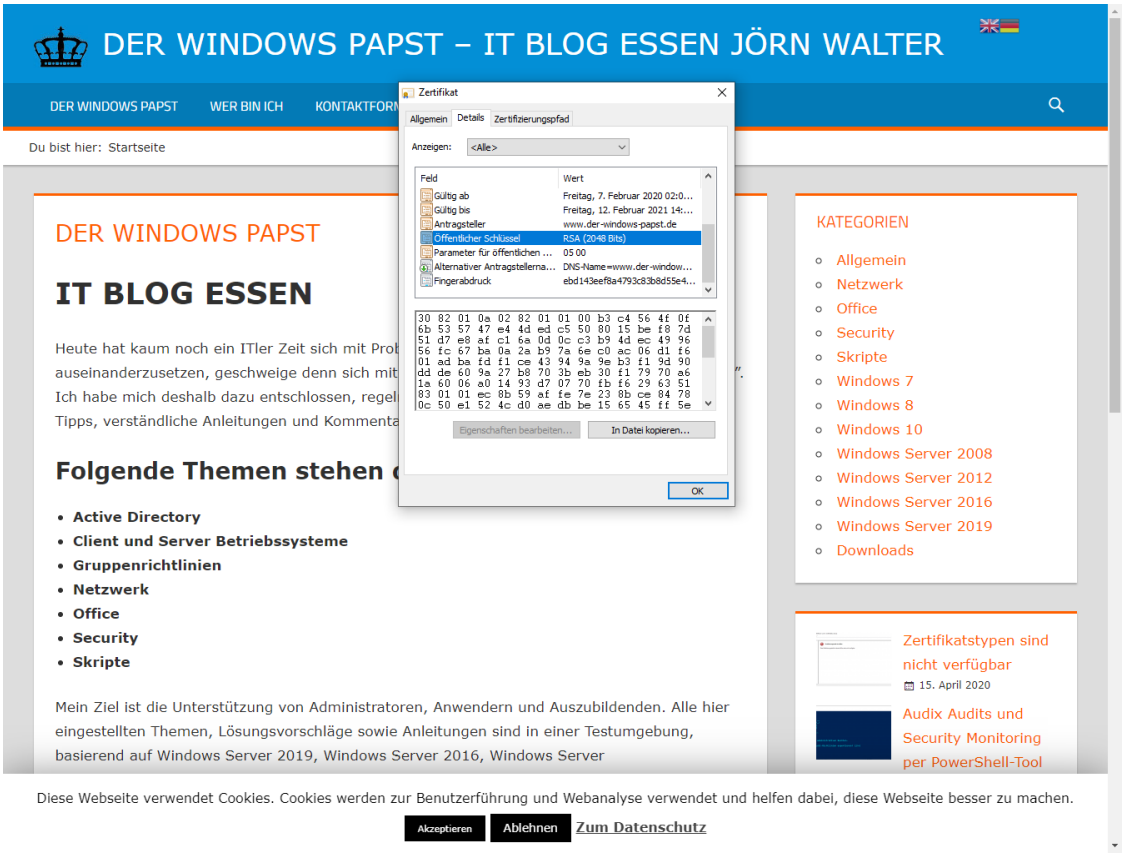


Fehlende Ciphersuiten unter TLS 1.2

In dieser Sammlung werden ausschließlich Suiten mit einem RSA Authentifizierungsalgorithmus eingesetzt.



Aus diesem Grund lässt sich die Webseite https://www.der-windows-papst.de auch aufrufen.

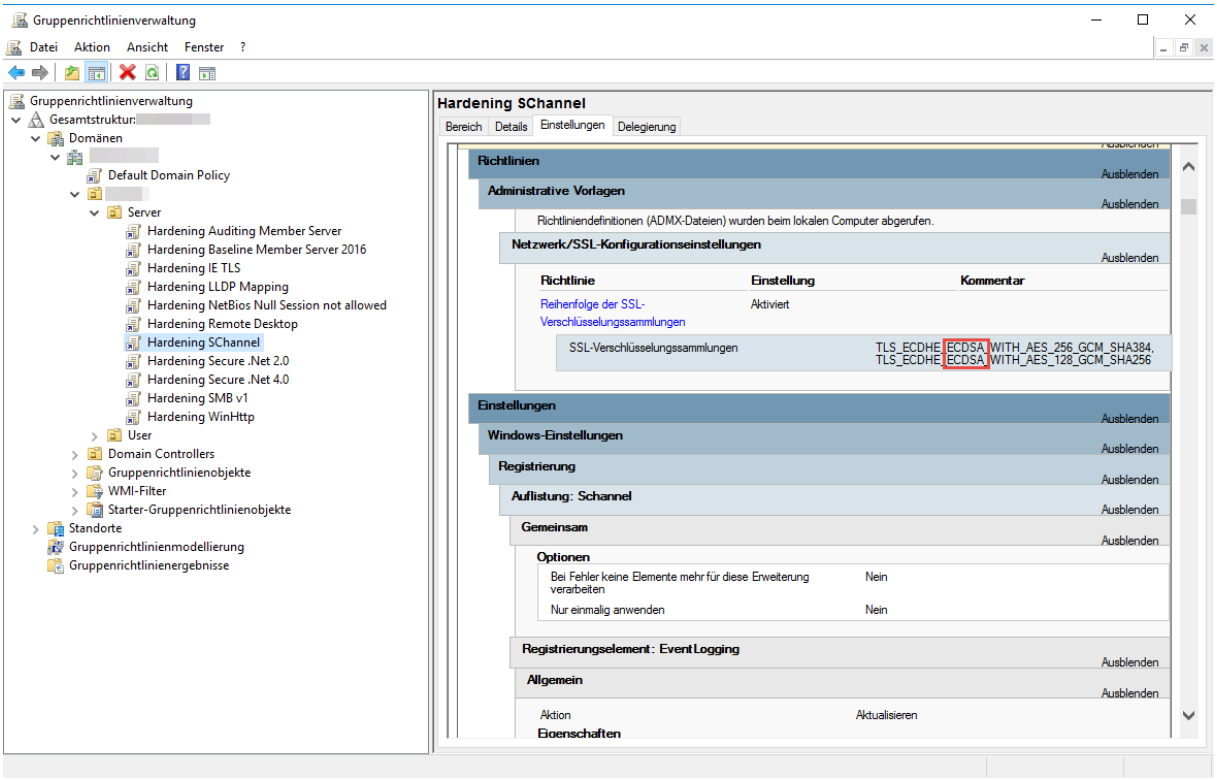


Erstellt von Jörn Walter **16.04.2020**

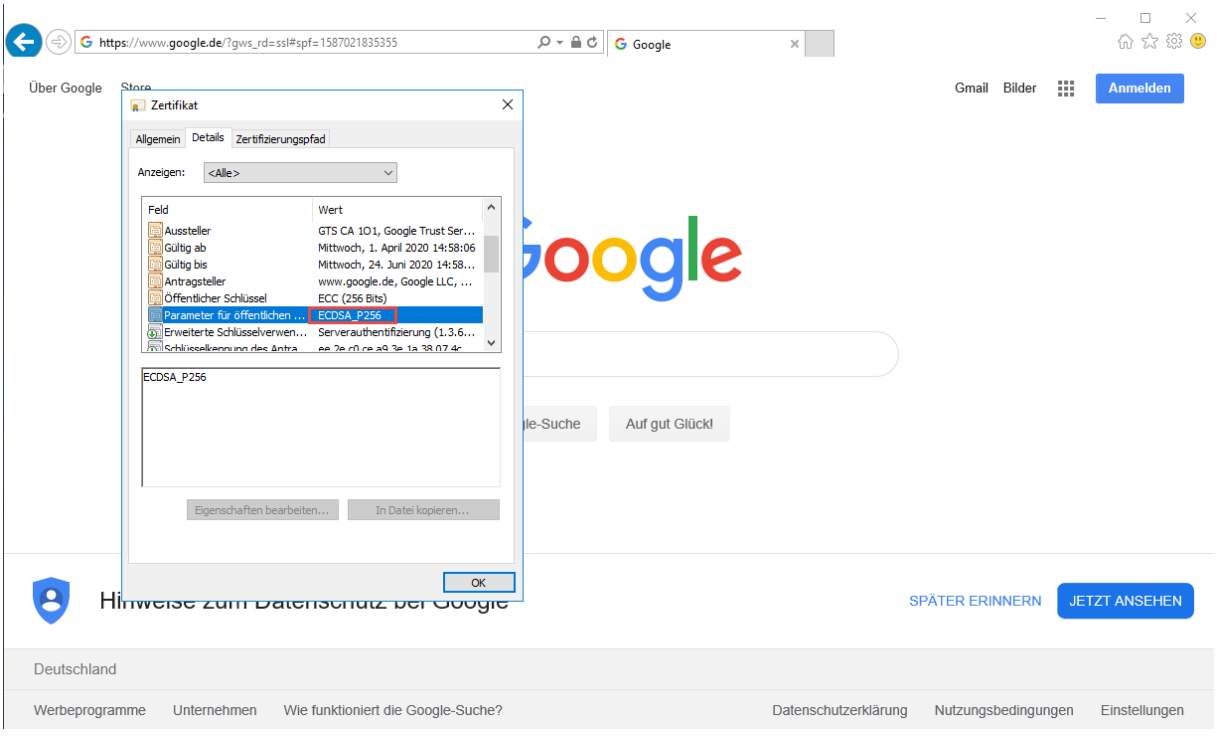
Fehlende Ciphersuiten unter TLS 1.2

Google hingegen nutzt aber ein Zertifikat mit einem Authentifizierungsalgorithmus der Güte ECDSA. Keine der oben eingesetzen Cipher-Suiten unterstützt ECDSA. Daher kommt es zu keiner Verbindung, um die Webseite https://www.google.de aufrufen zu könenn.

Nutze ich speziell für dieses Beispiel diese beiden ECDSA Cipher-Suiten…



…ist der Aufruf von https://www.google.de wieder möglich. Es kommt wieder eine Verbindung zustande.



Fehlende Ciphersuiten unter TLS 1.2

Optional:

Diese beiden Suiten benötigen ein Zertifikat mit einem RSA Authentifizierungsalgorithmus unterstützen aber zusätzlich PFS (Perfect Forwarding Secrecy).

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Diese beiden Suiten benötigen ein Zertifikat mit einem ECDSA Authentifizierungsalgorithmus unterstützen aber zusätzlich PFS (Perfect Forwarding Secrecy).

Der Einsatz von ECDHE ist was die Performance angeht besser als DHE. Der Einsatz von DHE bedeutet einen Leistungsabfall vom 2-8-fachen in Kauf nehmen zu müssen.

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Aus Kompatibilitätssicht nutzt man besser die Hybrideform:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Weitere Informationen:

https://www.der-windows-papst.de/2018/08/14/was-ist-eine-cipher-suite/

Fehlende Ciphersuiten unter TLS 1.2

Cipher Suiten die in Reihenfolge eingesetzt werden können:

PFS mit ECDHE

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

Erstellt von Jörn Walter **16.04.2020**