Click to verify

Iwantto ADD/ADJ Tls13 Suppose is installed on a Windows Server 2019 &/or a Hotfix? To connect with Alt+OG, At the end of OSD, on 20 of them, I have only 10 cipher suites available for sec. TLS ECDHE_RSA_WITH_AES_192_CBC_SHA256 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS ECDHE_RSA_WITH_AES_128_CBC_SHA TLS ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_NULL_SHA256 TLS_RSA_WITH_NULL_SHA TLS_PSK_WITH_AES_256_CBC_SHA384 TLS_PSK_WITH_AES_128_CBC_SHA256 TLS_PSK_WITH_AES_256_CBC_SHA TLS_PSK_WITH_AES_128_CBC_SHA TLS_PSK_WITH_3DES_EDE_CBC_SHA TLS_PSK_WITH_NULL_SHA384 TLS_PSK_WITH_NULL_SHA256 TLS_PSK_WITH_NULL_SHA TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384 TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256 TLS_ECDHE_PSK_WITH_NULL_SHA384 TLS_ECDHE_PSK_WITH_NULL_SHA256 Now, I have only 10 cipher suites available for sec. TLS. Without their help, I would have struggled to put this post together. Also, thanks to my colleagues Eric Baumgartner for his review. In light of Iranian vulnerabilities in specific TLS ciphersuites, we are recommending that customers who use Windows Server 2012 R2 and Windows 8.1 enable a subset of the available ciphersuites that will perform well in TLS 1.2 but still offer good security. Unfortunately, there is no ciphersuite that will perform well in TLS 1.2, but offer better security and interoperability than the ciphersuites we recommend in this blog. Instead, we have to make a choice between security and interoperability. Because of this, we are recommending that customers who use Windows Server 2012 R2 and Windows 8.1 enable a subset of the available ciphersuites