TLS Cipher Suites Release 55.02

Overview

This announcement provides information that may impact the ability of partner systems to connect with Commander systems using TLS, starting with release 55.02.

The Commander system uses Transport Level Security (TLS) protocol, version 1.2 or 1.3. For release 54 in February 2020, we distributed an announcement listing eight supported TLS cipher suites.

The security community has raised concerns over cipher suites that use Cipher-Block-Chaining (CBC).

Therefore, starting with release 55.02, the Commander will no longer support the four CBC cipher suites listed in the bulletin.

With release 55.02, Commander now supports two Elliptic Curve Cryptography (ECC) cipher suites for TLS v1.2 and two cipher suites specific to TLS v1.3, providing a greater range of connection capabilities.

In summary, with release 55.02, Commander supports four of the original TLS v1.2 cipher suites, two TLS v1.2 ECC cipher suites, and two TLS v1.3 cipher suites.

The following tables list all supported Algorithms and Ciphers. The minimum Diffie-Hellman key exchange size for all ciphers listed is 2048 bits.

Table 1 – Cipher Suite Names and Descriptions for TLS V1.2

Short Name (IANA)	Description
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	128-bit AES in Galois Counter Mode encryption with 128-bit AEAD authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate.
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	256-bit AES in Galois Counter Mode encryption with 128-bit AEAD authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate.
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	128-bit AES in Galois Counter Mode encryption with 128-bit AEAD authentication and ephemeral ECDH key exchange signed with an ECDSA certificate.
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	256-bit AES in Galois Counter Mode encryption with 128-bit AEAD message authentication and ephemeral ECDH key exchange signed with an ECDSA certificate.
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128-bit AES in Galois Counter Mode encryption with 128-bit AEAD message authentication and ephemeral ECDH key exchange signed with an RSA certificate.
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	256-bit AES in Galois Counter Mode encryption with 128-bit AEAD message authentication and ephemeral ECDH key exchange signed with an RSA certificate.

Table 2 – Cipher Suite Names and Descriptions for TLS V1.3

Short Name (IANA)	Description

TLS_AES_128_GCM_SHA256	128-bit AES in Galois Counter Mode encryption with 128-bit AEAD authentication and HKDF (HMAC-based Extract-and-Expand Key Derivation Function) with SHA256.
TLS_AES_256_GCM_SHA384	256-bit AES in Galois Counter Mode encryption with 128-bit AEAD authentication and HKDF (HMAC-based Extract-and-Expand Key Derivation Function) with SHA384