Appendix E: SSL Cipher Suites Supported by ApplinX

Appendix E: SSL Cipher Suites Supported by ApplinX

Following is a list of the SSL cipher suites supported when connecting to the host. These are relevant when running Oracle's JVM. It is possible to use any JSSE provider, including IBM.

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA

TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA

TLS_ECDH_RSA_WITH_AES_128_CBC_SHA

TLS_ECDH_RSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_AES_256_CBC_SHA

SSL_RSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

SSL_RSA_WITH_DES_CBC_SHA

SSL_DHE_RSA_WITH_DES_CBC_SHA

Appendix E: SSL Cipher Suites Supported by ApplinX

SSL_DHE_DSS_WITH_DES_CBC_SHA

SSL_RSA_EXPORT_WITH_DES40_CBC_SHA

SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

SSL_RSA_WITH_NULL_MD5

SSL_RSA_WITH_NULL_SHA

TLS_ECDH_ECDSA_WITH_NULL_SHA

TLS_ECDH_RSA_WITH_NULL_SHA

TLS_ECDHE_ECDSA_WITH_NULL_SHA

TLS_ECDHE_RSA_WITH_NULL_SHA

TLS_DH_anon_WITH_AES_128_CBC_SHA

TLS_DH_anon_WITH_AES_256_CBC_SHA

SSL_DH_anon_WITH_3DES_EDE_CBC_SHA

SSL_DH_anon_WITH_DES_CBC_SHA

TLS_ECDH_anon_WITH_AES_128_CBC_SHA

TLS_ECDH_anon_WITH_AES_256_CBC_SHA

TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA

SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

TLS_ECDH_anon_WITH_NULL_SHA

TLS_KRB5_WITH_3DES_EDE_CBC_SHA

TLS_KRB5_WITH_3DES_EDE_CBC_MD5

TLS_KRB5_WITH_DES_CBC_SHA

TLS_KRB5_WITH_DES_CBC_MD5

TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA

TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5