Cipher support on an External HSM (Thales/Safenet)

The following table lists the support for different ciphers on SSL entities, such as virtual server, frontend, backend, and internal services.

How to read the table

Unless a build number is specified, a cipher suite is supported for all builds in a release.

Example

- **10.5, 11.0, 11.1, 12.0, 12.1, 13.0, 13.1**: All builds of 10.5, 11.0, 11.1, 12.0, 12.1, 13.0, 13.1 releases.
- **11.1, 12.0, 12.1, 13.0, 13.1**: All builds of 11.1, 12.0, 12.1, 13.0, 13.1 releases.
- **10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0, 13.1**: Build 53.x and later in release 10.5. All builds of 11.0, 11.1, 12.0, 12.1, 13.0, 13.1 releases.
- **NA**: not applicable.

Cipher Suite Name	Hex Code	Wireshark Cipher Suite Name	Builds Supported (frontend)	Builds Supported (backend)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AES_256_CBC_SHA	11.0-62.x and later, 11.1, 12.0, 12.1, 13.0, 13.1	NA
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	11.0-62.x and later, 11.1, 12.0, 12.1, 13.0, 13.1	NA
TLS1.2-AES-256-SHA256	0x003d	TLS_RSA_WITH_AES_256_CBC_SHA256	11.0-62.x and later, 11.1, 12.0, 12.1, 13.0, 13.1	NA
TLS1.2-AES-128-SHA256	0x003c	TLS_RSA_WITH_AES_128_CBC_SHA256	11.0-62.x and later, 11.1, 12.0, 12.1, 13.0, 13.1	NA
TLS1.2-AES256-GCM-SHA384	0x009d	TLS_RSA_WITH_AES_256_GCM_SHA384	11.1, 12.0, 12.1, 13.0, 13.1	NA
TLS1.2-AES128-GCM-SHA256	0x009c	TLS_RSA_WITH_AES_128_GCM_SHA256	11.1, 12.0, 12.1, 13.0, 13.1	NA
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	12.1, 13.0, 13.1	NA
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0, 13.1	NA
TLS1.2-ECDHE-RSA-AES-256-SHA384	0xc028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	12.1, 13.0, 13.1	NA
TLS1.2-ECDHE-RSA-AES-128-SHA256	0xc027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	12.1, 13.0, 13.1	NA
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	0xc030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	12.1, 13.0, 13.1	NA
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	0xc02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	12.1, 13.0, 13.1	NA
TLS1.2-DHE-RSA-AES-256-SHA256	0x006b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	12.1, 13.0, 13.1	NA
TLS1.2-DHE-RSA-AES-128-SHA256	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	12.1, 13.0, 13.1	NA
TLS1.2-DHE-RSA-AES256-GCM-SHA384	0x009f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	12.1, 13.0, 13.1	NA
TLS1.2-DHE-RSA-AES128-GCM-SHA256	0x009e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	12.1, 13.0, 13.1	NA
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	12.1, 13.0, 13.1	NA
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0, 13.1	NA
TLS1-DHE-DSS-AES-256-CBC-SHA	0x0038	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	12.1, 13.0, 13.1 (VPX only)	NA
TLS1-DHE-DSS-AES-128-CBC-SHA	0x0032	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	12.1, 13.0, 13.1 (VPX only)	NA
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	12.1, 13.0, 13.1	NA
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	12.1, 13.0, 13.1	NA
SSL3-EDH-DSS-DES-CBC3-SHA	0x0013	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	12.1, 13.0, 13.1 (VPX only)	NA
TLS1-ECDHE-RSA-RC4-SHA	0xc011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	12.1, 13.0, 13.1	NA
TLS1-DHE-DSS-RC4-SHA	0x0066	TLS_DHE_DSS_WITH_RC4_128_SHA	12.1, 13.0, 13.1 (VPX only)	NA
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11.0-62.x and later, 11.1, 12.0, 12.1, 13.0, 13.1	NA
SSL3-RC4-SHA	0x0005	TLS_RSA_WITH_RC4_128	11.0-62.x and later, 11.1, 12.0, 12.1, 13.0, 13.1	NA
SSL3-RC4-MD5	0x0004	TLS_RSA_WITH_RC4_128	11.0-62.x and later, 11.1, 12.0, 12.1, 13.0, 13.1	NA
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_DES_CBC_SHA	11.0-62.x and later, 11.1, 12.0, 12.1, 13.0, 13.1	NA
SSL3-EDH-DSS-DES-CBC-SHA	0x0012	TLS_DHE_DSS_WITH_DES_CBC_SHA	12.1, 13.0, 13.1 (VPX only)	NA

Cipher Suite Name	Hex Code	Wireshark Cipher Suite Name	Builds Supported (frontend)	Builds Supported (backend)
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	12.1, 13.0, 13.1	NA
SSL3-ADH-RC4-MD5	0x0018	TLS_DH_anon_WITH_RC4_128_MD5	12.1, 13.0, 13.1	NA
SSL3-ADH-DES-CBC3-SHA	0x001b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	12.1, 13.0, 13.1	NA
SSL3-ADH-DES-CBC-SHA	0x001a	TLS_DH_anon_WITH_DES_CBC_SHA	12.1, 13.0, 13.1	NA
TLS1-ADH-AES-128-CBC-SHA	0x0034	TLS_DH_anon_WITH_AES_128_CBC_SHA	12.1, 13.0, 13.1	NA
TLS1-ADH-AES-256-CBC-SHA	0x003a	TLS_DH_anon_WITH_AES_256_CBC_SHA	12.1, 13.0, 13.1	NA
TLS1.3-AES128-GCM-SHA256	0x1301	TLS_AES_128_GCM_SHA256	12.1-50.x, 13.0, 13.1	NA
TLS1.3-AES256-GCM-SHA384	0x1302	TLS_AES_256_GCM_SHA384	12.1-50.x, 13.0, 13.1	NA
TLS1.3-CHACHA20-POLY1305-SHA256	0x1303	TLS_CHACHA20_POLY1305_SHA256	12.1-50.x, 13.0, 13.1	NA