Cipher support on a Citrix MPX 9700 FIPS appliance with firmware 2.2

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	10.5, 11.0, 11.1, 12.0, 12.1, 13.0, 13.1	10.5, 11.0, 11.1, 12.0, 12.1, 13.0, 13.1
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0, 13.1	10.5, 11.0, 11.1, 12.0, 12.1, 13.0, 13.1
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	11.1, 12.0, 12.1, 13.0, 13.1	11.1, 12.0, 12.1, 13.0, 13.1
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	11.1, 12.0, 12.1, 13.0, 13.1	11.1, 12.0, 12.1, 13.0, 13.1
TLS1.2-ECDHE-RSA-AES-256-SHA384	0xc028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	11.1, 12.0, 12.1, 13.0, 13.1	11.1 53.x and later, 12.0, 12.1, 13.0, 13.1
TLS1.2-ECDHE-RSA-AES-128-SHA256	0xc027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	11.1, 12.0, 12.1, 13.0, 13.1	11.1, 12.0, 12.1, 13.0, 13.1
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	11.1, 12.0, 12.1, 13.0, 13.1	11.1, 12.0, 12.1, 13.0, 13.1
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0, 13.1	10.5, 11.0, 11.1, 12.0, 12.1, 13.0, 13.1
TLS1.2-AES256-GCM-SHA384	0x009d	TLS_RSA_WITH_AES_256_GCM_SHA384	11.1 51.x and later, 12.0, 12.1, 13.0, 13.1	11.1 51.x and later, 12.0, 12.1, 13.0, 13.1
TLS1.2-AES128-GCM-SHA256	0x009c	TLS_RSA_WITH_AES_128_GCM_SHA256	11.1 51.x and later, 12.0, 12.1, 13.0, 13.1	11.1 51.x and later, 12.0, 12.1, 13.0, 13.1
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	0xc030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	11.1 51.x and later, 12.0, 12.1, 13.0, 13.1	11.1 53.x and later, 12.0, 12.1, 13.0, 13.1
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	0xc02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	11.1 51.x and later, 12.0, 12.1, 13.0, 13.1	11.1 51.x and later, 12.0, 12.1, 13.0, 13.1
TLS1.2-AES-256-SHA256	0x003d	TLS_RSA_WITH_AES_256_CBC_SHA256	11.1 52.x and later, 12.0, 12.1, 13.0, 13.1	11.1 51.x and later, 12.0, 12.1, 13.0, 13.1
TLS1.2-AES-128-SHA256	0x003c	TLS_RSA_WITH_AES_128_CBC_SHA256	11.1 52.x and later, 12.0, 12.1, 13.0, 13.1	11.1 52.x and later, 12.0, 12.1, 13.0, 13.1