

Cipher support on a Citrix MPX/SDX (N3) appliance

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

On an SDX appliance, if an SSL chip is assigned to a VPX instance, the cipher support of an MPX appliance applies. Otherwise, the normal cipher support of a VPX instance applies. From release 10.5 build 56.22, NetScaler MPX appliances support full hardware optimization for all ciphers. In earlier releases, part of ECDHE/DHE cipher optimization was done in software.

Use the 'show hardware' command to identify whether your appliance has N3 chips.

```
> sh hardware
```

```
Platform: NSMPX-22000 16*CPU+24*IX+12*E1K+2*E1K+4*CVM N3 2200100
```

```
Manufactured on: 8/19/2013
```

```
CPU: 2900MHZ
```

```
Host Id: 1006665862
```

```
Serial no: ENUK6298FT
```

```
Encoded serial no: ENUK6298FT
```

```
Done
```

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

Ciphersuite Name	Hex Code	Wireshark Ciphersuite Name	Builds Supported (frontend)	Builds Supported (backend)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AES_256_CB C_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CB C_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0

Ciphersuite Name	Hex Code	Wireshark Ciphersuite Name	Builds Supported (frontend)	Builds Supported (backend)
TLS1.2-AES-256-SHA256	0x003d	TLS_RSA_WITH_AES_256_CBC_SHA256	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1.2-AES-128-SHA256	0x003c	TLS_RSA_WITH_AES_128_CBC_SHA256	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1.2-AES256-GCM-SHA384	0x009d	TLS_RSA_WITH_AES_256_GCM_SHA384	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1.2-AES128-GCM-SHA256	0x009c	TLS_RSA_WITH_AES_128_GCM_SHA256	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	10.5-58.x and later, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	10.5-58.x and later, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1.2-ECDHE-RSA-AES-256-SHA384	0xc028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1.2-ECDHE-RSA-AES-128-SHA256	0xc027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	0xc030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	0xc02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1-ECDHE-ECDSA-AES256-SHA	0xc00a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	11.1, 12.0, 12.1, 13.0	11.1-51.x and later, 12.0,12,1
TLS1-ECDHE-ECDSA-AES128-SHA	0xc009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	11.1, 12.0, 12.1, 13.0	11.1-51.x and later, 12.0, 12.1, 13.0

Ciphersuite Name	Hex Code	Wireshark Ciphersuite Name	Builds Supported (frontend)	Builds Supported (backend)
TLS1.2-ECDHE-ECDSA-AES256-SHA384	0xc024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	11.1, 12.0, 12.1, 13.0	11.1-51.x and later, 12.0, 12.1, 13.0
TLS1.2-ECDHE-ECDSA-AES128-SHA256	0xc023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	11.1, 12.0, 12.1, 13.0	11.1-51.x and later, 12.0, 12.1, 13.0
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	0xc02c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	11.1, 12.0, 12.1, 13.0	11.1-51.x and later, 12.0, 12.1, 13.0
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	0xc02b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	11.1, 12.0, 12.1, 13.0	11.1-51.x and later, 12.0, 12.1, 13.0
TLS1.2-DHE-RSA-AES-256-SHA256	0x006b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1.2-DHE-RSA-AES-128-SHA256	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1.2-DHE-RSA-AES256-GCM-SHA384	0x009f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1.2-DHE-RSA-AES128-GCM-SHA256	0x009e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	10.5-53.x and later, 11.0, 11.1, 12.0, 12.1, 13.0	10.5-58.x and later, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	0xc008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	11.1, 12.0, 12.1, 13.0	11.1-51.x and later, 12.0, 12.1, 13.0
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-ECDHE-RSA-RC4-SHA	0xc011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	10.5-53.x and later, 11.0,	10.5-58.x and later, 11.0,

Ciphersuite Name	Hex Code	Wireshark Ciphersuite Name	Builds Supported (frontend)	Builds Supported (backend)
			11.1, 12.0, 12.1, 13.0	11.1, 12.0, 12.1, 13.0
TLS1-ECDHE-ECDSA-RC4-SHA	0xc007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	11.1, 12.0, 12.1, 13.0	11.1-51.x and later, 12.0, 12.1, 13.0
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-RC4-SHA	0x0005	TLS_RSA_WITH_RC4_128	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-RC4-MD5	0x0004	TLS_RSA_WITH_RC4_128	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_DES_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-EXP1024-RC4-SHA	0x0064	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-EXP-RC4-MD5	0x0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-EXP-DES-CBC-SHA	0x0008	TLS_RSA_EXPORT_WITH_DES_40_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-EXP-RC2-CBC-MD5	0x0006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-EXP-EDH-RSA-DES-CBC-SHA	0x0014	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-EXP1024-RC4-MD5	0x0060	TLS_RSA_EXPORT1024_WITH_RC4_56_MD5	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-EXP1024-RC2-CBC-MD5	0x0061	TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-ADH-RC4-MD5	0x0018	TLS_DH_anon_WITH_RC4_128_MD5	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0

Ciphersuite Name	Hex Code	Wireshark Ciphersuite Name	Builds Supported (frontend)	Builds Supported (backend)
SSL3-ADH-DES-CBC3-SHA	0x001b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-ADH-DES-CBC-SHA	0x001a	TLS_DH_anon_WITH_DES_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-ADH-AES-128-CBC-SHA	0x0034	TLS_DH_anon_WITH_AES_128_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1-ADH-AES-256-CBC-SHA	0x003a	TLS_DH_anon_WITH_AES_256_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-EXP-ADH-RC4-MD5	0x0017	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-EXP-ADH-DES-CBC-SHA	0x0019	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-NULL-MD5	0x0001	TLS_RSA_WITH_NULL_MD5	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
SSL3-NULL-SHA	0x0002	TLS_RSA_WITH_NULL_SHA	10.5, 11.0, 11.1, 12.0, 12.1, 13.0	10.5, 11.0, 11.1, 12.0, 12.1, 13.0
TLS1.2-DHE-RSA-CHACHA20-POLY1305	0xccea	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	13.0	13.0
TLS1.2-ECDHE-RSA-CHACHA20-POLY1305	0xccea8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	13.0	13.0
TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305	0xccea9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	13.0	13.0
TLS1.3-AES128_GCM-SHA256	0x1301	TLS_AES_128_GCM_SHA256	12.1-50.x, 13.0	NA
TLS1.3-AES256-GCM-SHA384	0x1302	TLS_AES_256_GCM_SHA384	12.1-50.x, 13.0	NA
TLS1.3-CHACHA20-POLY1305-SHA256	0x1303	TLS_CHACHA20_POLY1305_SHA256	12.1-50.x, 13.0	NA