

Silver Peak: SSL Acceleration Supportability Matrix

VXOA Release	Key Exchange	Ciphers	Digest	Protocol	Cert Format	Supported extension
6.2.x	RSA	AES128	MD5	ssl v3	PEM	SSL_EXT_SERVER_NAME: SSL_EXT_MAX_FRAGMENT_LENGTH: SSL_EXT_RENEGOTIATION_INFO: SSL_EXT_ELLIPTIC_CURVES: SSL_EXT_EC_POINT_FORMATS: SSL_EXT_SIGNATURE_ALGORITHMS:
	RSA	AES256	SHA1	TLS 1.0	PFX	
		RC4	SHA2 (SHA 256 supported)	TLS 1.1		
		3DES		TLS 1.2		
7.3.x	RSA	AES128	MD5	ssl v3	PEM	Support for all 6.2.x and following SSL_EXT_TRUSTED_CA_KEYS: SSL_EXT_SESSION_TICKET: SSL_EXT_HEARTBEAT: SSL_EXT_ALPN: SSL_EXT_STATUS_REQUEST: SSL_EXT_STATUS_REQUEST_V2: SSL_EXT_NEXT_PROTOCOL_NEGOTIATION:
	DHE	AES256	SHA1	TLS 1.0	PFX	
	ECDHE	AES128-GCM	SHA2 (SHA 384 supported)	TLS 1.1		
		AES256-GCM		TLS 1.2		
		RC4				
		3DES				
8.x	RSA	AES128	MD5	ssl v3	PEM	Same as 7.3
	DHE	AES256	SHA1	TLS 1.0	PFX	
	ECDHE	AES128-GCM	SHA2 (SHA 384 supported)	TLS 1.1		
		AES256-GCM		TLS 1.2		
		RC4				
		3DES				