[MS-TLSP]: Transport Layer Security (TLS) Profile

This topic lists the Errata found in [MS-TLSP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V10.0 – 2017/06/01.

Errata Published*	Description
2017/09/05	In Section 1, Introduction, added support for TLS 1.1 and TLS 1.2 in Windows Server 2008 SP2. Changed from: Support for TLS/SSL authentication is specified in [RFC5246], [RFC2246], [SSL3], and [PCT1]. Supported TLS extensions are specified in [RFC4366], [RFC3546], [RFC4681], and [RFC5077]. Additional supported cipher suites are defined in [RFC3268], [RFC4279], [RFC4492], [RFC5289], [RFC5487], and [IETFDRAFT-CURVE-25519-01]. This document specifies the differences in the Windows implementation from what is specified in the referenced documents, where applicable.<1> <1> Section 1: Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 implement TLS 1.2 as specified mainly in [RFC5246] with extensions from [RFC4366], [RFC4681], and [RFC5077], additional cipher suites from [RFC3268], [RFC4492], [RFC5289], TLS 1.1 from [RFC4346], and SSL from [SSL3]. Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012 implement TLS 1.2 as specified mainly in [RFC5246] with extensions from [RFC4366] and [RFC4681], additional cipher suites from [RFC3268], [RFC4492], [RFC5289], TLS 1.1 from [RFC4346], and SSL from [SSL3]. Windows Vista and Windows Server 2008 implement TLS 1.0 as specified mainly in [RFC2246] with extensions from [RFC3546] and [RFC4681], additional cipher suites from [RFC3268] and [RFC4492], and SSL from [SSL3]. Changed to: Support for TLS/SSL authentication is specified in [RFC5246], [RFC2246], [SSL3], and [PCT1]. Supported TLS extensions are specified in [RFC4366], [RFC3546], [RFC4681], and [RFC5077]. Additional supported cipher suites are defined in [RFC3268], [RFC4279], [RFC4492], [RFC5289], [RFC5487], and [IETFDRAFT-CURVE-25519-01]. This document specifies the differences in the Windows implementation from what is specified in the referenced documents, where applicable.<1> <1> Section 1: TLS 1.2, as specified in [RFC5246] with extensions from [RFC4366] and [RFC4681], additional cipher suites from [RFC3268], [RFC4492], [RFC5289], TLS 1.1 from [RFC4346], and SSL from [SSL3] are supported in Windows except in Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008 prior to Windows Server 2008 operating system with Service Pack 2 (SP2). [RFC5077] is supported in Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016.

Errata Published*	Description
	Windows Vista and Windows Server 2008 prior to Windows Server 2008 with SP2 implement TLS 1.0 as specified mainly in [RFC2246] with extensions from [RFC3546] and [RFC4681], additional cipher suites from [RFC3268] and [RFC4492], and SSL from [SSL3].

*Date format: YYYY/MM/DD