Microsoft

TLS 1.2 & Office 365: Are you ready?

New York Exchange User Group

Jon Butler
Microsoft Premier Field Engineer
jon.butler@microsoft.com

Tonight’s agenda

- Security concepts refresher
- What’s changing in Office 365?
- Why should you care?
- How to prepare
- Additional resources

What makes encryption work?

SSL

Netscape, 2.0 (1995), 3.0 (1996), prohibited in 2015

TLS

1.0 (1999), 1.1 (2006), 1.2 (2008)

Cipher suites

Schannel

WinHTTP

.NET

Client & Server – which is Exchange?

What’s changing in Office 365?

On October 31, 2018, Office 365 will no longer accept connections using encryption protocols older than TLS 1.2.

So what? What's the big deal?

What components of Exchange utilize encrypted connections?

EVERYTHING DOES!

What if I’m not an Office 365 subscriber?

Do you ever send an email to someone who is?

Do you receive encrypted email from someone who is?

Do you federate with any O365 tenants?

Do you access shared files from OneDrive for Business?

Do you join Skype for Business meetings?

Do you like to stay supported?

YES, YOU NEED TO PREPARE.

How to prepare your environment

- Eliminate out-of-support stuff
- Enable and set TLS 1.2 as default
- Patch your servers <u>and</u> workstations
- Investigate all 3rd parties – MDM, hygiene, vaults, etc.
- Consider apps and custom code!
- Test, test, test, test, test

You DO NOT have to disable TLS 1.0 and 1.1, just make sure TLS 1.2 is the default choice (unless you're PCI, etc.)

What definitely won’t work?

- Exchange 2007 and earlier
- Android 4.3 and earlier
- IE 10 and earlier
- Old versions of Firefox, Chrome, and Safari
- OS X 10.8.4 and earlier
- Windows XP & Vista

Operating system support

Windows OS	SSLv2	SSLv3	TLS 1.0	TLS 1.1	TLS 1.2
Windows Vista	Enabled	Enabled	Default	Not Supported	Not Supported
Windows Server 2008	Enabled	Enabled	Default	Disabled	Disabled
Windows 7 (WS2008 R2)	Enabled	Enabled	Default	Disabled	Disabled
Windows 8 (WS2012)	Disabled	Enabled	Enabled	Enabled	Default
Windows 8.1 (WS2012 R2)	Disabled	Enabled	Enabled	Enabled	Default
Windows 10	Disabled	Enabled	Enabled	Enabled	Default
Windows Server 2016	Not Supported	Disabled	Enabled	Enabled	Default

Current OS Guidance

Windows Server 2008 SP2

TLS 1.2 is not supported by default.

- Install all latest Windows Updates
  - Include recommended update KB4019276 for TLS 1.2
  - Include security update KB3161949 for updated WinHTTP
- If SHA512 required, install KB2973337
- If Exchange 2010, install KB3154517 for .NET update

Windows Server 2008 R2 SP1, Windows 7

TLS 1.2 is supported but not enabled by default.

- Install all latest Windows Updates
  - Include security update KB3161949 for updated WinHTTP
  - Include recommended update KB3080079 for RDP support
- If SHA512 required, install KB2973337
- If Exchange 2010, install KB3154518 for .NET update

Windows Server 2012, Windows 8

TLS 1.2 is the default.

- Install all latest Windows Updates
  - Include security update KB3161949 for updated WinHTTP
- If SHA512 required, install KB2973337
- If Exchange 2010, install KB3154519 for .NET update

Windows Server 2012 R2, Windows 8.1

TLS 1.2 is the default.

- Install all latest Windows Updates
  - Include security update KB3161949 for updated WinHTTP
- If SHA512 required, install KB2973337

Windows Server 2016, Windows 10

TLS 1.2 is the default.

- Install all latest Windows Updates

Current Exchange Guidance

Exchange Server 2003 & 2007

Upgrade, dude. Seriously. Come on.

Exchange Server 2010

- Install SP3 Rollup Update 19
- Install latest .NET 3.5.1 with patches

RU20 will allow disabling TLS 1.0 and 1.1

Exchange Server 2013

- Install Cumulative Update 19
- Install latest .NET 4.7.1 w/ patches – don’t miss this!!

CU20 will allow disabling TLS 1.0 and 1.1

Exchange Server 2016

- Install Cumulative Update 8
- Install latest .NET 4.7.1 w/ patches – don’t miss this!!

CU9 will allow disabling TLS 1.0 and 1.1

Workstations, app servers, black boxes

- All workstations should also be updated
- All app servers should also be updated
- All custom/3rd party apps should also be updated
  - Possible .NET supportability concerns, be thorough!
- Don’t forget printers, appliances, etc.

*TLS reports for SMTP are available in the S&CC

Additional resources

https://blogs.technet.microsoft.com/exchange/2018/01/26/exchange-server-tls-guidance-part-1-getting-ready-for-tls-1-2/

Watch for parts 2 and 3, coming soon

https://blogs.technet.microsoft.com/exchange/2018/02/09/an-update-on-office-365-requiring-tls-1-2/

KB4057306: Preparing for TLS 1.2 in Office 365

Solving the TLS 1.0 Problem