

<https://www.microsoft.com/en-us/download/details.aspx?id=55266>

<https://tecadmin.net/enable-tls-on-windows-server-and-iis/>

Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows

Applies to: Windows Server 2012 Datacenter

Windows Server 2012

Standard Windows Server 2012 Essentials

<https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi>

- free tool to make the TLS 1.2 REG keys automatically
<https://www.nartac.com/Products/IISCrypto/>

<https://trustzone.com/knowledge-base/how-to-enable-tls-1-2-on-windows-server-2008-2016/>

Final Notice for disabling of TLS1.0 and TLS 1.1 Support for Exchange Online Mail Flow

MC229914 · Published Dec 14, 2020

<https://admin.microsoft.com/AdminPortal/Home?ref=/MessageCenter/:/messages/MC229914>

Service

Exchange Online

Tag

ADMIN IMPACT

USER IMPACT

Message Summary

We will no longer support TLS 1.0 and TLS 1.1 from Exchange Online mail flow endpoints beginning January 11th 2021. As those versions of TLS are already retired (most recently communicated in MC218794, July '20), Exchange Online customers and their partners should already be using TLS1.2 to protect SMTP connections between their email servers or devices and Exchange Online.

Key Points:

- Major: Retirement
- Timing: January 11th, 2021
- Action: Review and assess impact for your organization

How this will affect your organization:

Organizations who are most at risk are those with hybrid routing and on-premises servers however there may be disruptions to mail flow for numerous other scenarios where these older TLS versions are still being used. If you have not done so already, please ensure that all mail servers and devices connecting to Exchange Online use TLS1.2. While some traffic may still flow after the change is made

because TLS is used opportunistically by default, connections involving on-premises or partner connectors require TLS and the certificates that are shared for authentication purposes.

To help identify traffic still using TLS1.0 and TLS 1.1 review: [Investigating TLS usage for SMTP in Exchange Online](#).

We'll be gradually making the change and so initial impact could be messages getting delayed and only when the change is completed will messages fail to be delivered to their destinations.

What you need to do to prepare:

Any mail servers, devices, or applications sending emails to your Exchange Online endpoint (.mail.protection.outlook.com) or receiving email from Exchange Online servers will need to be upgraded to make use of TLS1.2.

Resources:

- [Preparing for TLS 1.2 in Office 365 and Office 365 GCC](#)
- [Investigating TLS usage for SMTP in Exchange Online](#)

[Additional information](#)