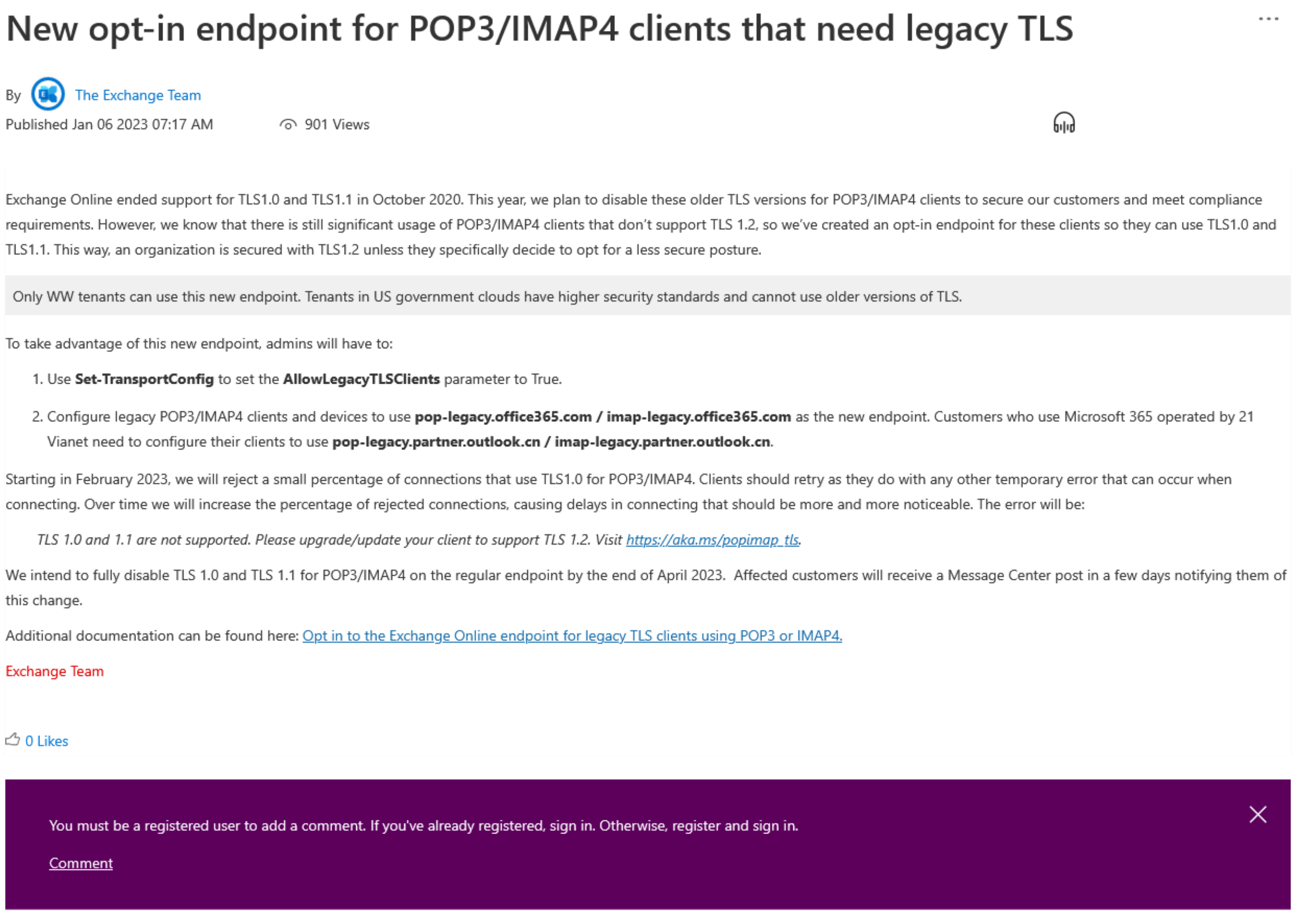
微软宣布 Exchange Onlin：将终止POP3和IMAP4的TLS 1.0/1.1 支持

1 月 7 日消息，微软本周发布公告，将会下月开始为使用 Post Office Protocol 3（POP 3）和 Internet Message Access Protocol 4（IMAP 4）协议的 Exchange Online 用户终止对 TLS 1.0/1.1 的支持。



New opt-in endpoint for POP3/IMAP4 clients that need legacy TLS

By The Exchange Team
Published Jan 06 2023 07:17 AM   901 Views

Exchange Online ended support for TLS1.0 and TLS1.1 in October 2020. This year, we plan to disable these older TLS versions for POP3/IMAP4 clients to secure our customers and meet compliance requirements. However, we know that there is still significant usage of POP3/IMAP4 clients that don't support TLS 1.2, so we've created an opt-in endpoint for these clients so they can use TLS1.0 and TLS1.1. This way, an organization is secured with TLS1.2 unless they specifically decide to opt for a less secure posture.

Only WW tenants can use this new endpoint. Tenants in US government clouds have higher security standards and cannot use older versions of TLS.

To take advantage of this new endpoint, admins will have to:

1. Use **Set-TransportConfig** to set the **AllowLegacyTLSClients** parameter to True.
2. Configure legacy POP3/IMAP4 clients and devices to use **pop-legacy.office365.com / imap-legacy.office365.com** as the new endpoint. Customers who use Microsoft 365 operated by 21 Vianet need to configure their clients to use **pop-legacy.partner.outlook.cn / imap-legacy.partner.outlook.cn**.

Starting in February 2023, we will reject a small percentage of connections that use TLS1.0 for POP3/IMAP4. Clients should retry as they do with any other temporary error that can occur when connecting. Over time we will increase the percentage of rejected connections, causing delays in connecting that should be more and more noticeable. The error will be:

TLS 1.0 and 1.1 are not supported. Please upgrade/update your client to support TLS 1.2. Visit https://aka.ms/popimap_tls.

We intend to fully disable TLS 1.0 and TLS 1.1 for POP3/IMAP4 on the regular endpoint by the end of April 2023. Affected customers will receive a Message Center post in a few days notifying them of this change.

Additional documentation can be found here: Opt in to the Exchange Online endpoint for legacy TLS clients using POP3 or IMAP4.

Exchange Team

You must be a registered user to add a comment. If you've already registered, sign in. Otherwise, register and sign in.

微软在公告中表示，组织可以通过配置继续在 Exchange Online 客户端上使用 TLS 1.0/1.1 更新。不过本配置更改仅适用于“ 特别决定选择不太安全的状态 ”的组织。

微软解释说，从下个月开始，为这些 POP 3 和 IMAP 4 客户端禁用 Exchange Online 中的 TLS 1.0 和 TLS 1.1 支持将是一个渐进的过程：

从 2023 年 2 月开始，我们开始拒绝对 POP3 / IMAP4 使用 TLS1.0 的连接 。客户端在处理连接时可能会一些连接失败情况。随着时间的推移，我们将增加拒绝连接的百分比，让连接延迟越来越明显。

组织最终会收到一条错误消息，通知他们不支持 TLS 1.0 和 TLS 1.1。在 2023 年 4 月之后 POP 3 和 IMAP 4 客户端将禁止使用这些安全协议。

如果可能，组织应该转向使用更安全的 TLS 1.2 安全协议。早在 2020 年 10 月，微软就已经为其使用 POP 3 和 IMAP 4 以外的其它客户端协议的非政府 Exchange Online 客户禁用了 TLS 1.0 和 TLS 1.1 支持。

Exchange Online 团队一直让客户了解该服务使用的各种过期或不安全的协议。上个月，它宣布终止对 Exchange Online 的基本身份验证支持，这是一项历时数年的重大安全改进，以及许多公开警告，最终得以实施。

TLS 的全称是传输层安全性协议。传输层安全性协议及其前身安全套接层是一种安全协议，目的是为互联网通信提供安全及数据完整性保障。网景公司在 1994 年推出首版网页浏览器－网景导航者时，推出 HTTPS 协议，以 SSL 进行加密，这是 SSL 的起源。IETF 将 SSL 进行标准化，1999 年公布 TLS 1.0 标准文件。

本文链接：https://dqcm.net/zixun/16731573725457.html