

升级终端以支持适用于Umbrella服务的TLS 1.2

目录

[简介](#)

[TLS 1.2要求概述](#)

[TLS 1.0/1.1支持的更新](#)

[保护AnyConnect或漫游客户端设备](#)

[安全Web网关支持](#)

[Umbrella Active Directory连接器要求](#)

[Umbrella代理：最低版本要求](#)

[Windows漫游客户端或AnyConnect模块](#)

[macOS漫游客户端或AnyConnect模块](#)

[其他常见问题](#)

[如果终端在截止日期前未更新，会发生什么情况？](#)

[注册表项是否适用于旧版本？](#)

[是否可以仅测试TLS 1.2？](#)

[为什么弃用TLS 1.0和1.1？](#)

[为什么选择2020年3月31日？](#)

[这会影响使用最新设备的用户吗？](#)

[更新TLS 1.2的终端后，是否需要进一步操作以重新启用Umbrella支持？](#)

[如何确认TLS 1.2的终端支持？](#)

[Windows Web浏览器支持](#)

[Windows .NET Framework支持](#)

[适用于Apple Mac和其他系统](#)

简介

本文档介绍如何为需要TLS 1.2的Umbrella服务准备终端和应用。

TLS 1.2要求概述

截至2020年3月31日，Umbrella服务器和服务不再支持传输层安全(TLS)1.0和1.1。所有终端必须支持TLS 1.2才能与Umbrella一起正常工作。

TLS 1.0/1.1支持的更新

- 除AnyConnect、Umbrella漫游客户端和AD连接器外，Umbrella在2020年3月终止了对TLS 1.0/1.1的支持。
- 由于后端依赖性，某些控制面板和API服务继续接受TLS 1.0/1.1连接，直到2021年1月27日。在此日期之后，这些服务不再接受TLS 1.0/1.1连接。
- 必须检查无法访问控制面板或API的设备以获取TLS 1.2支持。

保护AnyConnect或漫游客户端设备

Umbrella将最后期限延长至2021年1月27日，以便完成对TLS 1.2的升级。不再有进一步的扩展。在2021年1月27日之后不符合TLS 1.2要求的AnyConnect和漫游客户端设备不再受到Umbrella的保护。

安全Web网关支持

- Umbrella不支持在安全网关产品中使用TLS 1.0或1.1的HTTPS流量。
- 在2021年1月27日之前，仅当禁用HTTPS解密时，安全Web网关才为这些协议提供有限的支持。
- [将所有客户端操作系统配置为支持TLS 1.2。](#)
- 根据需要升级或修改非浏览器应用程序，以确保TLS 1.2兼容性。请与应用程序供应商联系以获取指导。

Umbrella Active Directory连接器要求

Umbrella不支持在生命周期已终止的Windows操作系统上部署的Active Directory连接器。运行在不支持的Windows版本（Windows Server 2008、2008 R2或Windows 7）上的AD连接器停止与Umbrella同步，并在2021年1月27日进入错误状态。

Umbrella代理：最低版本要求

Windows漫游客户端或AnyConnect模块

- Cisco Umbrella漫游客户端：版本2.2.356或更高版本
- 带Umbrella漫游模块的Cisco AnyConnect: [版本4.8.02042或更高版本](#)
- 要使用较旧的客户端版本，请通过Windows注册表更改配置TLS 1.2（请参阅下面的步骤）。
- Microsoft .NET Framework: [版本4.6.2或更高版本，或带有.NET 3.5.1的修补的Windows 7](#)（AnyConnect需要.NET 4.x或更高版本）
- 支持的Windows版本：7、8、8.1、10

macOS漫游客户端或AnyConnect模块

- 任何版本的Umbrella漫游客户端或AnyConnect漫游模块都支持TLS 1.2
- 支持的macOS版本：10.9或更高版本

其他常见问题

如果终端在截止日期前未更新，会发生什么情况？

无法协商TLS 1.2连接的终端无法访问Umbrella系统，包括控制面板、智能代理服务和阻止页面。对于在AnyConnect、Umbrella Enterprise Roaming Client或Umbrella AD Connector中运行Umbrella漫游模块的客户，客户端无法连接到任何Umbrella服务。这会导致客户端无法与

Umbrella控制面板同步配置和状态。

现有漫游客户端停止激活并在下一次服务启动时保持未保护状态。不支持TLS 1.2的新客户端无法向Umbrella注册。这些客户端无法打开；DNS继续通过本地网络堆栈进行解析，但漫游客户端安全服务不会激活。

尝试访问受阻站点或通过智能代理路由的设备，无法连接。使用漫游客户端的设备无法访问Umbrella网站、阻止页面或代理服务。

注册表项是否适用于旧版本？

是，适用于AnyConnect。应用注册表编辑后继续使用旧版本以首选强加密。在列出的最低版本之前，漫游客户端启动HTTPS连接，但未明确指定TLS 1.2强加密。如果.NET支持TLS 1.2，则默认使用它。注册表项强制使用.NET强加密，以复制新客户端版本中的更新。不支持早于最新版本的独立漫游客户端。

是否可以仅测试TLS 1.2？

Yes. [在Windows注册表中禁用TLS 1.0和TLS 1.1，以验证设备是否仅使用TLS 1.2完全运行。](#)

为什么弃用TLS 1.0和1.1？

TLS 1.0和1.1已经过时，缺乏对现代加密算法的支持。它们包含攻击者可以利用的漏洞。 [Internet工程任务组正在弃用这两种协议](#)。大多数加密互联网流量使用TLS 1.2，它是在十年前推出的。

为什么选择2020年3月31日？

在此时间范围内，业界正在弃用TLS 1.0和1.1。 [Google](#)、[Microsoft](#)、[Apple](#)和[Mozilla](#)都宣布其浏览器自2020年3月起不再支持TLS 1.0和1.1。

这会影响使用最新设备的用户吗？

否。大多数网站支持TLS 1.2。根据[Qualys SSL Labs](#),95.2%的网站支持TLS 1.2。预计这一数字将在2020年3月增加。少数网站无法运行，但整体用户影响最小。确保最新设备包含用于Windows计算机的.NET的正确版本。

更新TLS 1.2的终端后，是否需要进一步操作以重新启用Umbrella支持？

在大多数情况下，不需要采取进一步的行动。客户端使用安全TLS 1.2协议与Umbrella系统重新建立通信。对于Umbrella企业漫游客户端或Umbrella漫游客户端，如果在客户端软件更新期间系统脱机，则恢复可能会出现延迟。客户端需要在服务完全恢复之前下载更新。

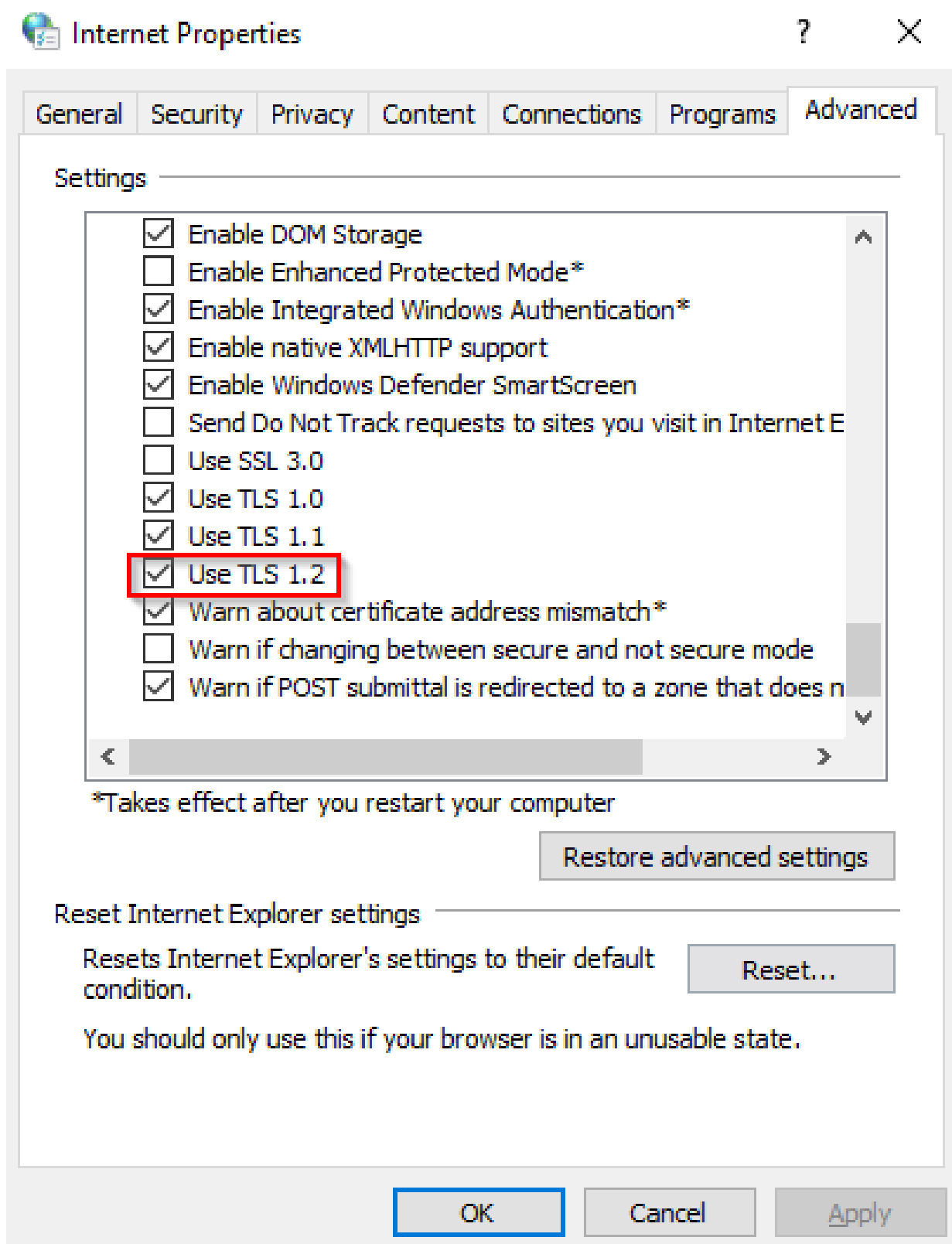
如何确认TLS 1.2的终端支持？

- Windows Web浏览器支持
 - 访问Umbrella控制面板和相关网站。

- [运行SSL Labs Browser Test](#)。在Protocols部分的TLS 1.2旁边显示“**Yes**”（ 确认 ）。

- Windows .NET Framework支持

- 适用于企业漫游客户端、AnyConnect漫游模块或AD连接器。
- .NET 4.6.2或更高版本提供本地TLS 1.2支持。
- 以前的版本需要注册表编辑(4.x)或注册表编辑和手动修补程序补丁(3.5)。
- 此信息适用于在.NET framework上运行的Umbrella软件，包括AD连接器和漫游客户端
-
- 通过完成Microsoft提供的说明，在操作系统级别禁用SSL、TLS 1.[0](#)和[TLS 1.1](#)。



blobid0.png

- 适用于Apple Mac和其他系统
- 执行[SSL Labs Browser Test](#)。确认Protocols部分的TLS 1.2旁边显示“Yes”。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。