

网络或Web服务器阻止的思科TMS系统反馈

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络或Web服务器阻止的思科TMS系统反馈](#)

简介

本文档介绍如何排除网络或Web服务器阻止的思科网真管理套件(TMS)的反馈问题。

先决条件

要求

思科建议您了解思科TMS。

使用的组件

本文档中的信息基于思科TMS。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络或Web服务器阻止的思科TMS系统反馈

思科TMS依靠从系统发送的反馈，并根据序列号、MAC地址和IP地址验证与其连接的终端。大多数思科网真和第三方系统通过匿名的HTTP或HTTPS连接发送此反馈，如果网络上有需要身份验证的Web代理，这些连接可能会被阻止。在这种情况下，您应该与代理的管理员联系，为发往思科TMS的流量添加例外。

如果防火墙阻止从系统到思科TMS的新连接，则还可以阻止反馈到思科TMS。

提示：思科[TMS支持文档](#)概述了每种系统类型必须具有哪些端口和协议。

当管理员在安装思科TMS后手动修改互联网信息服务(IIS)配置并禁用对Web目录的匿名访问时，会发生上一次常见连接故障。

注意：匿名访问仅对思科TMS的某些部分开放，并且不能禁用，因为系统在发送反馈时不使用用户名和密码。

要更正任何IIS配置错误，请卸载Cisco TMS并重新安装。只要数据库保持完整且安装程序正确重建网站属性，就不会丢失任何数据。