在启用Umbrella时解决协作（前沿）代理连接问题

目录

问题

启用Cisco Umbrella时，Cowork(Frontier)代理在笔记本电脑上无法正常工作。当Cisco Umbrella处于非活动状态时，代理按预期运行。当Umbrella处于活动状态时，用户无法使用Cowork代理功能，当用户遇到此问题时，Cisco Umbrella中看不到任何阻止日志。提供的错误屏幕截图显示了Umbrella操作期间应用程序故障。

环境

- 在企业笔记本电脑上部署的Cisco Umbrella
- Cowork(Frontier)代理应用程序
- 在Cisco Umbrella中启用SSL/TLS流量检查
- 在Cowork应用程序中实现证书锁定

分辨率

通过将Cowork应用程序添加到Cisco Umbrella中的Do Not Decrypt(DND)列表，问题得以解决。此配置更改允许Cowork代理绕过SSL/TLS检查并维护其与Cowork服务器的直接加密连接。

配置DND列表的步骤

步骤 1：访问Cisco Umbrella控制面板并导航至SSL解密策略配置。

步骤 2：将Cowork-related domains和URLs添加到Do Not Decrypt列表，以绕过此应用程序的SSL检查。

步骤 3：应用策略更改，并留出时间让配置传播到所有终端。

步骤 4：在启用Cisco Umbrella的情况下测试Cowork agent功能，以验证操作是否正确。

验证

实施DND列表配置后，Cowork应用程序在启用Cisco Umbrella的情况下正常运行。内部测试确认，在几天监控后问题不再出现，所有用户都能如预期一样访问Cowork功能。

原因

Cowork(Frontier)代理使用证书锁定作为安全机制。证书固定意味着应用经过硬编码，仅接受和信任其自己的特定服务器证书。当Cisco Umbrella拦截流量并显示思科证书而不是原始服务器证书时，Cowork应用会检测到此更改，假定连接不安全，并故意丢弃连接以保护数据。这是实施证书固定安全措施的应用的预期行为。

相关内容

- 为Microsoft应用程序创建有效的“不解密”列表
- 思科技术支持和下载

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）。