

了解常见证书和TLS协议错误

目录

[简介](#)

[概述](#)

[证书错误](#)

[上游证书已过期](#)

[上游证书自签名](#)

[缺少中间证书](#)

[上游证书缺少主题名称。](#)

[上游证书缺少公用名。](#)

[上游证书不受信任](#)

[证书中的主机名与预期不同](#)

[已撤销上游证书](#)

[TLS握手错误](#)

[不支持的上游密码](#)

[上行TLS版本不匹配](#)

[小于1024位的上游DH密钥](#)

[解决方法](#)

简介

本文档介绍Umbrella Dashboard Activity Search中的常见证书和TLS协议错误。

概述

由于证书和TLS错误而阻止的HTTP流量现在可在Umbrella Dashboard Activity Search中查看。本文提供常见错误消息列表以及每个错误的简要说明。

证书错误

上游证书已过期

网站提供的证书已过期。请与网站管理员联系以报告此问题。

上游证书自签名

网站提供的服务器证书不是由证书颁发机构签名的，因此Umbrella无法确定证书是否可信。

自签名证书有时在服务器托管面向受限受众的资源时使用。例如，IT安全设备的网络门户通常默认使用自签名证书。无法将Umbrella配置为信任自签名证书。

缺少中间证书

Umbrella无法为所有中间机构获取证书，因此无法验证整个信任链。

Web服务器证书通常为证书颁发机构的中间证书颁发/签名。这些中间证书也可以由其他中间证书颁发。Web服务器证书（也称为“枝叶证书”）和任何中间证书形成回根证书的链。网站必须将中间证书与服务器证书捆绑在一起，以便Umbrella验证整个信任链。请与网站管理员联系以报告此问题。

或者，如果证书包括“授权信息访问”扩展，Umbrella会尝试自动获取中间人CA。请注意，启用HTTPS解密和文件检查时，Umbrella仅支持AIA扩展。

上游证书缺少主题名称。

证书的Subject字段不包含用于标识此证书的可分辨名称(DN)。这是由证书颁发机构颁发的所有证书的要求，因此是Cisco Umbrella的要求。请与网站管理员联系以报告此问题。

上游证书缺少公用名。

网站提供的证书没有公用名称。通用名称(CN)字段是Umbrella SWG必需的。这包含证书主机名，验证证书是否匹配用户请求的资源需要该主机名(例如，键入到浏览器中的地址)。请与网站管理员联系以报告此问题。

上游证书不受信任

证书不受Cisco Umbrella信任。此错误通常意味着Cisco不信任颁发证书的根CA。

Umbrella SWG有一个内置的已知受信任根证书颁发机构列表，我们可从信誉可靠的源更新该列表。如果网站的证书不是由此列表上的CA签署，则证书验证失败。如果您认为Umbrella缺少可信任的根CA，请与技术支持联系。

证书中的主机名与预期不同

用户请求的资源(例如键入到浏览器中的地址)与证书的公用名(CN)或主题备用名(SAN)不匹配，因此Umbrella无法信任此请求的证书。请与网站管理员联系以报告此问题。

已撤销上游证书

网站提供的证书已被证书颁发机构撤销。

Umbrella执行OCSP（在线证书状态协议）检查以确定证书是否被CA撤销。请与网站管理员联系以报告此问题。

TLS握手错误

不支持的上游密码

无法完成TLS握手。这通常意味着网站不支持Umbrella SWG使用的任何密码套件列表。如果较早或

过时的Web服务器只支持较弱的TLS密码，则可能会发生此错误。请与网站管理员联系以报告此问题。

上行TLS版本不匹配

无法完成TLS握手，因为网站不支持与Umbrella SWG相同的TLS版本。目前，Umbrella SWG代理在客户端连接到Umbrella SWG以及从Umbrella SWG代理连接到目标Web服务器时都支持TLS 1.2和TLS 1.3。

小于1024位的上游DH密钥

无法完成TLS握手，因为网站使用不受Umbrella支持的弱Diffie-Hellman密钥。请与网站管理员联系以报告此问题。

解决方法

通过在Cisco Umbrella中进行配置更改可以解决这些问题。只有当您信任服务器和证书的真实性时，才能执行此操作。

解决方法可以使用“选择性解密列表”条目禁用解密，或使用“外部域”条目完全绕过Umbrella的流量。禁用解密时，Umbrella不执行证书验证。请注意，在大多数情况下，当流量从Umbrella绕过时，浏览器仍会显示错误或警告 — Web浏览器执行类似的证书验证。

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）。