

排除HSTS和固定证书错误

目录

[简介](#)

[证书错误](#)

[可能的解决方案](#)

[策略管理和漫游客户端](#)

[忽略证书异常错误（仅限Windows的Chrome）](#)

[Firefox、Safari和Chrome for Mac OS X](#)

[Internet Explorer](#)

简介

本文档介绍如何清除无法绕过的“您的连接不受信任/非私有”证书错误。

证书错误

当出现*.opendns.com或*.cisco.com的证书错误，但无法通过Cisco Umbrella文档[管理Cisco Umbrella根证书](#)中所述的添加证书例外来绕过时，请使用以下步骤允许清除证书错误。

当无法通过添加例外来绕过证书错误时，这是因为现代浏览器中实施了HTTP严格传输安全(HSTS)或预加载的证书固定。某些浏览器和某些网站之间的通信方式包括使用HTTPS的要求，并且不可能出现旁路或异常。当[HSTS](#)对网站处于活动状态时，HTTPS页面的这种额外安全性会阻止Umbrella阻止页面和绕过阻止页面机制工作。

因此，无法通过[Block Page Bypass](#)(BPB)（实际上，Bypass屏幕甚至可能未出现）访问相关页面。这些方法可能允许访问BPB登录，但在登录后，证书错误再次出现并拒绝访问。如果您在Google Chrome、Mozilla Firefox和Safari中看到无法绕过的证书错误，并且您正在尝试访问绕行登录，请查看本文的其余部分。



注意：针对此问题的解决方案现已推出，该解决方案更易于管理且适用于所有站点。

因此，此信息仍然适用，但是现在可以使用永久解决方案进行解决。尝试通过Cisco Umbrella文档安装思科根CA：[管理思科Umbrella根证书](#)

重要信息：如果域在HSTS固定列表上，则无法添加异常，因为如果运行Chrome、Safari或Firefox(Internet Explorer(IE)不受影响)，则列表实际上是不可绕行的。Block Page Bypass不适用于此类网站。有关这三个浏览器使用HSTS的服务的完整列表，请查看[Google Chromium代码搜索](#)。此列表中值得注意的服务包括：

- Google (和Google资源，例如Gmail、Youtube或Google Docs)
- 收存箱
- 推特
- 脸书

如果这对您或您的用户造成问题，并且您希望看到对Block Page Bypass的更改以帮助缓解此问题，请发送电子邮件至umbrella-support@cisco.com或您的客户经理提交功能请求。我们的产品管理

和工程团队意识到证书和阻止页面绕行的困难，并正在测试此功能的替代重新设计。

可能的解决方案

有几种方法可以解决这些问题。首先，这些部分演示如何使用更精细的策略来解决此问题。其次，您可以使用浏览器配置，但这些配置与受此问题影响的浏览器的子集无关。

策略管理和漫游客户端

您的网络配置或可接受的使用率(HR)策略可能存在问题，导致无法提供此解决方案。如果允许用户仅在特定时间（如午休时间）访问这些域，策略管理不是有效的解决方案。Umbrella无法通过我们的服务提供基于时间的策略应用，因此仅允许用户随时访问站点可能会有问题。在共享计算机（如公共终端）上，Umbrella漫游客户端无法区分用户，也无法轻松允许合适的人使用合适的域。

当考虑非粒度身份（如站点或网络）时，策略管理效果较差，除非管理员愿意为该网络的所有用户提供相同的访问权限。当策略管理应用于允许访问站点的用户子集，而网络其余部分不能访问站点时，策略管理效果最佳，并且通过在用户计算机上安装漫游客户端并应用正确的策略层次结构来挑选这些用户。



注意：思科于2024年4月2日宣布雨伞漫游客户端寿命终止。Umbrella漫游客户端的最后支持日期是2025年4月2日。所有Umbrella漫游客户端功能当前在Cisco安全客户端中可用。思科仅提供思科安全客户端的未来创新。我们建议客户立即开始计划和安排迁移。有关如何从Umbrella漫游客户端迁移到Cisco安全客户端的指导，请参阅[此知识库文章](#)。

正确的策略管理是解决此问题的最佳解决方案，因为浏览器首先不会收到失败的验证响应。如果允许某些用户访问他们通常需要使用“阻止页面绕行”才能访问的站点，则您可以为这些用户配置单独的策略，并将允许他们使用的域添加到“允许列表”中。由于不会阻止用户的请求，因此浏览器永远不会收到来自证书不匹配的域的请求。您可以使用[Umbrella漫游客户端](#)提供这些特定策略。这意味着您将某些域放入允许列表中，以便某些用户在一天内的所有时间处理这些错误。



注意：Umbrella漫游客户端是一种将特定策略分发到多个用户的有效方法，但是如果已启用Active Directory(AD)集成，您也可以将这些允许的策略应用到特定AD用户。

忽略证书异常错误 (仅限Windows的Chrome)

仅适用于Windows的Chrome可配置为忽略证书例外错误，这将缓解此错误。浏览器被告知忽略该错误，改为看到正常的Umbrella块页面。

重要信息：此方法比调整策略管理更具风险，因为浏览器配置为忽略证书错误。因此，浏览器可能会受到中间人(MiTM)攻击。因此，我们不能建议将此作为处理此错误的安全方法，但它是解决方法。

这些配置更改必须针对每台计算机进行，这使得大型环境难以实现，但确实能正常工作。

Firefox、Safari和Chrome for Mac OS X

无法将Firefox、Safari和Chrome for Mac OS X 配置为忽略固定域的证书例外错误，并始终遵守

HSTS列表。对于这些错误，没有已知的解决方法。

Internet Explorer

Internet Explorer(IE)不实施HSTS限制。因此，IE不需要配置，也不显示此错误。如果Microsoft选择在浏览器中实施HSTS，IE的未来版本可能会对此进行更改。

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）。