

解决SWG和Symantec LiveUpdate兼容性问题

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题](#)

[强制SAML和HTTPS排除](#)

[解决方案](#)

[原因](#)

简介

本文档介绍如何解决安全Web网关(SWG)和Symantec产品与LiveUpdate的兼容问题。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco安全Web网关。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

本文面向采用LiveUpdate的安全Web网关(SWG)和Symantec产品的用户。如果您未将这些产品与SWG配合使用，则本文不适用。

本文适用于Symantec用户在SAML用户身份验证处于活动状态时，通过云交付防火墙(CDFW)、AnyConnect SWG代理、PAC文件或任何其他方法使用SWG的Symantec用户。在默认配置中，使用SWG可能导致Symantec崩溃，从而导致Windows中出现蓝屏。

强制SAML和HTTPS排除

当SAML身份验证在SWG上处于活动状态时，并非来自支持会话的浏览器的所有查询都会收到无法完成的重定向响应。在某些情况下，这可能会导致在发出请求的应用程序中出现意外行为。

解决方案

- 将liveupdate.symantecliveupdate.com添加到HTTPS解密绕行列表。
 - 这也会绕过SAML身份验证要求。
- 如果在AnyConnect中使用PAC或SWG模块，请将liveupdate.symantecliveupdate.com添加到Domain Management > External Domains列表。

原因

在Symantec LiveUpdate中，必须将liveupdate.symantecliveupdate.com添加到HTTPS解密例外列表，以允许LiveUpdate运行。这不包括来自SAML要求的这些请求，并使用标准策略响应来回应请求。

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）。