

了解Umbrella LA版本的阻止密码保护文件上传DLP功能

目录

[简介](#)

[背景信息](#)

[如何阻止受密码保护的文件上传？](#)

[如何打包阻止密码保护文件上传？](#)

[如何访问此功能？](#)

[是否可以在Umbrella控制面板中启用或禁用此功能？](#)

[在哪里可以找到支持的文件类型列表？](#)

简介

本文档介绍阻止密码保护文件上传DLP功能的有限可用性(LA)。

背景信息

阻止密码保护文件上传是防止数据丢失的重要措施，因为密码保护文件无法由DLP解决方案检查。

如何阻止受密码保护的文件上传？

启用此功能后，“阻止密码保护文件上传”(Block Password Protected File Upload)将应用于使用实时DLP (如内联) 规则配置的任何目标。

如果要阻止所有受密码保护的文件上传，必须至少有一个在Destination规则条件中设置“All Destinations”的Realtime DLP规则。

相反，如果只想阻止受密码保护的文件上传到特定目标，则必须确保它们没有在“目标”规则条件中设置“所有目标”的“实时DLP”规则。



注意：实时DLP规则中的目标例外项不适用于“阻止密码保护文件上传”，仍适用于所有目标。

如何打包阻止密码保护文件上传？

此功能可用于所有包含DLP的Umbrella软件包（例如SIG-A和DLP插件）。

如何访问此功能？

请打开支持票证，考虑注册此有限可用性功能。

是否可以在Umbrella控制面板中启用或禁用此功能？

现在不行。在您加入LA计划后，我们将代表您启用该计划。

在哪里可以找到支持的文件类型列表？

“阻止密码保护文件上传”支持的文件类型列表位于[此处](#)，并且可与LA客户共享。

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）。