配置安全Web设备以允许访客访问

目录

简介

本文档介绍允许未安装解密证书的用户通过安全Web设备(SWA)访问Internet的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 已安装物理或虚拟SWA。
- 许可证已激活或已安装。
- 安装向导已完成。
- 对SWA图形用户界面(GUI)的管理访问。

使用的组件

本文档不限于特定的软件和硬件版本。

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。

场景概述

本文讨论10.10.10.0/24 Wi-Fi子网内的网络访问控制方案。环境由两个不同的用户组组成，需要不同的安全和访问策略：

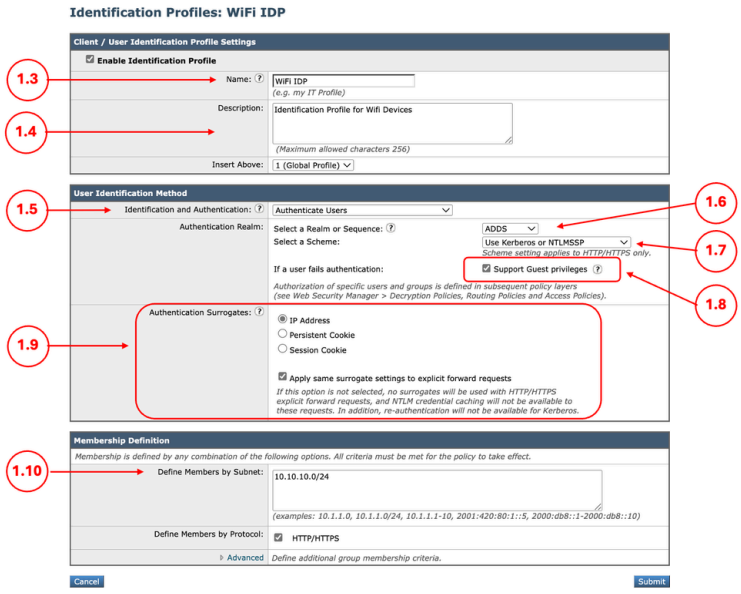
- 受管设备:公司发放的笔记本电脑，它们经过完全身份验证并安装了SWA解密证书。这些设备受信任，通常受标准企业访问策略的约束。
- 非托管/访客设备：未经身份验证且缺少SWA解密证书的个人笔记本电脑和移动设备。

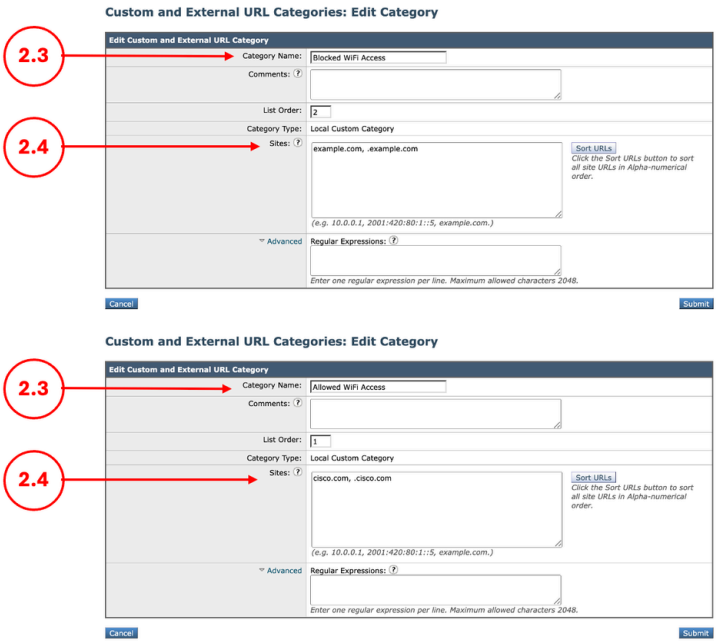
目标:
该公司旨在对未受管设备实施限制性Web访问策略，限制其连接到允许的URL的特定子集，同时确保公司资源保持安全。

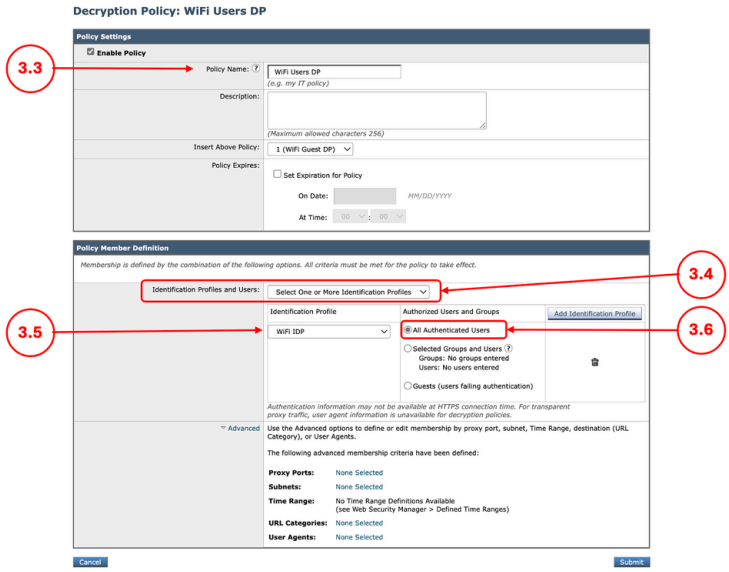
注意：由于解密证书在非受管设备上不受信任，因此无法解密HTTPS流量，并且必须将操作设置为通过。

配置步骤

步骤1.创建标识配置文件。	第1.1步：从SWA GUI，导航到网络安全管理器并选择标识配置文件。 第1.2步：点击添加标识配置文件。 步骤1.3.定义配置文件名称。 第1.4步(可选)定义说明。 第1.5步：选择Authenticate Users in Identification and Authentication。 第1.6步：从选择领域或序列中选择Active Directory领域。 第1.7步：从选择方案，选择所需的身份验证协议。 提示：请勿在Select a Scheme列表中选择Basic Authentication。 第1.8步：选择Support Guest privileges的复选框。 第1.9步(可选)根据您的设计，您可以通过启用Apply same surrogate settings to explicit forward requests来启用替代。 警告：由于无法解密流量，因此透明部署中不选

	⚠ 择Persistent Cookie或Session Cookie。 第1.10步：在“按子网定义成员”中定义IP地址子网。 步骤1.11.提交并提交更改。  图像 — 定义标识配置文件
步骤2.（可选）为允许和阻止的URL创建自定义URL类别	第2.1步：从GUI导航到网络安全管理器，然后选择自定义和外部URL类别。 第2.2步：单击Add Category以创建新的自定义URL类别。 第2.3步：为新类别输入Name。 第2.4步：定义要阻止访问的网站的域和/或子域。 第2.5步：提交更改。 第2.6步：使用相同的步骤为允许访问的网站创建URL类别。

	 图像 — 定义自定义URL类别
步骤3.创建受管设备的解密策略	第3.1步：从GUI，导航到网络安全管理器，然后选择解密策略 第3.2步：点击Add Policy。 第3.3步：输入新策略的Name。 第3.4步：从Identification Profiles和Users下拉菜单中选择一个或多个Identification Profiles。 第3.5步：选择在第1步中创建的Identification Profile。 第3.6步：选择所有身份验证用户。 第3.7步：单击提交。



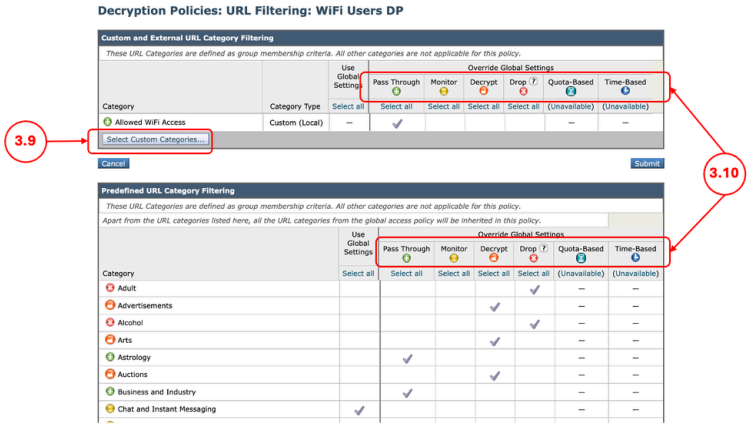
为受管设备创建解密策略

第3.8步：在Decryption Policies页中，点击新策略的URL Filtering中的链接。

第3.9步(可选)您可以通过点击选择自定义类别(Select Custom Categories)并在类别名称前面选择Include in Policy)来添加任何自定义URL类别

第3.10步：为每个自定义和外部URL类别过滤和预定义URL类别过滤配置操作。

第3.11步。单击提交



映像 — 配置解密策略的操作

步骤4.创建非托管设备的解密策略

第4.1步：从GUI，导航到网络安全管理器，然后选择解密策略

第4.2步：点击Add Policy。

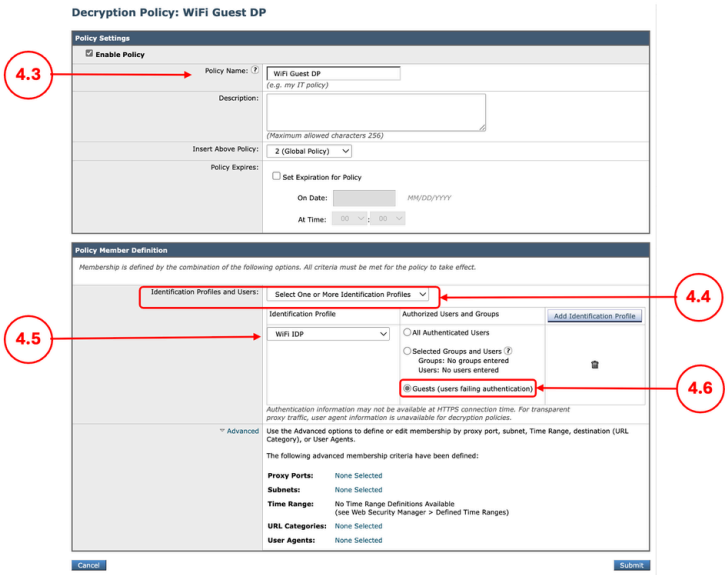
第4.3步：输入新策略的Name。

第4.4步：从Identification Profiles和Users下拉菜单中选择一个或多个Identification Profiles。

第4.5步：选择在第1步中创建的Identification Profile。

第4.6步：选择访客（身份验证失败的用户）。

第4.7步：单击提交。



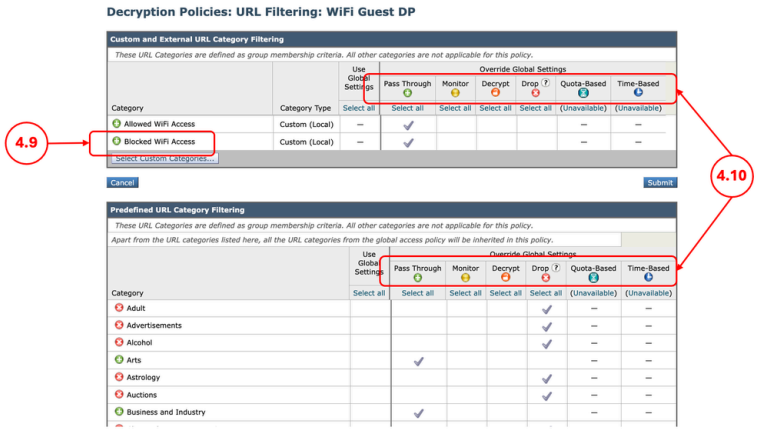
创建非托管设备的解密策略

第4.8步：在Decryption Policies页中，点击新策略的URL Filtering中的链接。

第4.9步(可选)您可以通过点击选择自定义类别(Select Custom Categories)并在类别名称前面选择Include in Policy)来添加任何自定义URL类别

第4.10步：为每个自定义和外部URL类别过滤和预定义URL类别过滤配置操作。

注意：请勿使用Decrypt作为操作，因为SWA解密证书在非受管设备上不受信任。

<table>
<tr>
<td></td>
<td>


映像 — 非托管设备的解密操作

第4.11步：向下滚动Uncategorized URLs部分选择正确的操作。

图像 — 未分类的URL

提示：对于安全方面，最好将操作设置为Drop，以防任何URL需要访问，您可以将它们添加到分配给策略的自定义URL类别中。

第4.12步。单击提交</td>
</tr>
<tr>
<td>步骤5.创建受管设备的访问策略</td>
<td>第5.1步：从GUI导航到网络安全管理器并选择访问策略

第5.2步：点击Add Policy。

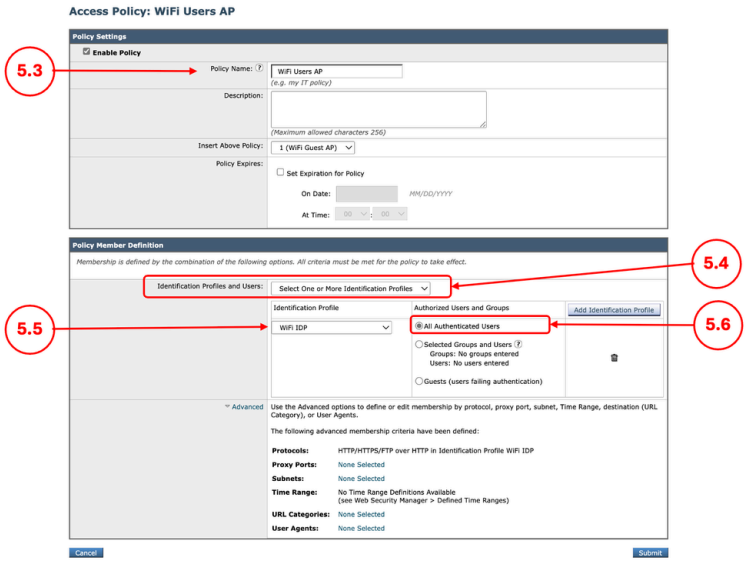
第5.3步：输入新策略的Name。

第5.4步：从Identification Profiles和Users下拉菜单中选择一个或多个Identification Profiles。

第5.5步：选择在第1步中创建的Identification Profile。

步骤5.6.选择All Authenticated Users(所有经过身份验证的用户)。

第5.7步：单击提交。</td>
</tr>
</table>

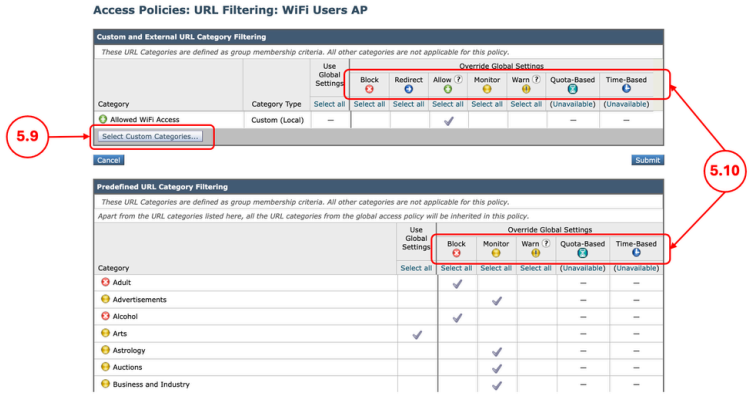
<table>
<tr>
<td></td>
<td>


映像 — 受管设备的访问策略

第5.8步：在Access Policies页中，点击新策略的URL Filtering中的链接。

第5.9步(可选)您可以通过点击选择自定义类别(Select Custom Categories)并在类别名称前面选择Include in Policy)来添加任何自定义URL类别

第5.10步：为每个自定义和外部URL类别过滤和预定义URL类别过滤配置操作。



映像 — 受管设备的访问策略URL过滤

第5.11步。单击提交。</td>
</tr>
<tr>
<td>步骤6.创建非受管设备的访问策略</td>
<td>第6.1步：从GUI导航到Web Security Manager，然后选择Access Policies

第6.2步：点击Add Policy。

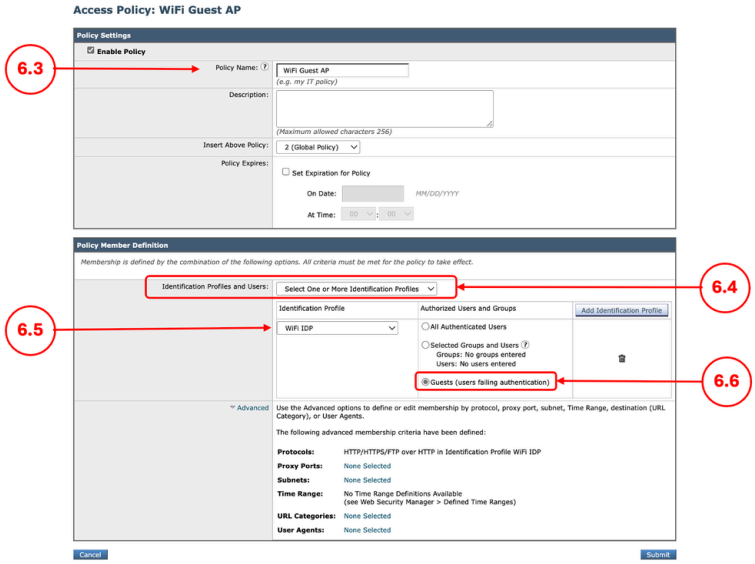
第6.3步：输入新策略的Name。</td>
</tr>
</table>

第6.4步：从Identification Profiles和Users下拉菜单中选择一个或多个Identification Profiles。

第6.5步：选择在第1步中创建的Identification Profile。

第6.6步：选择访客（身份验证失败的用户）。

第6.7步：单击提交。

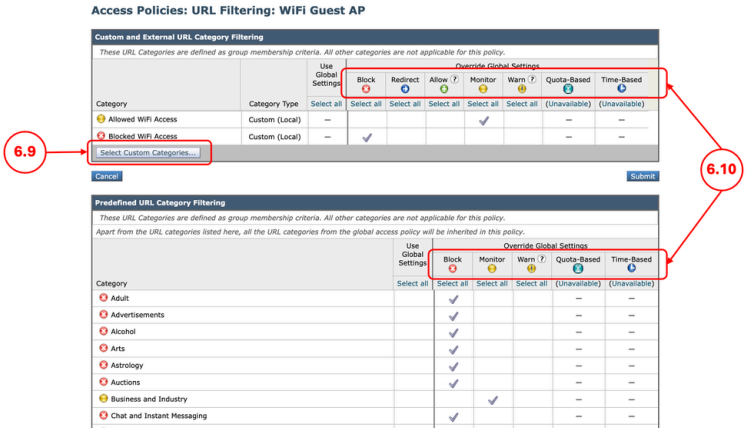


映像 — 非受管设备的访问策略

第6.8步：在Access Policies页中，点击新策略的URL Filtering中的链接。

第6.9步(可选)您可以通过点击选择自定义类别(Select Custom Categories)并在类别名称前面选择Include in Policy)来添加任何自定义URL类别

第6.10步：为每个自定义和外部URL类别过滤和预定义URL类别过滤配置操作。



映像 — 非受管设备的访问策略URL过滤

第6.11步：向下滚动Uncategorized URLs部分选择正确的操作。

图像 — 访问策略未分类的URL

提示：对于安全方面，最好将操作设置为Block，以防任何URL需要访问，您可以将它们添加到分配给策略的自定义URL类别中。

第6.12步。单击提交

步骤7.（可选）为受管设备创建思科数据安全策略

注意：如果您不想过滤受管设备的上传流量，可以跳过此步骤。

第7.1步：从GUI中，导航到Web Security Manager，然后选择Cisco Data Security。

第7.2步：点击Add Policy。

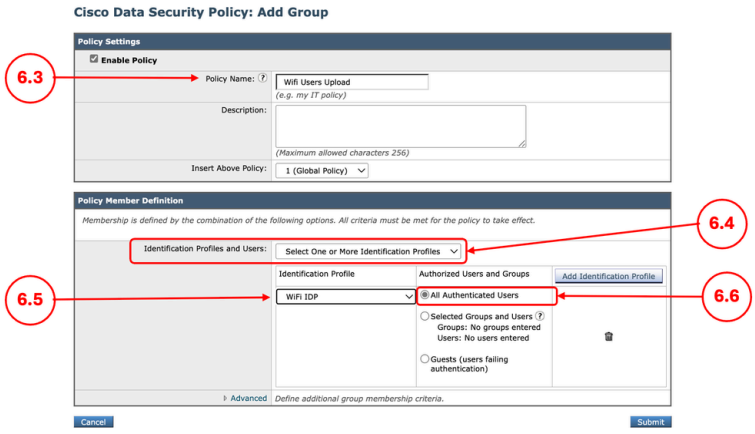
第7.3步：输入新策略的Name。

第7.4步：从Identification Profiles和Users下拉菜单中选择一个或多个Identification Profiles。

第7.5步：选择在第1步中创建的Identification Profile。

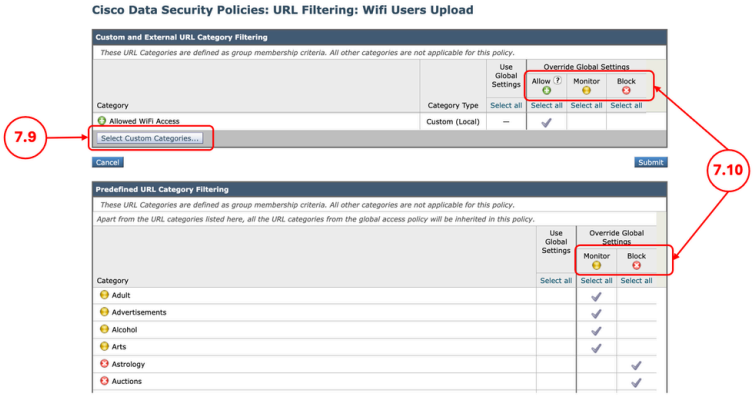
步骤7.6.选择All Authenticated Users(所有经过身份验证的用户)。

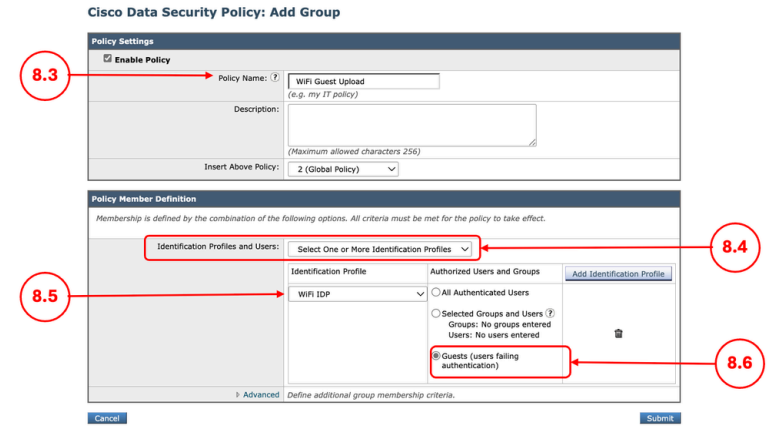
第7.7步：单击提交。



映像 — 适用于受管设备的思科数据安全策略

第7.8步：在Cisco Data Security Policies页中，点击新策略的URL Filtering中的链接。

	第7.9步(可选)您可以通过点击选择自定义类别(Select Custom Categories)并在类别名称前面选择Include in Policy)来添加任何自定义URL类别 第7.10步：为每个自定义和外部URL类别过滤和预定义URL类别过滤配置操作。  映像 — 受管设备的上传操作 第7.11步。单击提交。
步骤8.（可选）创建非托管设备的思科数据安全策略 注意：如果您不想过滤未管理设备的上传流量，可以跳过此步骤。	第8.1步：从GUI中，导航到Web Security Manager并选择Cisco Data Security。 第8.2步：点击Add Policy。 第8.3步：输入新策略的Name。 第8.4步：从Identification Profiles和Users下拉菜单中选择一个或多个Identification Profiles。 第8.5步：选择在第1步中创建的Identification Profile。 步骤8.6.选择All Authenticated Users(所有经过身份验证的用户)。 第8.7步：单击提交。



映像 — 适用于非受管设备的思科数据安全策略

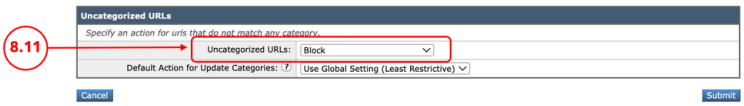
第8.8步：在Cisco Data Security Policies页中，点击新策略的URL Filtering中的链接。

第8.9步(可选)您可以通过点击选择自定义类别(Select Custom Categories)并在类别名称前面选择Include in Policy)来添加任何自定义URL类别

第8.10步：为每个自定义和外部URL类别过滤和预定义URL类别过滤配置操作。

映像 — 非受管设备的上传操作

第8.11步：向下滚动Uncategorized URLs部分选择正确的操作。



图像 — 未分类URL的上传操作

提示：对于安全方面，最好将操作设置为Block，以防任何URL需要访问，您可以将它们添

	加到分配给策略的自定义URL类别中。 第8.12步。单击提交
步骤9.保存更改	步骤9.1.提交更改

相关信息

- 思科安全网络设备AsyncOS 15.0用户指南 — LD（有限部署） — 故障排除……
- 阻止SWA中的可执行文件下载
- 阻止安全Web设备中的上传流量
- 阻止安全网络设备中的流量
- 绕过安全网络设备中的身份验证
- 在SWA中配置Microsoft O365租户限制
- 配置安全Web设备的初始设置
- 绕过安全Web设备中的Microsoft更新流量

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）。