在SWA上配置Microsoft 365租户限制

目录

简介

先决条件

- 要求
- 使用的组件

配置步骤

报告和日志

- 日志
- 报告

相关信息

简介

本文档介绍在安全网络设备(SWA)中配置Microsoft 365租户限制的流程。

先决条件

要求

Cisco 建议您了解以下主题：

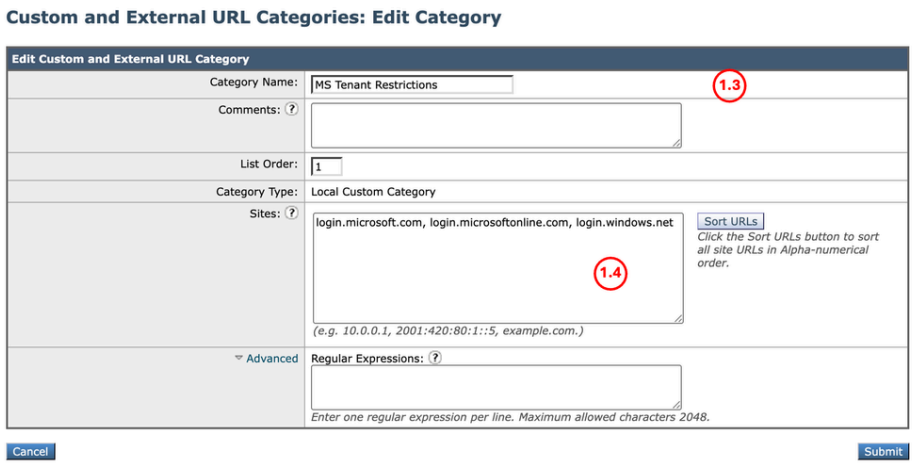
- 访问SWA的图形用户界面(GUI)
- SWA的管理权限。
- 具备SWA管理知识。

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。

配置步骤

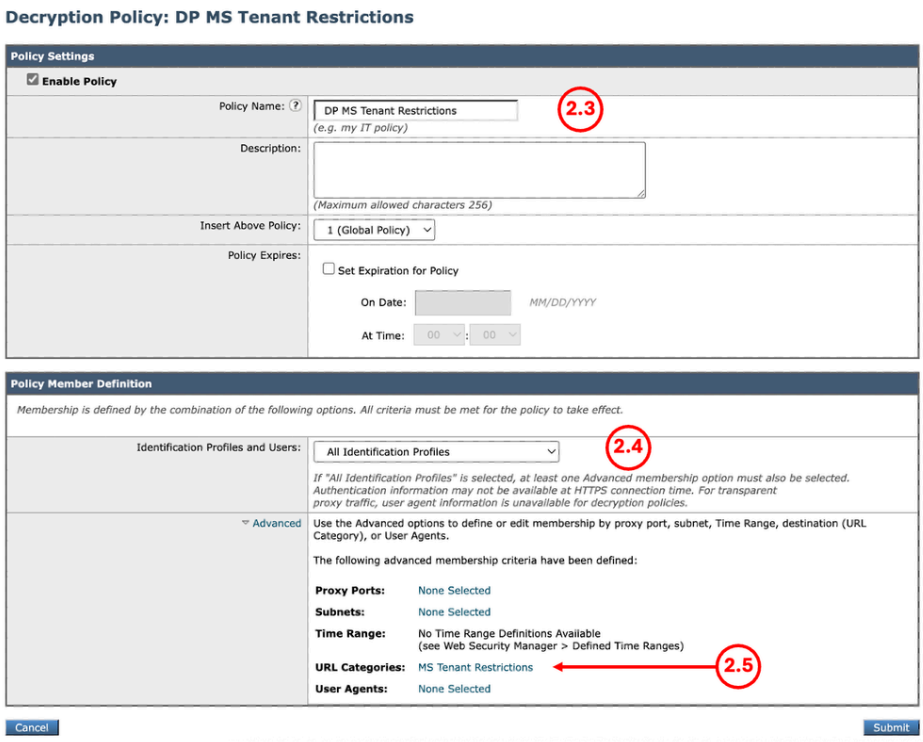
步骤1.为网站创建自定义URL类别。	第1.1步：从GUI导航到Web Security Manager，然后选择Custom and External URL Categories。 步骤1.2.单击Add Category创建新的自定义URL类别。 步骤1.3.为新类别输入Name。 步骤1.4.在站点部分定义以下URL: `login.microsoft.com, login.microsoftonline.com, login.windows.net` 步骤1.5.提交更改。  图像 — 自定义URL类别 提示：有关如何配置自定义URL类别的详细信息，请访问：在安全Web设备中配置自定义URL类别
步骤2.解密流量。	第2.1步：从GUI导航到网络安全管理器，然后选择解密策略。 第2.2步。点击Add Policy。 步骤2.3.输入策略的名称。 第2.4步：选择必须应用到此策略的标识配置文件。 提示：如果绕过Microsoft URL的身份验证，并且要为所有用

户配置此策略，请选择所有标识配置文件>所有用户

第2.5步：从策略成员定义部分，单击URL类别链接以添加自定义URL类别。

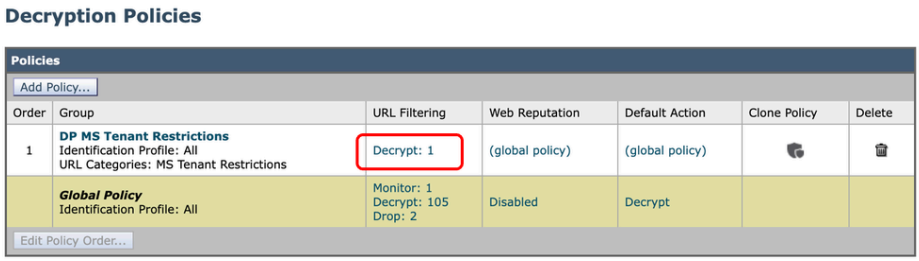
第2.6步：选择在第1步中创建的URL类别。

步骤2.7.单击Submit。



映像 — 配置解密策略

第2.8步：在解密策略页面中，点击在步骤1中创建的URL过滤中的链接。

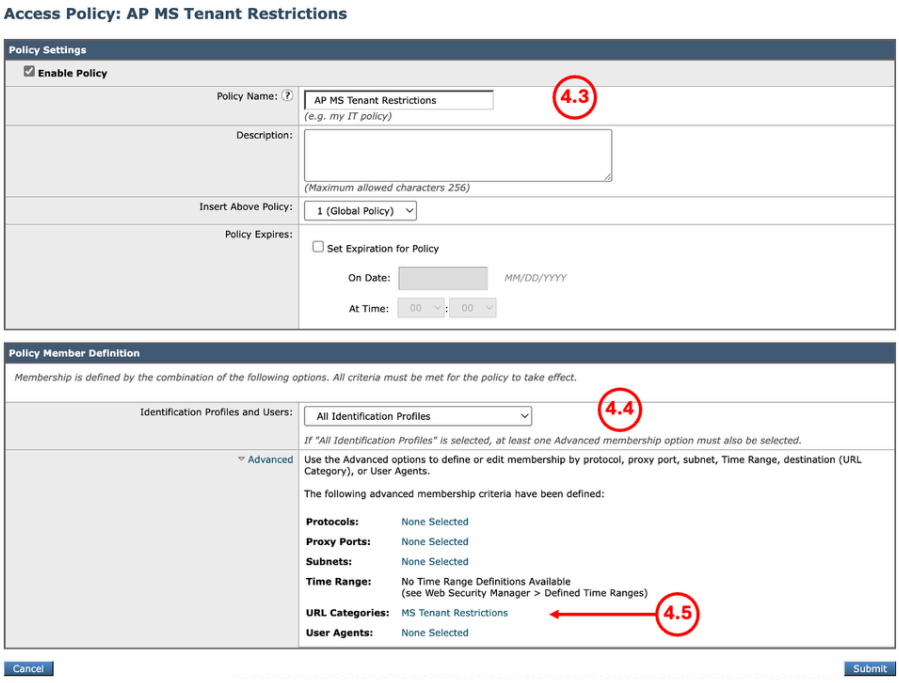


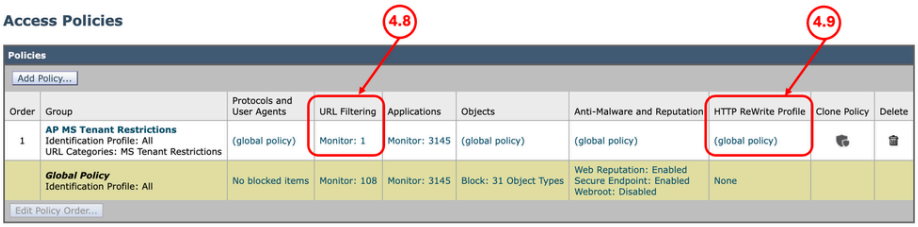
图像 — 编辑URL过滤操作

第2.9步：选择解密作为“自定义URL类别”的操作。

步骤2.10.单击Submit。

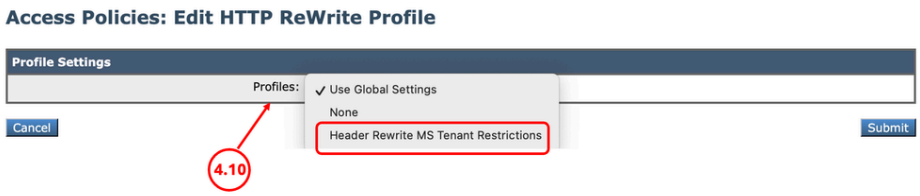
	Decryption Policies: URL Filtering: DP MS Tenant Restrictions **Custom and External URL Category Filtering** *These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.* Override Global Settings Category / Category Type / Use Global Settings / Pass Through / Monitor / Decrypt / Drop / Quota-Based / Time-Based Select all / Select all / Select all / Select all / Select all / (Unavailable) / (Unavailable) MS Tenant Restrictions / Custom (Local) / – / – / – / ✓ / – / – / – Cancel / Submit 图像 — 解密自定义URL类别
步骤3.创建HTTP重写配置文件。	第3.1步：从GUI中，导航到Web Security Manager，然后选择HTTP ReWrite Profiles。 步骤3.2.单击Add Profile。 步骤3.3.输入新配置文件的Name。 步骤3.4.将Restrict-Access-To-Tenants用于第一个报头名称。 第3.5步：对于Restrict-Access-To-Tenants设置，请使用<permitted tenant list>值，该值必须是允许用户访问的租户的逗号分隔列表。 步骤3.6.单击Add Row。 第3.7步。使用Restrict-Access-Context作为第二个报头名称。 第3.8步。对于Restrict-Access-Context设置，请使用单个目录ID的值指定定义租户限制的租户。 步骤3.9.单击Submit。 **HTTP ReWrite: Edit Profile** **Profile Settings** Profile Name: Header Rewrite MS Tenant Restrictions Headers: Header Name / Header Value / Text Format / Binary Encoding / Add Row / Copy Row Restrict-Access-To-Tenants / [redacted]9.onmicrosoft.com / ASCII / No Encoding Restrict-Access-Context / [redacted]2-9505-4097-a69a-c1553ef / ASCII / No Encoding *Note:* *HTTP header variables available for modification: X-Client-IP, X-Authenticated-User, X-Authenticated-Groups* *$ReqMeta can be used to fetch standard HTTP header variables* *Example: If the value of Header is entered as Username-{$ReqMeta[X-Authenticated-User]) and X-Authenticated-User is joesmith, the final Header Value that gets replaced will be Username-joesmith* *$ReqHeader can be used to access values of the standard HTTP headers or values of the other headers defined under this HTTP Header Re-Write Profile.* *Example:* *Header1: Value1;* *Header2: Value0-{$ReqHeader[Header1])-Value2-{$ReqMeta[X-Authenticated-User])* *If X-Authenticated-User is joesmith and Header1 value is Value1 then the value of Header2 will be Value0-Value1-Value2-joesmith* *If value of any header field is empty, that header will be removed from the HTTP header fields and shall not be part of the HTTP header information.* Cancel / Submit 图像 — 添加HTTP重写配置文件 提示：有关租户限制以及如何收集租户信息的详细信息，请访问：Microsoft学习 — 限制对租户的访问

步骤4.创建访问策略。	第4.1步：从GUI导航到网络安全管理器，然后选择访问策略。 步骤4.2.单击Add Policy。 步骤4.3.输入策略的名称。 第4.4步：选择必须应用到此策略的标识配置文件。 提示：如果绕过Microsoft URL的身份验证，并且要为所有用户配置此策略，请选择：所有标识配置文件>所有用户。 第4.5步：从策略成员定义部分，单击URL类别链接以添加自定义URL类别。 第4.6步：选择在步骤1中创建的URL类别。 步骤4.7.单击Submit。  映像 — 创建访问策略 第4.8步：在访问策略页中，确保URL过滤的操作设置为监控。 第4.9步：点击HTTP重写配置文件中的链接，将HTTP报头配置文件添加到该策略。



映像 — 访问策略属性

第4.10步：选择在步骤3中创建的HTTP重写配置文件。



图像 — 添加HTTP重写配置文件

步骤4.11.单击Submit。

步骤4.12.提交更改。

报告和日志

日志

您可以将自定义字段添加到访问日志或W3C日志，以查看HTTP报头重写配置文件名称。

访问日志中的格式说明符	W3C日志中的日志字段	描述
%]	x-http-rewrite-profile-name	HTTP报头重写配置文件名称。

报告

您可以生成网络跟踪报告，以便按访问策略名称查看流量报告。

使用以下步骤生成报告：

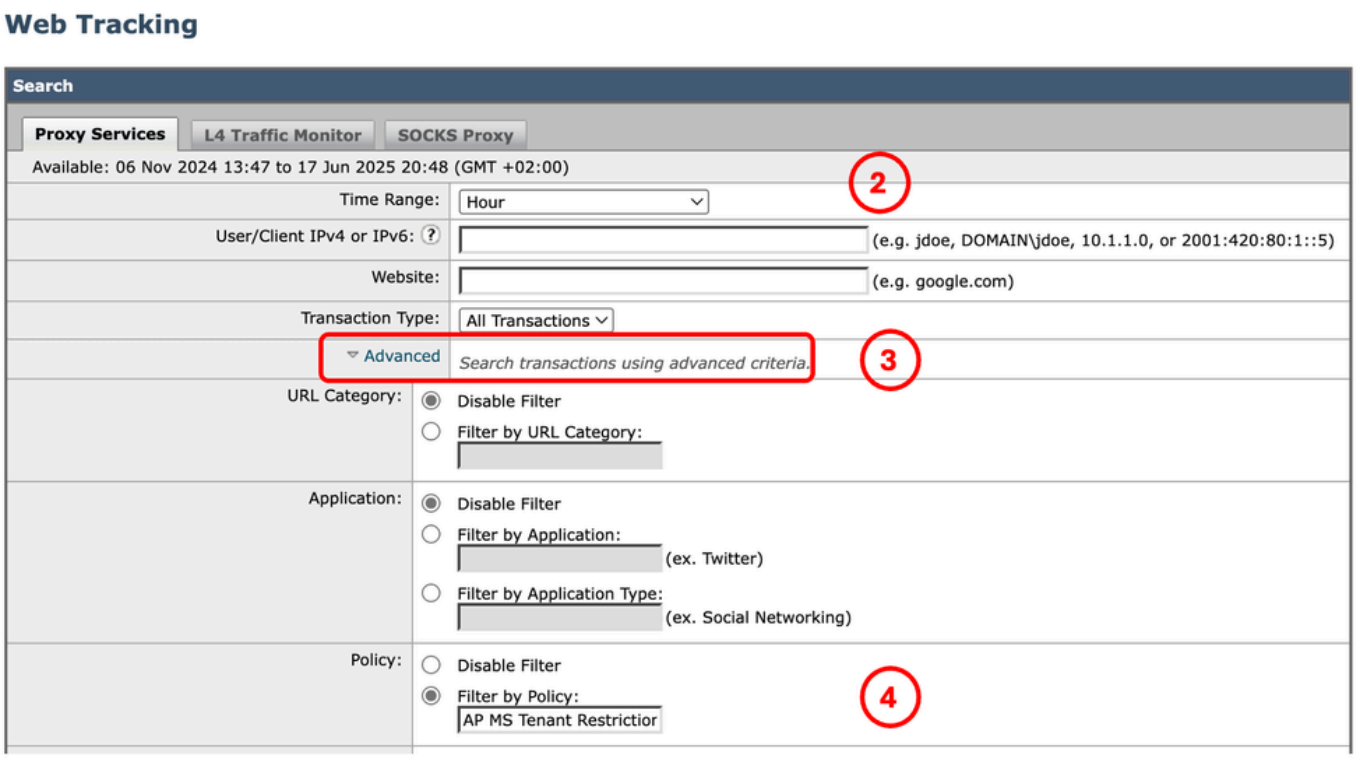
步骤1.从GUI中选择Reporting，然后选择Web Tracking。

步骤2.选择所需的时间范围。

步骤3.单击Advanced链接以使用高级条件搜索事务处理。

第4步：在Policy部分，选择Filter by Policy，并键入之前创建的Access Policy的名称。

步骤5.单击Search查看报告。



图像 — Web跟踪报告

相关信息

- 思科安全Web设备AsyncOS 15.2用户指南
- 思科安全邮件和Web虚拟设备安装指南
- 在安全Web设备中配置自定义URL类别 — 思科
- 使用安全Web设备最佳实践
- 为安全Web设备配置防火墙
- 在安全Web设备中配置解密证书
- 在SWA中配置并排除SNMP故障
- 在带有Microsoft服务器的安全Web设备中配置SCP推送日志
- 在SWA中启用特定YouTube频道/视频并阻止YouTube的其余部分
- 了解安全Web设备中的HTTPS访问日志格式

- 访问安全Web设备日志
- 绕过安全网络设备中的身份验证
- 阻止安全网络设备中的流量
- 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）。