在安全访问中通过DLP阻止TXT上传

目录

简介

本文档介绍在带有DLP的思科安全访问中阻止.TXT文件上传的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全访问管理。
- 防数据丢失(DLP)。

Cisco 建议您：

- 对思科安全访问的管理访问。

使用的组件

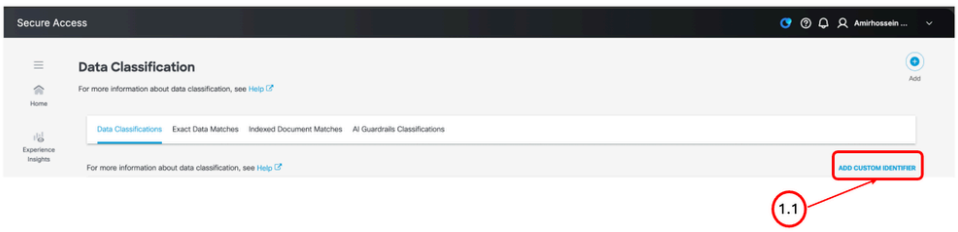
本文档不限于特定的软件和硬件版本。

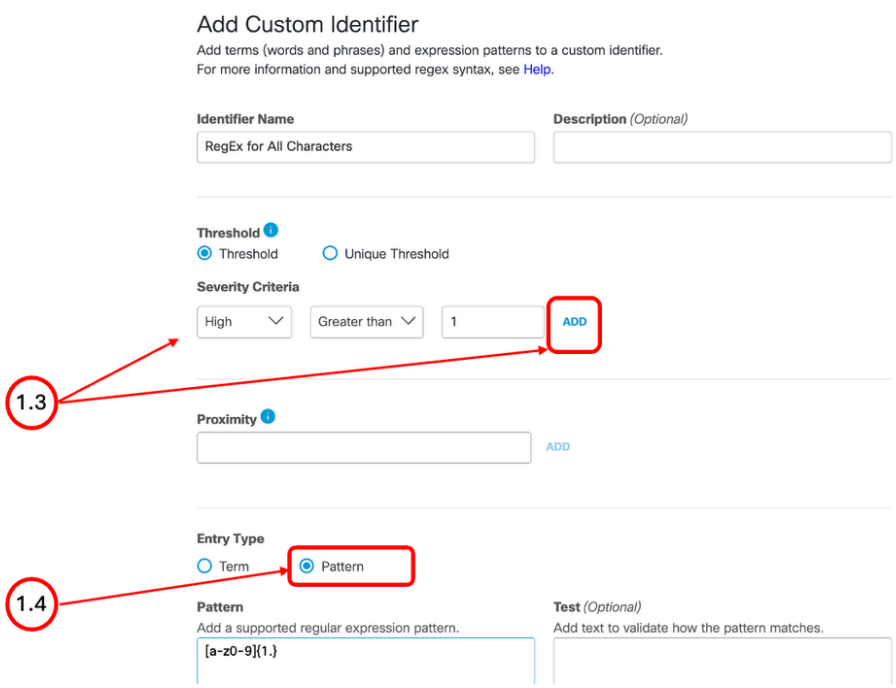
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

开始使用前

1. 请谨慎使用这些步骤，因为它们会为DLP进程增加额外负载并可能导致性能降低。在TXT文件阻止可用之前，您可以参考此链接了解当前支持的文件类型：思科安全访问 — 支持的文件类型
2. 本文包括可用作引用的正则表达式示例。在使用任何示例之前，请确保您完全了解匹配条件和它们用于识别的模式。如果需要，您还可以创建自己的正则表达式。在所有情况下，请仔细验证表达式，以确保它正确覆盖了所有的预期匹配条件和可能的变体。
3. 确保在应用DLP策略之前解密流量。DLP检测需要访问已解密的内容；无法扫描加密流量以查找DLP匹配项。

配置步骤

分类	步骤
步骤1.创建数据分类	第1.1步：从Cisco Secure Access管理门户，导航到Secure > Data Classification，然后点击Add Custom Identifier。  图像 — 创建新的自定义标识符 步骤1.2.定义新标识符的名称 第1.3步：从Threshold部分配置Severity Criteria并点击Add。 步骤1.4.分别定义每个正则表达式，然后点击添加。 提示：本文中提供的正则表达式仅是示例。使用它们之前，请验证该表达式是否正确包含所有所需的匹配条件和可能的变体。

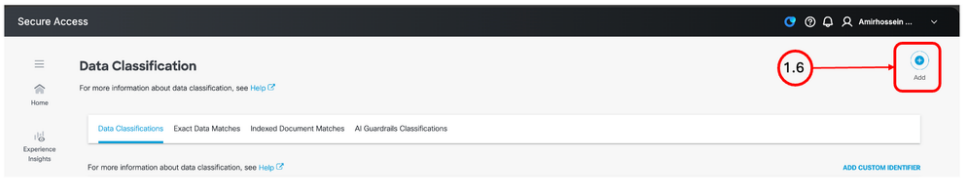


图像 — 添加自定义标识符

注意：如果正则表达式超过10个，则需要使用相同的步骤创建另一个自定义标识符。

第1.5步。单击保存。

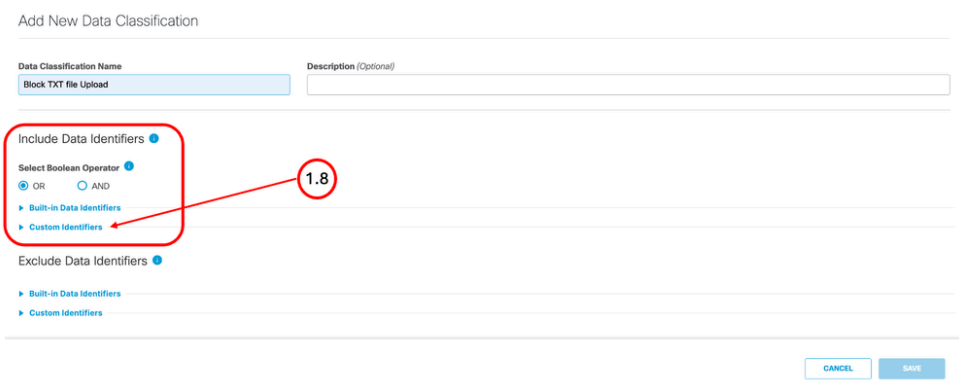
步骤1.6.单击Add图标以创建新的数据分类



图像 — 创建新数据分类

步骤1.7.定义名称。

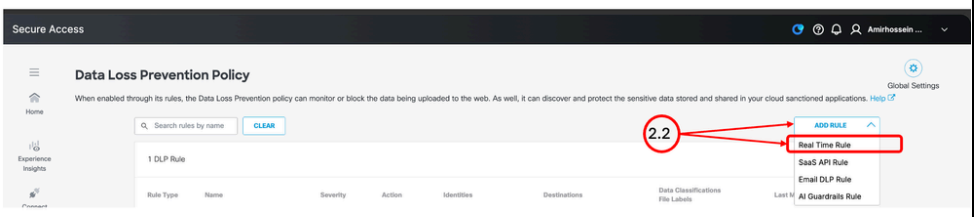
第1.8步：从Include Data Identifiers部分点击Custom Identifier，然后选择您在前面的步骤中创建的标识符。

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


图像 — 配置数据分类

步骤1.9.单击保存。
</td>
</tr>
<tr>
<td>步骤2.配置DLP策略</td>
<td>
第2.1步：从思科安全访问管理门户，导航到安全>数据丢失保护策略

第2.2步：点击Add Rule，然后选择Real Time Rule。



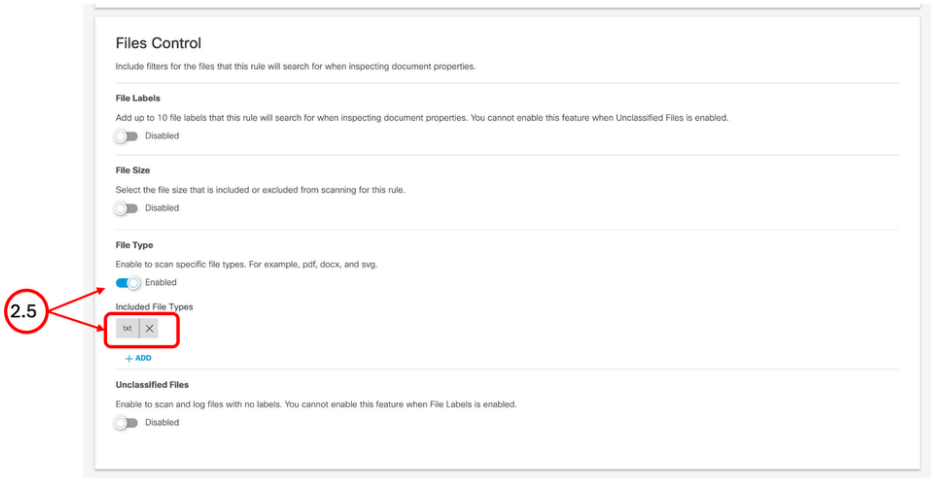
映像 — 创建新的实时DLP策略

步骤2.3.定义策略名称。

第2.4步：从Data Classifications部分，选择您在第1步中创建的Data Classification。

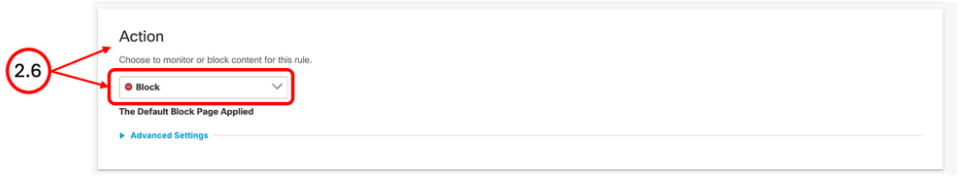
注意：最多允许5分钟时间将新创建的数据分类显示在DLP策略列表中。

步骤2.5.从Files Control部分，启用File Type并选择TXT。
</td>
</tr>
</table>



映像 — 配置文件类型

第2.6步：从Action部分，选择Block。



图像 — 将操作设置为阻止

步骤2.7.保存更改。

监控

要检查DLP活动及相关日志，请转到监控>防数据丢失。使用可用的过滤器缩小结果范围并确定相关的DLP事件。

正则表达式示例

匹配日语平假名、片假名和汉字字符：

```
[ぁ-けァ-ヲー-□]{1,}
```

匹配大写拉丁字母：

```
[A-Z]{1,}
```

匹配小写拉丁字母和数字：

```
[a-z0-9]{1,}
```

匹配常见标点符号：

```
[.,;:!?]
```

匹配单引号、双引号和回溯：

```
['"`]
```

匹配圆括号、方括号和花括号：

```
[()\[\]{}]
```

匹配通用符号和特殊字符：

```
[@#$%^&*+=|\\/_~-]
```

匹配À-Unicode范围内的拉ÿ丁字符：

```
[À-ÿ]
```

匹配西里尔字符：

```
[È-ж]
```

匹配希腊语和科普特字符：

[ㅏ-ㅢ]

匹配阿拉伯文字字符：

[ـ-ۏ]

匹配CJK统一象形文字：

[丄-□]

将选定的波兰字符与变音符匹配：

[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]

匹配朝鲜语韩文音节：

[가-힣]

相关信息

思科安全访问支持DLP的文件类型的完整列表：https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Cisco Secure Access DLP支持的文件类型 — Cisco Community:https://community.cisco.com/t5/security-knowledge-base/cisco-secure-access-complete-list-of-dlp-supported-file-types/ta-p/5274268

思科安全访问DLP配置和策略参考：https://securitydocs.cisco.com/docs/csa/olh/161419.dita

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）。