在安全訪問中阻止通過DLP上傳TXT

目錄

簡介

本檔案介紹在使用DLP的Cisco安全存取中阻止.TXT檔案上傳的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全存取管理。
- 防資料丟失(DLP)。

思科建議您：

- 對思科安全訪問的管理訪問。

採用元件

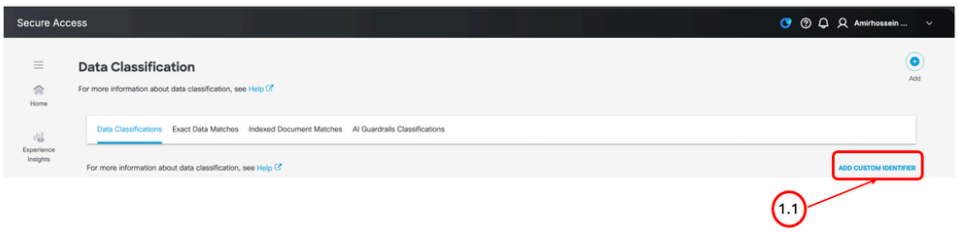
本文件所述內容不限於特定軟體和硬體版本。

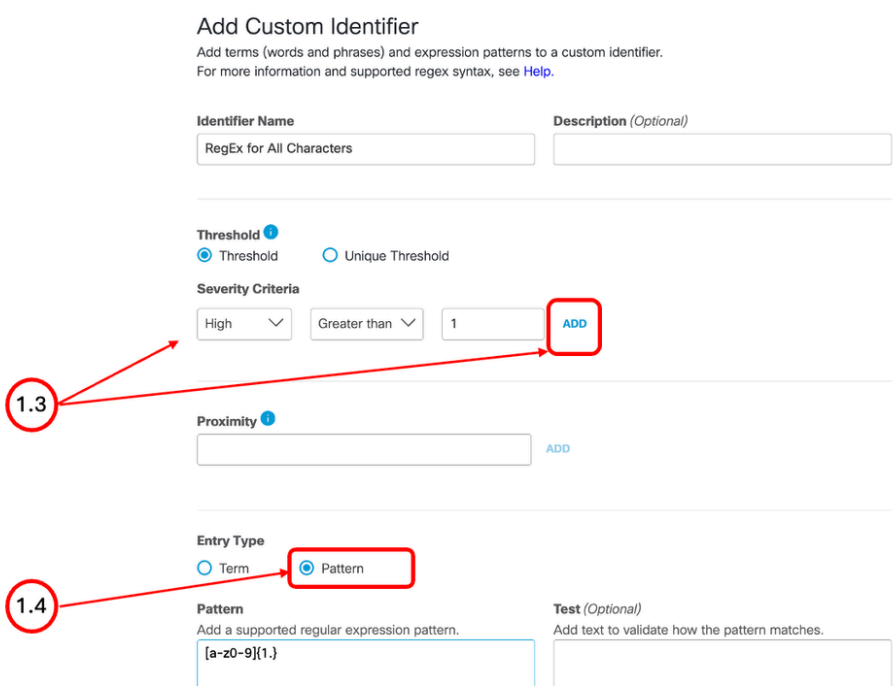
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

開始之前

1. 請謹慎使用這些步驟，因為它們會為DLP進程增加額外負載並可能導致效能降低。在TXT檔案阻止可用之前，您可以參考此連結瞭解當前支援的檔案型別：Cisco Secure Access — 支援的檔案型別
2. 本文包括可用作引用的正規表示式示例。使用任何示例之前，請確保您完全瞭解匹配條件以及它們旨在識別的模式。如果需要，還可以建立自己的正規表示式。在所有情況下，請仔細驗證表達式，以確保其正確包含了所有預期的匹配條件和可能的變化。
3. 確保在應用DLP策略之前解密流量。DLP檢測要求訪問已解密的內容；無法掃描加密流量以查詢DLP匹配項。

設定步驟

類別	步驟
步驟1.建立資料分類	步驟1.1.從Cisco Secure Access管理門戶導航到Secure > Data Classification，然後點選Add Custom Identifier。  影象 — 建立新的自定義識別符號 步驟1.2.定義新識別符號的名稱 步驟1.3.從Threshold部分配置Severity Criteria，然後按一下Add。 步驟1.4.單獨定義每個正規表示式，然後按一下Add。 提示：本文中提供的正規表示式僅是示例。使用它們之前，請驗證表達式是否正確包含了所有必需的匹配條件和可能的變體。

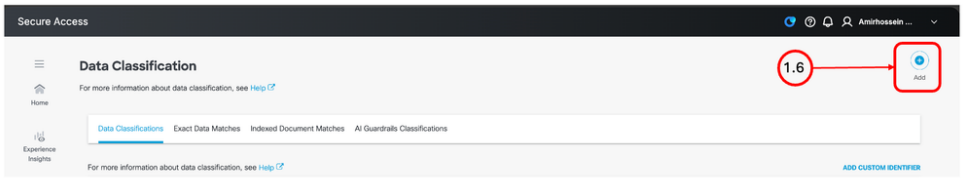


影象 — 新增自定義識別符號

附註：如果正規表示式超過10個，則需要使用相同的步驟建立另一個自定義識別符號。

步驟1.5.按一下Save。

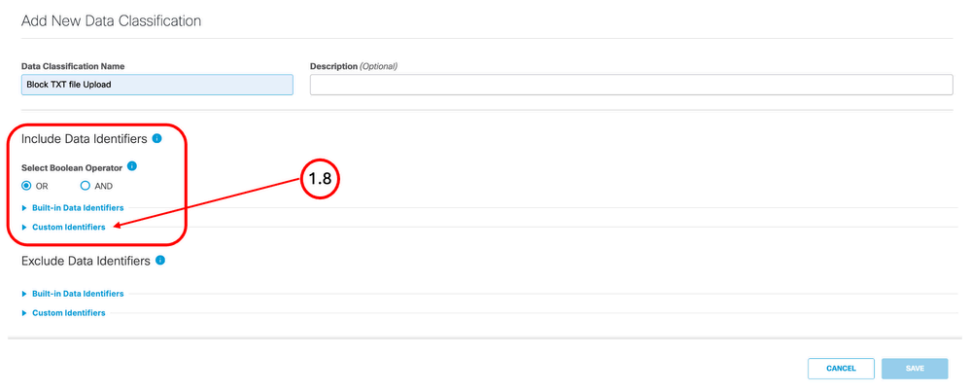
步驟1.6.單擊Add圖標以建立新的資料分類



影象 — 建立新資料分類

步驟1.7.定義名稱。

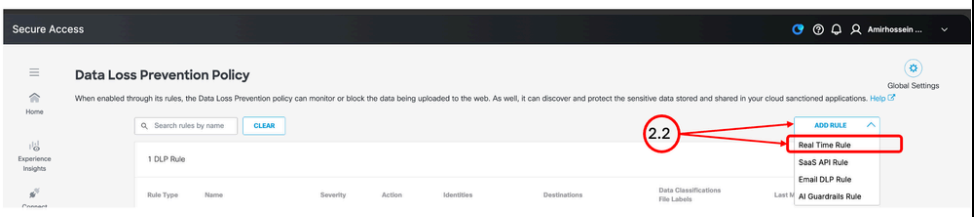
步驟1.8.從包含資料識別符號部分，按一下自定義識別符號，然後選擇您在前面的步驟中建立的識別符號。

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

影象 — 配置資料分類

步驟1.9.按一下Save。</td>
</tr>
<tr>
<td>步驟2.配置DLP策略</td>
<td>步驟2.1.從思科安全訪問管理門戶導航到安全>資料丟失防護策略

步驟2.2.單擊Add Rule並選擇Real Time Rule。

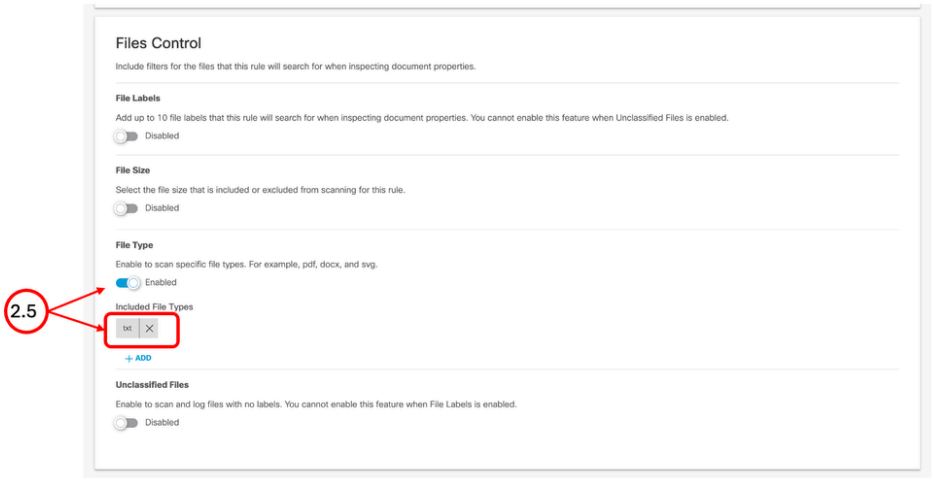
影象 — 建立新的即時DLP策略

步驟2.3.定義策略名稱。

步驟2.4.從Data Classifications部分，選擇在步驟1中建立的Data Classification。

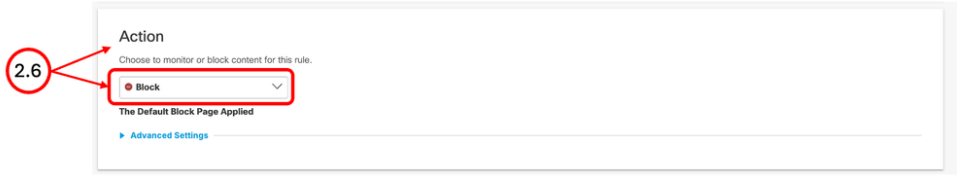
附註：最多允許5分鐘時間讓新建立的資料分類出現在DLP策略清單中。

步驟2.5.從Files Control部分啟用File Type並選擇TXT。</td>
</tr>
</table>



影象 — 配置檔案型別

步驟2.6.從Action部分中選擇Block。



影象 — 將操作設定為「阻止」

步驟2.7. 儲存變更。

監控

要檢查DLP活動及相關日誌，請轉至監控>資料丟失防護。使用可用的過濾器縮小結果範圍，識別相關的DLP事件。

正規表示式示例

匹配日文平假名、片假名和漢字字元：

```
[ぁ-□ァ-ヂー-□]{1,}
```

匹配大寫拉丁字母：

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

匹配小寫拉丁字母和數字：

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

匹配常見標點符號：

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

匹配單引號、雙引號和回溯：

```
['"`]
```

匹配括弧、方括弧和花括弧：

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

匹配通用符號和特殊字元：

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

匹配À-Unicode範圍內的拉丁文ÿ字元：

```
[À-ÿ]
```

匹配西里爾字元：

```
[È-⁎]
```

匹配希臘語和科普特語字元：

```
[ㅏ-ㅢ]
```

匹配阿拉伯文字字元：

```
[ـ-ۓ]
```

匹配CJK統一表意文字：

```
[丄-□]
```

將選定的波蘭字元與變音符匹配：

```
[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]
```

匹配朝鮮語韓文音節：

```
[가-힣]
```

相關資訊

思科安全訪問支援DLP的檔案型別的完整清單：https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Cisco Secure Access DLP支援的檔案型別 — Cisco社群：https://community.cisco.com/t5/security-knowledge-base/cisco-secure-access-complete-list-of-dlp-supported-file-types/ta-p/5274268

Cisco Secure Access DLP配置和策略參考：https://securitydocs.cisco.com/docs/csa/olh/161419.dita

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。