Block TXT Upload via DLP in Secure Access

Contents

Introduction

This document describes the steps to block .**TXT** file upload in Cisco Secure Access with DLP.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Access administration.
- Data Loss Prevention (DLP).

Cisco recommends that you have:

- Administrative Access to Cisco Secure Access.

Components Used

This document is not restricted to specific software and hardware versions.

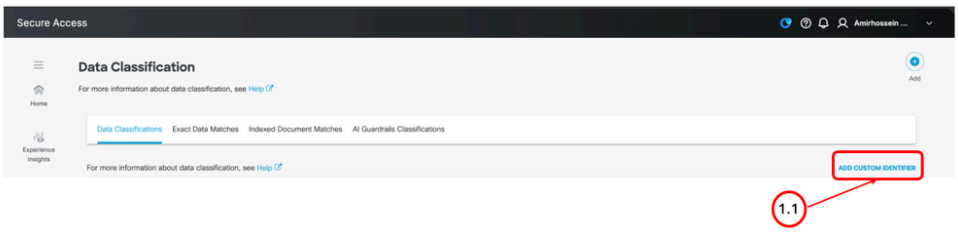
The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Before you Begin

1. Please use these steps with caution, as they add extra load to the DLP process and can cause performance degradation. Until TXT file blocking is available, you can refer to this link for the currently supported file types: Cisco Secure Access – Supported File Types
2. This article includes sample regular expressions that can be used as a reference. Before using any of the examples, ensure that you fully understand the matching conditions and the patterns they are designed to identify. You can also create your own regular expressions when required. In all cases, carefully validate the expression to ensure that it correctly covers all intended matching conditions and possible variations.
3. Ensure that the traffic is decrypted before applying DLP policies. DLP inspection requires access to the decrypted content; encrypted traffic cannot be scanned for DLP matches.

Configuration Steps

Category	Steps
Step 1. Create Data Classification	**Step 1.1.** From the Cisco Secure Access management portal, navigate to **Secure** > **Data Classification** and click the **Add Custom Identifier**.  *Image - Create a New Custom Identifier* **Step 1.2.** Define a name for the new Identifier **Step 1.3.** From the **Threshold** section configure **Severity Criteria** and click **Add**. **Step 1.4.** Define each Regular Expressions separately and click **Add.** **Tip**: The regular expressions provided in this article are examples only. Before using them, verify that the expression correctly covers all required matching conditions and possible variations.

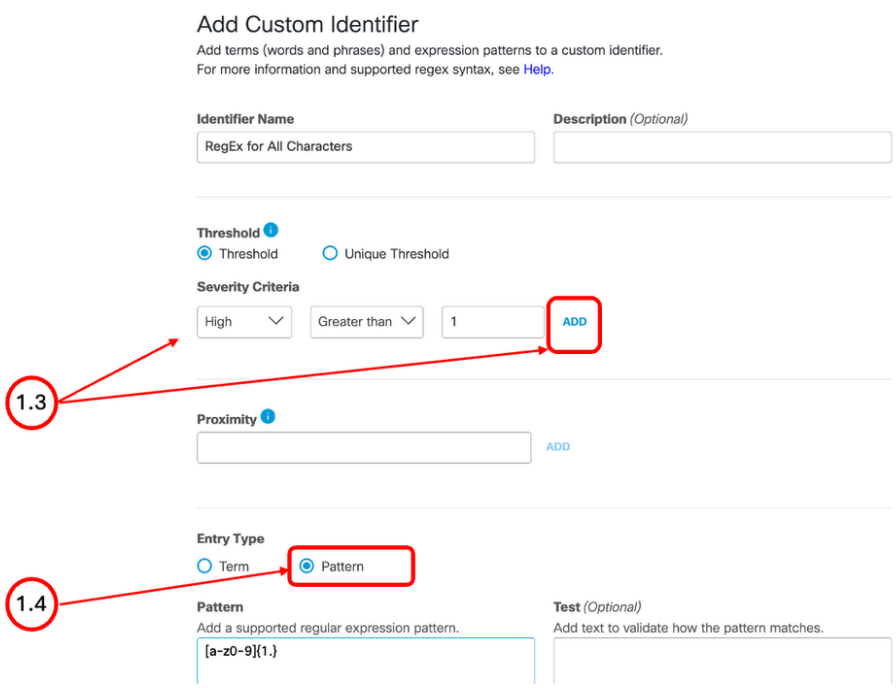


Image - Add Custom Identifier

Note: If there are more than 10 Regular Expressions, you need to use the same steps to create another Custom Identifier.

Step 1.5. Click **Save**.

Step 1.6. Click the **Add** icon to create a new Data Classification

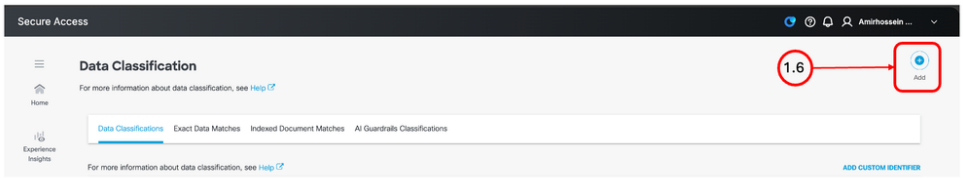


Image - Create a New Data Classification

Step 1.7. Define a **Name**.

Step 1.8. From **Include Data Identifiers** section click on **Custom Identifier** and choose the Identifier(s) that you created in previous steps.

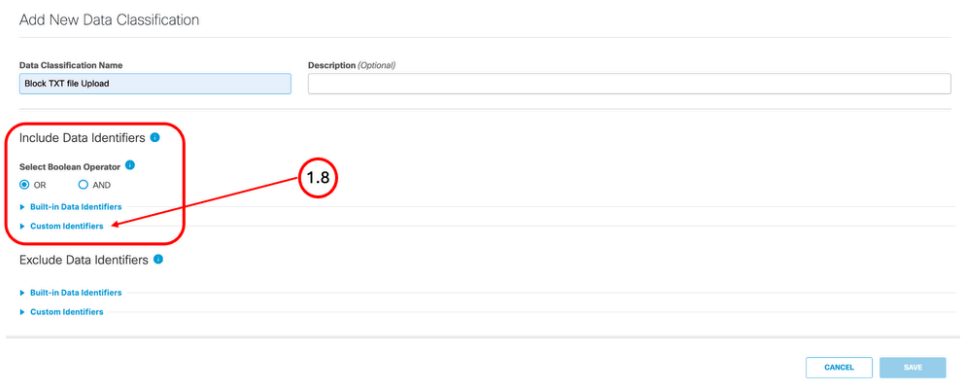


Image - Configure the Data Classification

Step 1.9. Click **Save**.

Step 2. Configure the DLP Policy

Step 2.1. From the Cisco Secure Access management portal, navigate to **Secure > Data Loss Prevention Policy**

Step 2.2. Click **Add Rule** and select **Real Time Rule.**

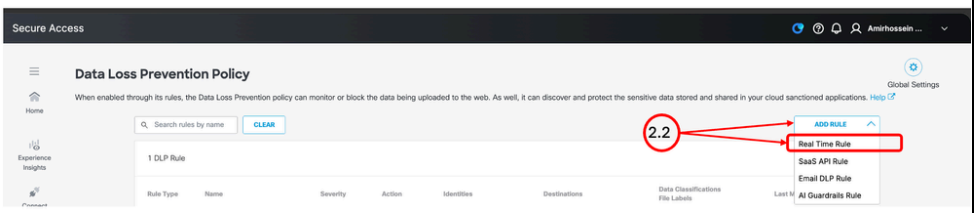


Image - Create a New Real Time DLP Policy

Step 2.3. Define the Policy **Name**.

Step 2.4. From the **Data Classifications** section, select the Data Classification that you created on **Step 1**.

Note: Allow up to 5 minutes for newly created data classifications to appear in the DLP policy list.

Step 2.5. From the **Files Control** section, enable the **File Type** and select **TXT**.

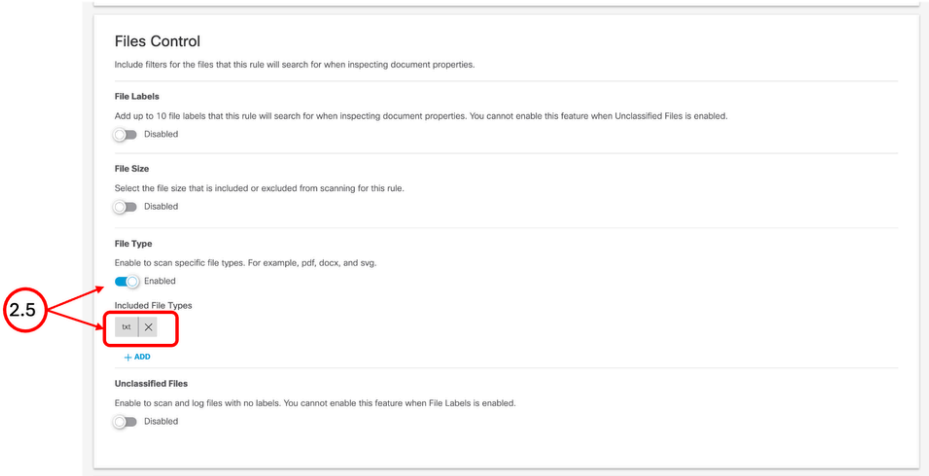


Image - Configure File Type

Step 2.6. From the **Action** section, choose **Block**.

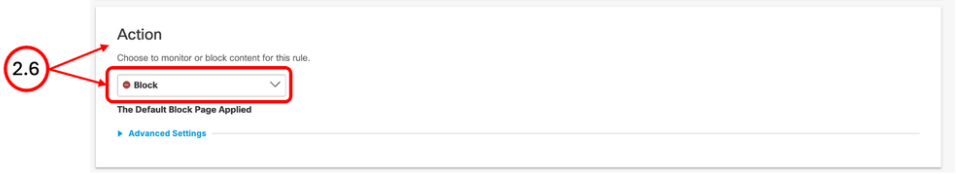


	Image - Set the Action to Block **Step 2.7**. **Save** the changes.

Monitoring

To check DLP activity and related logs, go to **Monitor > Data Loss Prevention**. Use the available filters to narrow the results and identify the relevant DLP events.

Sample Regular Expressions

Matches Japanese Hiragana, Katakana, and Kanji characters:

```
[ぁ-けァ-ヲー-□]{1,}
```

Matches uppercase Latin letters:

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

Matches lowercase Latin letters and digits:

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

Matches common punctuation characters:

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

Matches single quotes, double quotes, and backticks:

```
['"`]
```

Matches parentheses, square brackets, and curly brackets:

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

Matches common symbols and special characters:

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

Matches Latin characters in the À-ÿ Unicode range:

```
[À-ÿ]
```

Matches Cyrillic characters:

```
[È-ж]
```

Matches Greek and Coptic characters:

```
[Ͱ-ͻ]
```

Matches Arabic-script characters:

```
[-ۿ]
```

Matches CJK Unified Ideographs:

```
[丄-□]
```

Matches selected Polish characters with diacritics:

```
[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]
```

Matches Korean Hangul syllables:

[가-힣]

Related Information

Cisco Secure Access complete list of DLP-supported file types:
https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Cisco Secure Access DLP-supported file types — Cisco Community:
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 configuration and policy reference:
https://securitydocs.cisco.com/docs/csa/olh/161419.dita