# Bloquer le téléchargement TXT via DLP dans Secure Access

## Table des matières



## Introduction

Ce document décrit les étapes à suivre pour bloquer le téléchargement de fichiers .TXT dans Cisco Secure Access avec DLP.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration de Cisco Secure Access.
- Prévention des pertes de données (DLP).

Cisco vous recommande d'avoir :

- Accès administratif à Cisco Secure Access.

### Composants utilisés

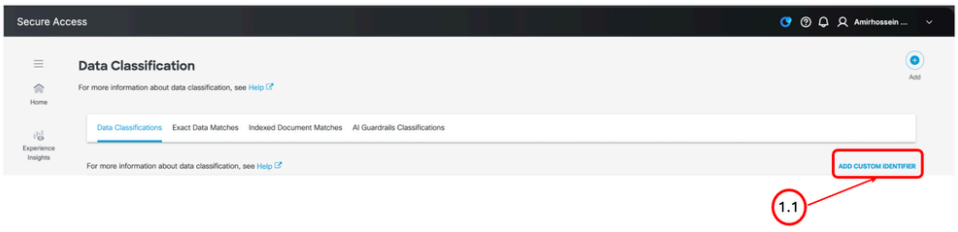
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Avant de commencer

1. Veuillez utiliser ces étapes avec prudence, car elles ajoutent une charge supplémentaire au processus DLP et peuvent entraîner une dégradation des performances. Tant que le blocage des fichiers TXT n'est pas disponible, vous pouvez consulter ce lien pour connaître les types de fichiers actuellement pris en charge : Accès sécurisé Cisco - Types de fichiers pris en charge
2. Cet article inclut des exemples d'expressions régulières qui peuvent être utilisées comme référence. Avant d'utiliser l'un des exemples, assurez-vous de bien comprendre les conditions de correspondance et les modèles qu'elles sont conçues pour identifier. Vous pouvez également créer vos propres expressions régulières si nécessaire. Dans tous les cas, validez soigneusement l'expression pour vous assurer qu'elle couvre correctement toutes les conditions de correspondance prévues et les variations possibles.
3. Assurez-vous que le trafic est déchiffré avant d'appliquer les stratégies DLP. L'inspection DLP nécessite l'accès au contenu décrypté ; Le trafic chiffré ne peut pas être analysé pour les correspondances DLP.

## Configuration Steps

| Catégorie | Étapes |
|---|---|
| Étape 1. Créer une classification des données | Étape 1.1. À partir du portail de gestion Cisco Secure Access, accédez à Secure > Data Classification et cliquez sur Add Custom Identifier.<br>  <br>Image - Créer un nouvel identificateur personnalisé<br>Étape 1.2. Définir un nom pour le nouvel identificateur |

Étape 1.3. Dans la section Threshold (Seuil), configurez Severity Criteria (Critères de gravité) et cliquez sur Add.

Étape 1.4. Définissez chaque expression régulière séparément et cliquez sur Ajouter.

Conseil : les expressions régulières fournies dans cet article ne sont que des exemples. Avant de les utiliser, vérifiez que l'expression couvre correctement toutes les conditions de correspondance requises et les variations possibles.

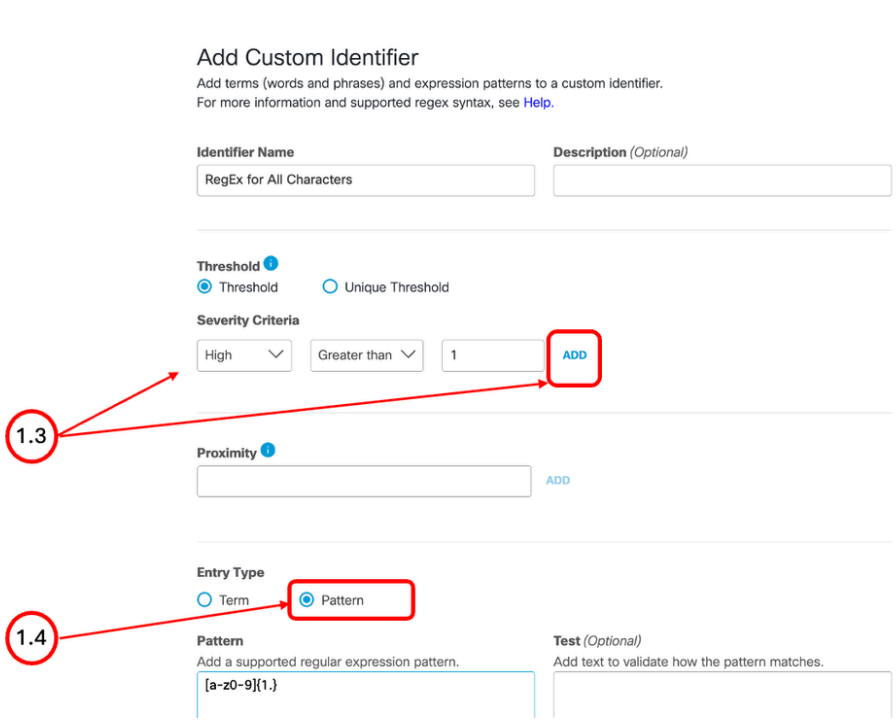



Image - Ajouter un identificateur personnalisé

Remarque : S'il existe plus de 10 expressions régulières, vous devez suivre les mêmes étapes pour créer un autre identificateur personnalisé.

Étape 1.5. Cliquez sur Save.

Étape 1.6. Cliquez sur l'icône Ajouter pour créer une classification des données

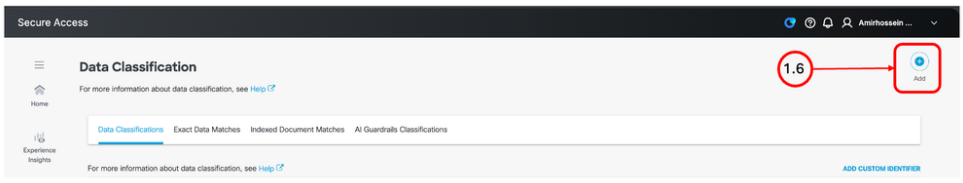
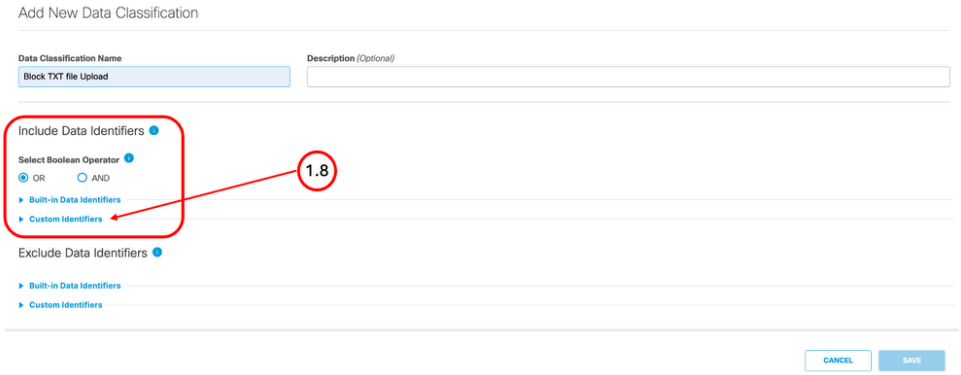
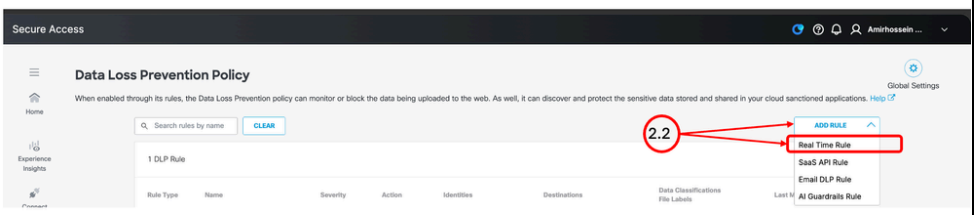



Image - Créer une nouvelle classification des données

| | |
|---|---|
| | Étape 1.7. Définissez un nom.<br><br>Étape 1.8. Dans la section Inclure les identificateurs de données, cliquez sur Identificateur personnalisé et choisissez le ou les identificateurs que vous avez créés dans les étapes précédentes.<br><br>  <br>Image : configuration de la classification des données<br><br>Étape 1.9. Cliquez sur Save. |
| Étape 2 : configuration de la stratégie DLP | Étape 2.1. À partir du portail de gestion Cisco Secure Access, accédez à Secure > Data Loss Prevention Policy<br><br>Étape 2.2. Cliquez sur Add Rule et sélectionnez Real Time Rule.<br><br>  <br>Image - Créer une nouvelle stratégie DLP en temps réel<br><br>Étape 2.3. Définissez le nom de la stratégie.<br><br>Étape 2.4. Dans la section Classification des données, sélectionnez la classification des données que vous avez créée à l'étape 1.<br><br>Remarque : Attendez jusqu'à 5 minutes que les classifications de données nouvellement créées apparaissent dans la liste des stratégies DLP.<br><br>Étape 2.5. Dans la section Contrôle des fichiers, activez le type de fichier et sélectionnez TXT. |

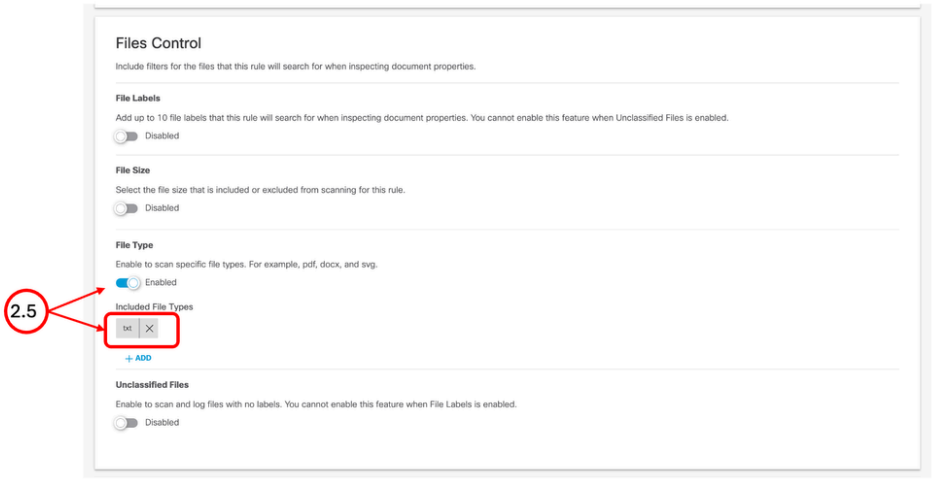



Image - Configurer le type de fichier

Étape 2.6. Dans la section Action, sélectionnez Block.

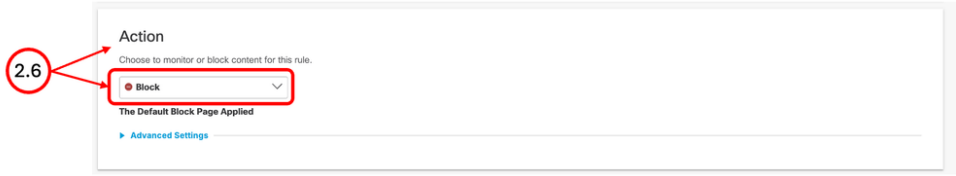



Image - Définir l'action sur Bloquer

Étape 2.7. Enregistrer les modifications

# Surveillance

Pour vérifier l'activité DLP et les journaux associés, accédez à Monitor > Data Loss Prevention. Utilisez les filtres disponibles pour affiner les résultats et identifier les événements DLP pertinents.

## Exemples d'expressions régulières

Correspond aux caractères japonais Hiragana, Katakana et Kanji :

```
[ぁ-けァ-ヲー-□]{1,}
```

Correspond aux lettres latines en majuscules :

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

Correspond aux lettres et chiffres latins minuscules :

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

Correspond aux caractères de ponctuation courants :

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

Correspond aux guillemets simples, aux guillemets doubles et aux backticks :

```
['"`]
```

Correspond aux parenthèses, crochets et accolades :

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

Correspond aux symboles courants et aux caractères spéciaux :

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

Correspond aux caractères latins de la plage Unicode À-ÿ :

```
[À-ÿ]
```

Correspond aux caractères cyrilliques :

```
[È-ж]
```

Correspond aux caractères grecs et coptes :

```
[ㅏ-ㅢ]
```

Correspond aux caractères arabes :

```
[ء-ۿ]
```

Correspond à Idéogrammes unifiés CJC :

```
[丠-龻]
```

Fait correspondre les caractères polonais sélectionnés avec des signes diacritiques :

```
[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]
```

Correspond aux syllabes coréennes du hangûl :

```
[가-힣]
```

# Informations connexes

Cisco Secure Access fournit la liste complète des types de fichiers pris en charge par DLP : https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Types de fichiers pris en charge par Cisco Secure Access DLP — Communauté Cisco : https://community.cisco.com/t5/security-knowledge-base/cisco-secure-access-complete-list-of-dlp-supported-file-types/ta-p/5274268

Référence des politiques et de la configuration DLP Cisco Secure Access : https://securitydocs.cisco.com/docs/csa/olh/161419.dita

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.