# Blocca caricamento TXT tramite DLP in accesso sicuro

## Sommario



## Introduzione

In questo documento viene descritto come bloccare il caricamento di file .TXT in Cisco Secure Access con DLP.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione di Cisco Secure Access.
- Prevenzione della perdita dei dati (DLP).

Cisco raccomanda:

- Accesso amministrativo a Cisco Secure Access.

### Componenti usati

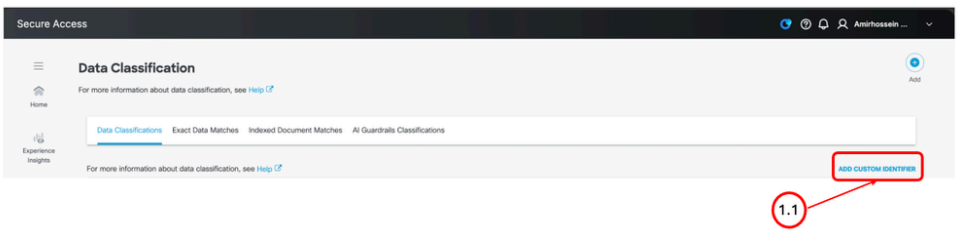
Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Operazioni preliminari

1. Attenersi alla procedura descritta di seguito con cautela, in quanto aggiunge un carico aggiuntivo al processo di prevenzione della perdita dei dati e può causare una riduzione delle prestazioni. Finché non sarà disponibile il blocco dei file TXT, è possibile fare riferimento a questo collegamento per i tipi di file attualmente supportati: Cisco Secure Access - Tipi di file supportati
2. In questo articolo sono incluse espressioni regolari di esempio che possono essere utilizzate come riferimento. Prima di utilizzare uno degli esempi, accertatevi di aver compreso appieno le condizioni di corrispondenza e i modelli che sono stati progettati per identificare. Se necessario, potete anche creare espressioni regolari personalizzate. In tutti i casi, convalidare con attenzione l'espressione per assicurarsi che copra correttamente tutte le condizioni di corrispondenza previste e le possibili variazioni.
3. Prima di applicare i criteri di prevenzione della perdita dei dati, verificare che il traffico sia decrittografato. L'ispezione DLP richiede l'accesso al contenuto decriptato; non è possibile analizzare il traffico crittografato per trovare le corrispondenze DLP.

## Procedura di configurazione

| Categoria | Passi |
|---|---|
| Passaggio 1. Creazione della classificazione dei dati | Passaggio 1.1. Dal portale di gestione di Cisco Secure Access, passare a Secure > Data Classification e fare clic su Add Custom Identifier.<br>  <br>Immagine - Crea un nuovo identificatore personalizzato<br>Passaggio 1.2. Assegnare un nome al nuovo identificatore |

Passaggio 1.3. Dalla sezione Soglia configurare i criteri di gravità e fare clic su Aggiungi.

Passaggio 1.4. Definire ciascuna espressione regolare separatamente e fare clic su Aggiungi.

Suggerimento: le espressioni regolari fornite in questo articolo sono solo esempi. Prima di utilizzarle, verificare che l'espressione copra correttamente tutte le condizioni di corrispondenza richieste e le possibili variazioni.

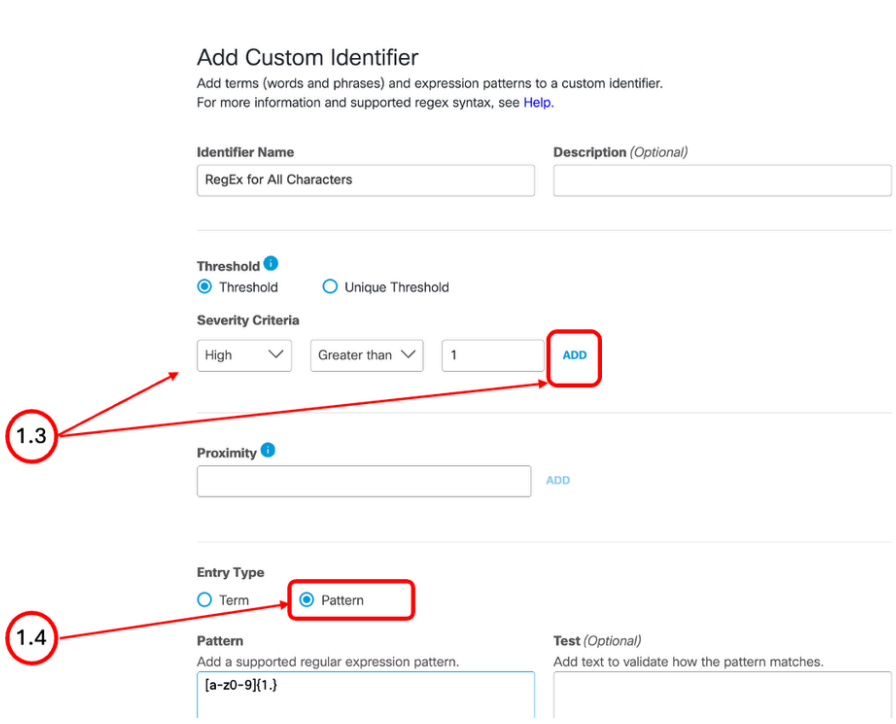



Immagine - Aggiungi identificatore personalizzato

Nota: Se sono presenti più di 10 espressioni regolari, è necessario utilizzare gli stessi passaggi per creare un altro identificatore personalizzato.

Passaggio 1.5. Fare clic su Save (Salva).

Passaggio 1.6. Fare clic sull'icona Aggiungi per creare una nuova classificazione dei dati

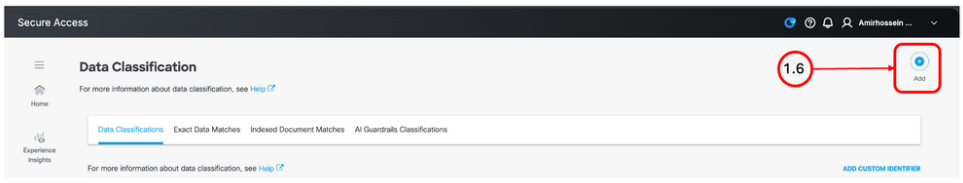
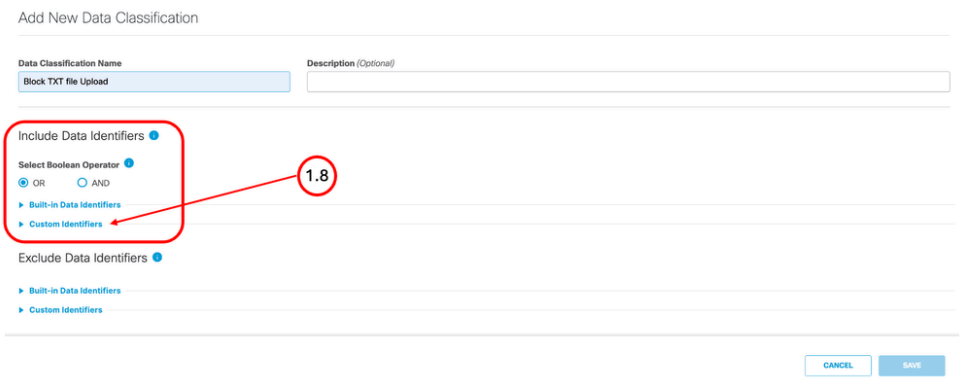
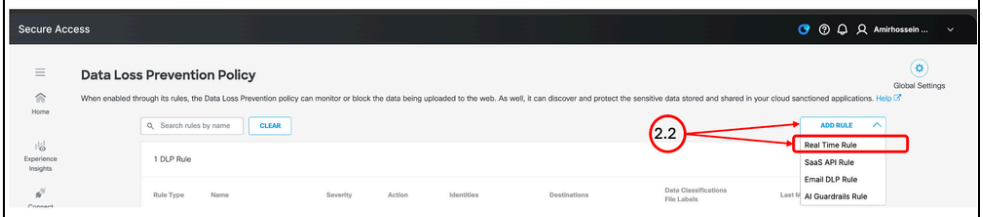



Immagine - Crea una nuova classificazione dati

| | |
|---|---|
| | Passaggio 1.7. Definire un nome.<br><br>Passaggio 1.8. Dalla sezione Includi identificatori dati fare clic su Identificatore personalizzato e scegliere gli identificatori creati nei passaggi precedenti.<br><br>  <br>Immagine - Configurazione della classificazione dei dati<br><br>Passaggio 1.9. Fare clic su Save (Salva). |
| Passaggio 2. Configurare i criteri di prevenzione della perdita dei dati | Passaggio 2.1. Dal portale di gestione di Cisco Secure Access, passare a Secure > Data Loss Prevention Policy (Policy di prevenzione della perdita dei dati)<br><br>Passaggio 2.2. Fare clic su Aggiungi regola e selezionare Regola in tempo reale.<br><br>  <br>Immagine - Crea nuovi criteri di prevenzione della perdita dei dati in tempo reale<br><br>Passaggio 2.3. Definire il nome del criterio.<br><br>Passaggio 2.4. Dalla sezione Classificazioni dati, selezionare la Classificazione dati creata nel Passaggio 1.<br><br>Nota: L'elenco dei criteri di prevenzione della perdita dei dati può contenere fino a 5 minuti per le nuove classificazioni dei dati create.<br><br>Passaggio 2.5. Dalla sezione Controllo file, abilitare il tipo di file e selezionare TXT. |

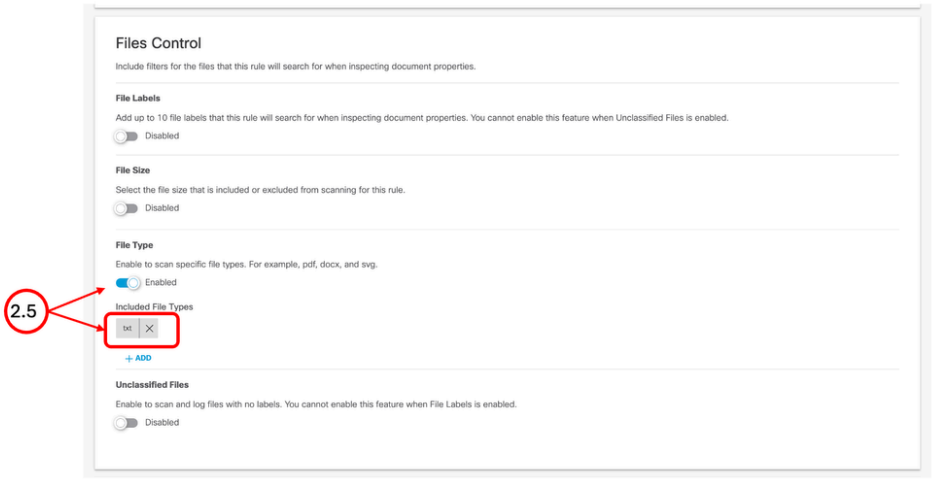



Immagine - Configura tipo di file

Passaggio 2.6. Dalla sezione Azione, scegliere Blocca.

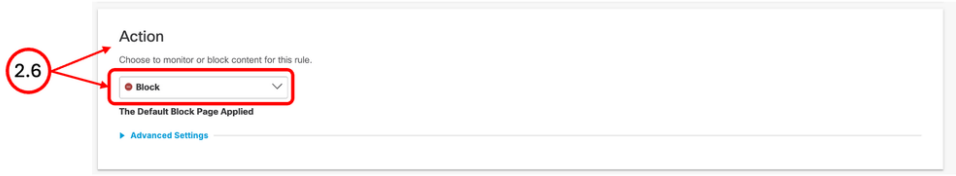



Immagine - Imposta l'azione su Blocca

Passaggio 2.7. Salvare le modifiche

# Controllo

Per controllare l'attività di prevenzione della perdita dei dati e i log correlati, passare a Monitoraggio > Prevenzione della perdita dei dati. Utilizzare i filtri disponibili per restringere i risultati e identificare gli eventi DLP rilevanti.

## Espressioni regolari di esempio

Corrisponde ai caratteri giapponesi Hiragana, Katakana e Kanji:

```
[ぁ-□ァ-ヺー-□]{1,}
```

Trova/sostituisce le lettere latine maiuscole:

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

Trova/sostituisce le lettere e le cifre latine minuscole:

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

Trova/sostituisce i caratteri di punteggiatura comuni:

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

Trova/sostituisce le virgolette semplici, le virgolette doppie e le virgolette inverse:

```
['"`]
```

Trova/sostituisce parentesi quadre, parentesi quadre e parentesi graffe:

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

Trova/sostituisce i simboli comuni e i caratteri speciali:

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

Corrisponde ai caratteri latini nell'intervallo À-ÿ Unicode:

```
[À-ÿ]
```

Trova/sostituisce i caratteri cirillici:

```
[È-ж]
```

Trova/sostituisce i caratteri greci e copti:

```
[Ͱ-Ͽ]
```

Corrisponde ai caratteri in alfabeto arabo:

```
[ء-ۿ]
```

Trova/sostituisce gli ideogrammi unificati CJK:

```
[丠-龥]
```

Trova/sostituisce i caratteri polacchi selezionati con segni diacritici:

```
[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]
```

Corrisponde alle sillabe Hangul coreane:

```
[가-힣]
```

# Informazioni correlate

Cisco Secure Access: elenco completo dei tipi di file supportati da DLP: https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Tipi di file supportati da Cisco Secure Access DLP — Cisco Community: https://community.cisco.com/t5/security-knowledge-base/cisco-secure-access-complete-list-of-dlp-supported-file-types/ta-p/5274268

Informazioni di riferimento sulla configurazione e i criteri di prevenzione della perdita dei dati di Cisco Secure Access: https://securitydocs.cisco.com/docs/csa/olh/161419.dita

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).