Blockieren des TXT-Uploads über SvD in sicherem Zugriff

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Sperren des Uploads von .TXT-Dateien in Cisco Secure Access mit DLP beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Access-Administration
- Schutz vor Datenverlusten (Data Loss Prevention, DLP):

Cisco empfiehlt Folgendes:

- Administrator-Zugriff auf Cisco Secure Access

Verwendete Komponenten

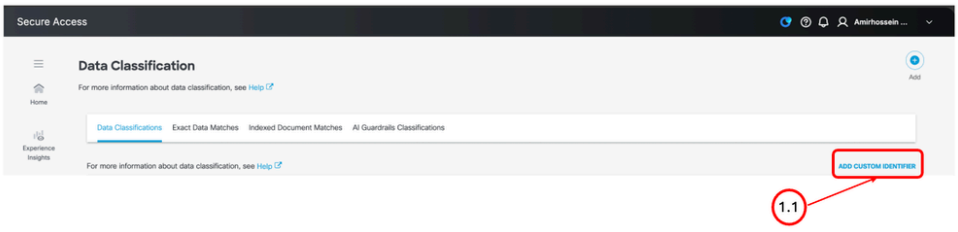
Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Vorbereitungen

1. Gehen Sie bei diesen Schritten mit Vorsicht vor, da sie den DLP-Prozess zusätzlich belasten und zu Leistungseinbußen führen können. Bis die TXT-Dateiblockierung verfügbar ist, können Sie für die derzeit unterstützten Dateitypen auf diesen Link zugreifen: Cisco Secure Access - Unterstützte Dateitypen
2. Dieser Artikel enthält reguläre Beispielausdrücke, die als Referenz verwendet werden können. Bevor Sie eines der Beispiele verwenden, stellen Sie sicher, dass Sie die Übereinstimmungsbedingungen und die Muster, die sie identifizieren sollen, vollständig verstehen. Sie können bei Bedarf auch eigene reguläre Ausdrücke erstellen. Validieren Sie den Ausdruck in allen Fällen sorgfältig, um sicherzustellen, dass er alle vorgesehenen Übereinstimmungsbedingungen und möglichen Variationen richtig abdeckt.
3. Stellen Sie sicher, dass der Datenverkehr entschlüsselt wird, bevor Sie SvD-Richtlinien anwenden. Für die DLP-Inspektion ist der Zugriff auf den entschlüsselten Inhalt erforderlich. verschlüsselter Datenverkehr kann nicht nach DLP-Übereinstimmungen gescannt werden.

Konfigurationsschritte

Kategorie	Schritte
Schritt 1: Datenklassifizierung erstellen	Schritt 1.1: Navigieren Sie im Cisco Secure Access Management-Portal zu Sicher > Datenklassifizierung, und klicken Sie auf Benutzerdefinierten Bezeichner hinzufügen.  Bild - Erstellen eines neuen benutzerdefinierten Bezeichners Schritt 1.2. Definieren eines Namens für die neue Kennung

Schritt 1.3. Konfigurieren Sie im Abschnitt Schwellenwert die Schweregradkriterien, und klicken Sie auf Hinzufügen.

Schritt 1.4. Definieren Sie jeden regulären Ausdruck separat, und klicken Sie auf Hinzufügen.

Tipp: Die in diesem Artikel bereitgestellten regulären Ausdrücke sind nur Beispiele. Überprüfen Sie vor der Verwendung, ob der Ausdruck alle erforderlichen Übereinstimmungsbedingungen und möglichen Variationen richtig abdeckt.

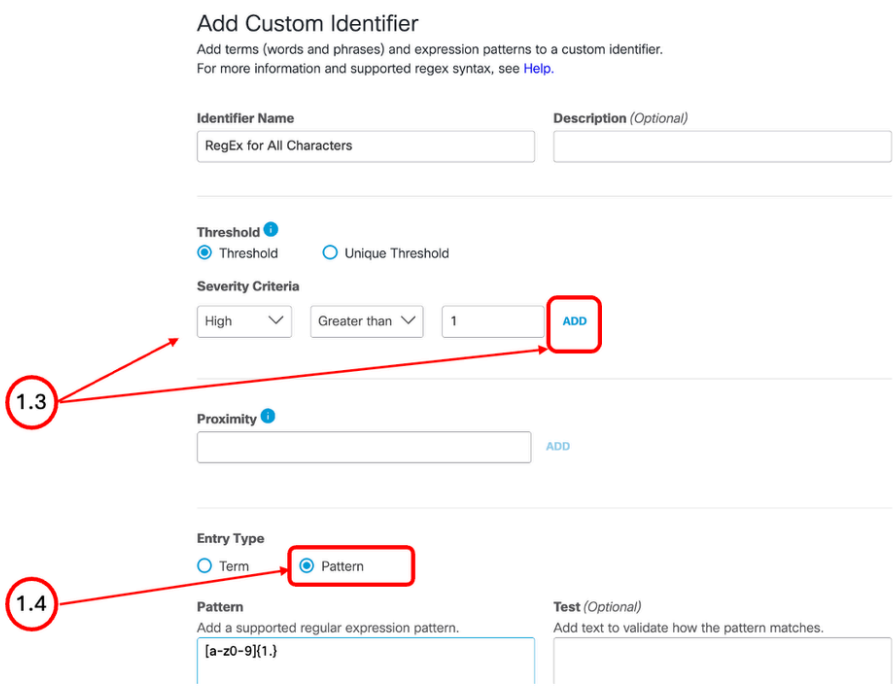


Bild - Benutzerdefinierten Bezeichner hinzufügen

Anmerkung: Wenn es mehr als 10 reguläre Ausdrücke gibt, müssen Sie die gleichen Schritte verwenden, um einen weiteren benutzerdefinierten Bezeichner zu erstellen.

Schritt 1.5: Klicken Sie auf Save (Speichern).

Schritt 1.6: Klicken Sie auf das Symbol Hinzufügen, um eine neue Datenklassifizierung zu erstellen.

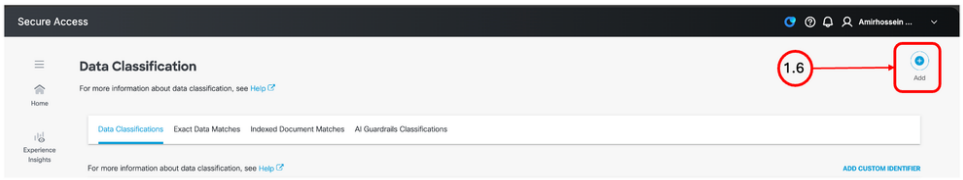
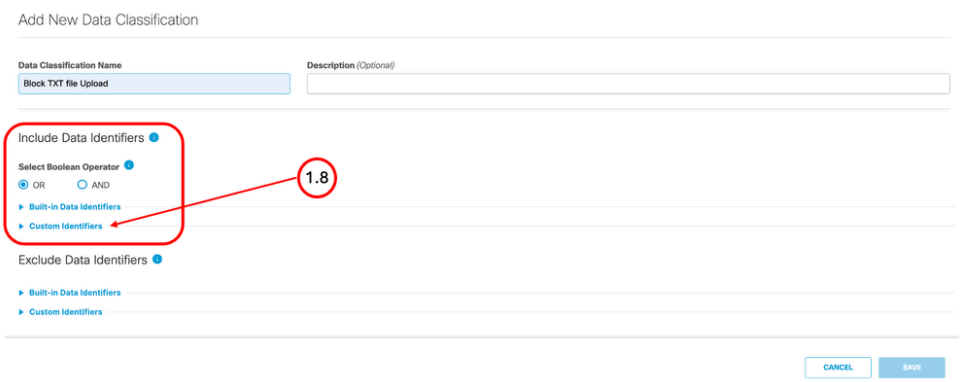
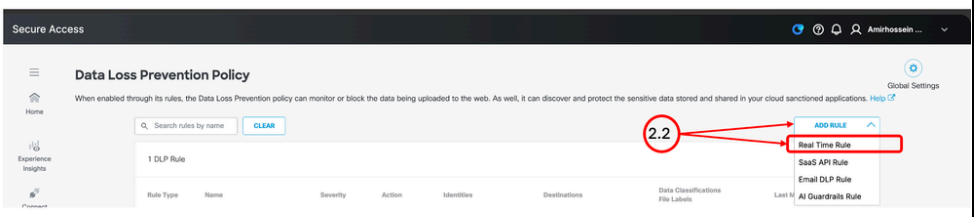


	Bild - Erstellen einer neuen Datenklassifizierung Schritt 1.7. Definieren eines Namens. Schritt 1.8. Klicken Sie im Abschnitt Datenbezeichner einschließen auf Benutzerdefinierte Kennzeichnung, und wählen Sie die Bezeichner aus, die Sie in den vorherigen Schritten erstellt haben.  Bild - Konfigurieren der Datenklassifizierung Schritt 1.9: Klicken Sie auf Save (Speichern).
Schritt 2: Konfigurieren der SvD-Policy	Schritt 2.1: Navigieren Sie im Cisco Secure Access Management-Portal zu Sicher > Richtlinie zum Schutz vor Datenverlust. Schritt 2.2. Klicken Sie auf Regel hinzufügen und wählen Sie Echtzeitregel aus.  Bild - Erstellen einer neuen DLP-Richtlinie in Echtzeit Schritt 2.3: Definieren des Policy-Namens. Schritt 2.4. Wählen Sie im Abschnitt Datenklassifizierungen die Datenklassifizierung aus, die Sie in Schritt 1 erstellt haben. Anmerkung: Es kann bis zu 5 Minuten dauern, bis neu erstellte Datenklassifizierungen in der SvD-Richtlinienliste angezeigt werden. Schritt 2.5. Aktivieren Sie im Abschnitt Dateisteuerung den Dateityp, und wählen Sie TXT aus.

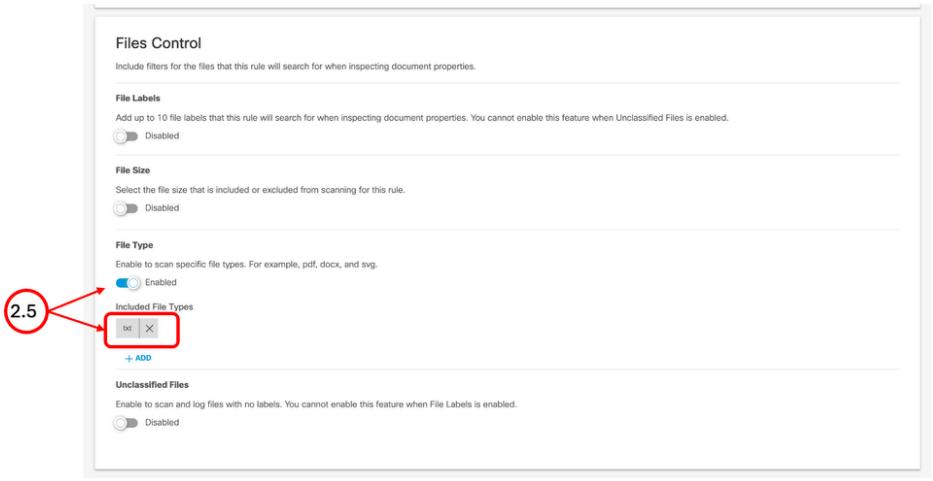


Image: Dateityp konfigurieren

Schritt 2.6. Wählen Sie im Abschnitt Aktion die Option Blockieren aus.

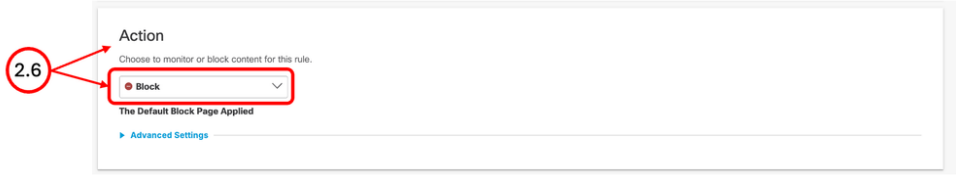


Bild: Setzen Sie die Aktion auf Blockieren.

Schritt 2.7. Speichern der Änderungen

Überwachung

Um die SvD-Aktivität und die zugehörigen Protokolle zu überprüfen, gehen Sie zu Monitor > Data Loss Prevention. Verwenden Sie die verfügbaren Filter, um die Ergebnisse einzugrenzen und die relevanten DLP-Ereignisse zu identifizieren.

Beispiele für reguläre Ausdrücke

Entspricht den japanischen Schriftzeichen Hiragana, Katakana und Kanji:

```
[ぁ-ゖァ-ヺー-□]{1,}
```

Entspricht lateinischen Großbuchstaben:

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

Entspricht lateinischen Kleinbuchstaben und Ziffern:

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

Entspricht gängigen Satzzeichen:

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

Entspricht einfachen Anführungszeichen, doppelten Anführungszeichen und Backticks:

```
['"`]
```

Entspricht Klammern, eckigen und geschweiften Klammern:

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

Entspricht gängigen Symbolen und Sonderzeichen:

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

Entspricht lateinischen Zeichen im Bereich À-Czech Unicode:

```
[À-ÿ]
```

Entspricht kyrillischen Zeichen:

```
[È-ж]
```

Entspricht griechischen und koptischen Zeichen:

```
[Ͱ-ϿⲀ]
```

Entspricht arabisch geschriebenen Zeichen:

```
[ـۿ]
```

Entspricht CJK Unified Ideographs:

```
[丄-𠀋]
```

Gleicht ausgewählte polnische Zeichen mit diakritischen Zeichen ab:

```
[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]
```

Entspricht koreanischen Hangul-Silben:

```
[가-힣]
```

Zugehörige Informationen

Cisco Secure Access - vollständige Liste der DLP-unterstützten Dateitypen: https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Von Cisco Secure Access DLP unterstützte Dateitypen - Cisco Community: https://community.cisco.com/t5/security-knowledge-base/cisco-secure-access-complete-list-of-dlp-supported-file-types/ta-p/5274268

Konfiguration und Richtlinienreferenz für Cisco Secure Access DLP: https://securitydocs.cisco.com/docs/csa/olh/161419.dita

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.