보안 액세스에서 DLP를 통한 TXT 업로드 차단

목차

소개

이 문서에서는 DLP를 사용하는 Cisco Secure Access에서 .TXT 파일 업로드를 차단하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Access 관리
- DLP(Data Loss Prevention)

Cisco에서는 다음과 같은 작업을 수행할 것을 권장합니다.

- Cisco 보안 액세스에 대한 관리 액세스.

사용되는 구성 요소

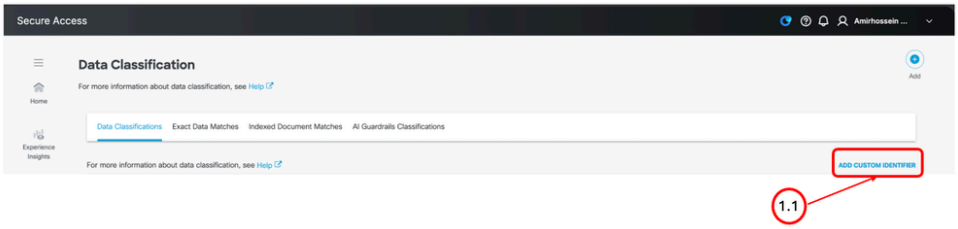
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

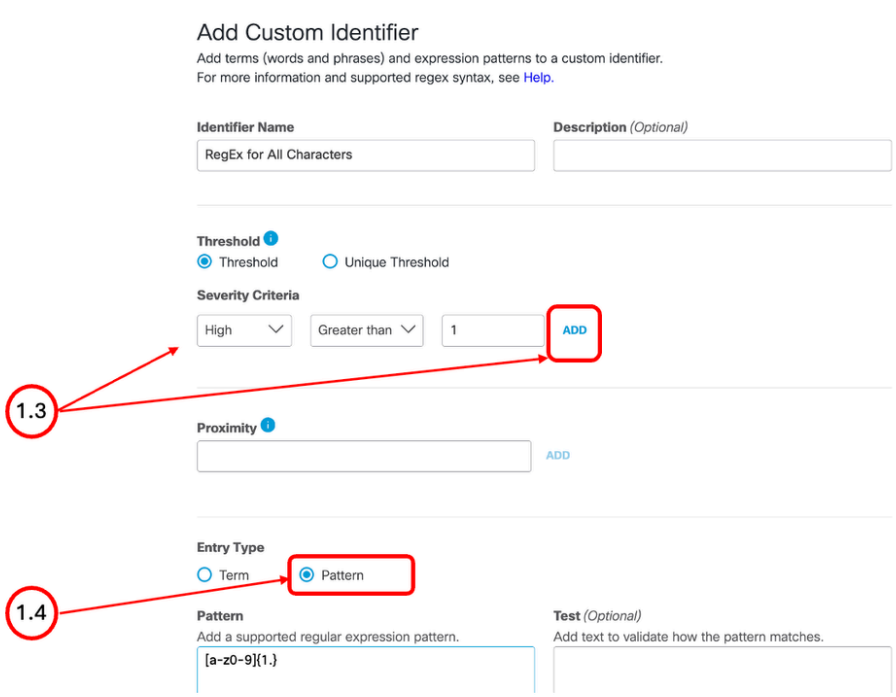
시작하기 전에

1. DLP 프로세스에 추가 로드가 추가되고 성능 저하의 원인이 될 수 있으므로 이 단계를 신중하게 사용하십시오. TXT 파일 차단을 사용할 수 있을 때까지 현재 지원되는 파일 유형에 대해 이 링크를 참조할 수 있습니다. Cisco Secure Access - 지원되는 파일 유형
2. 이 문서에는 참조로 사용할 수 있는 샘플 정규식이 포함되어 있습니다. 예제를 사용하기 전에 일치하는 조건 및 해당 조건이 식별하도록 설계된 패턴을 완전히 이해해야 합니다. 필요한 경우 고유한 정규식을 만들 수도 있습니다. 모든 경우, 의도한 일치 조건 및 가능한 변형을 모두 올바르게 포함하도록 식을 신중하게 검증합니다.
3. DLP 정책을 적용하기 전에 트래픽이 해독되었는지 확인합니다. DLP 검사를 수행하려면 해독된 콘텐츠에 액세스해야 합니다. 암호화된 트래픽에서 DLP 일치를 검사할 수 없습니다.

컨피그레이션 단계

카테고리	단계
1단계. 데이터 분류 생성	1.1단계. Cisco Secure Access 관리 포털에서 Secure(보안) > Data Classification(데이터 분류)으로 이동하고 Add Custom Identifier(맞춤형 식별자 추가)를 클릭합니다.  이미지 - 새 사용자 지정 식별자 만들기 1.2단계. 새 식별자의 이름을 정의합니다. 1.3단계. Threshold(임계값) 섹션에서 Severity Criteria(심각도 기준)를 구성하고 Add(추가)를 클릭합니다. 1.4단계. 각 정규식을 개별적으로 정의하고 Add(추가)를 클릭합니다.

팁: 이 문서에서 제공하는 정규식은 예시에 불과합니다. 사용하기 전에 필요한 모든 일치 조건 및 가능한 변형을 식에 올바르게 포함하는지 확인하십시오.

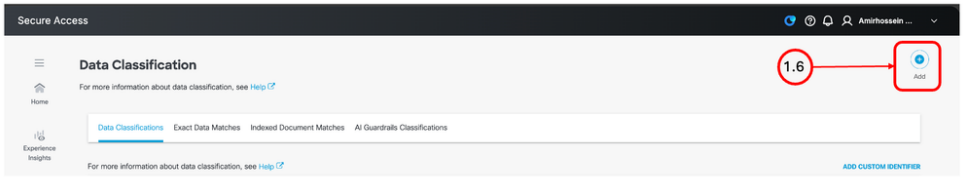


이미지 - 사용자 지정 식별자 추가

참고: 정규식이 10개 이상인 경우 동일한 단계를 사용하여 다른 사용자 지정 식별자를 만들어야 합니다.

1.5단계. Save를 클릭합니다.

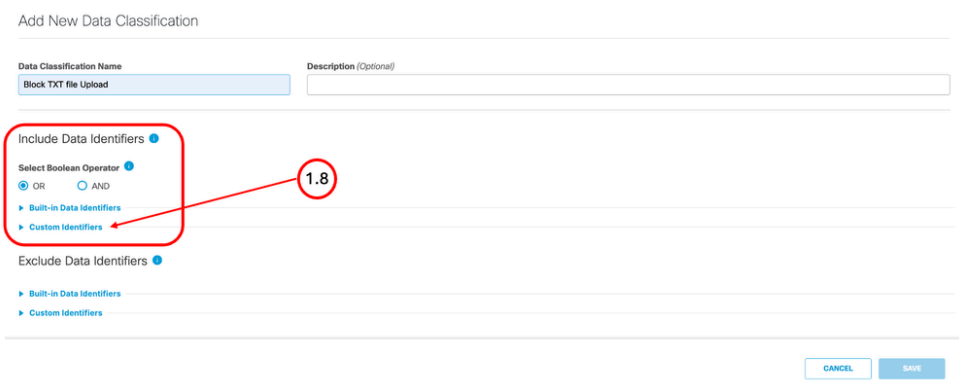
1.6단계. 새 데이터 분류를 생성하려면 추가 아이콘을 누릅니다



이미지 - 새 데이터 분류 생성

1.7단계. 이름을 정의합니다.

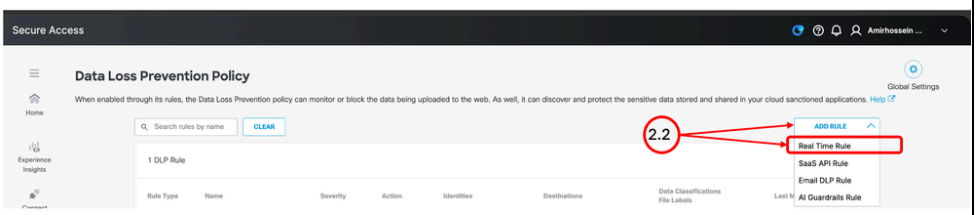
1.8단계. Include Data Identifiers(데이터 식별자 포함) 섹션에서 Custom Identifier(사용자 지정 식별자)를 클릭하고 이전 단계에서 생성한 식별자를 선택합니다.

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


이미지 - 데이터 분류 구성

1.9단계. Save를 클릭합니다.
</td>
</tr>
<tr>
<td>2단계. DLP 정책 구성</td>
<td>
2.1단계. Cisco Secure Access 관리 포털에서 Secure(보안) > Data Loss Prevention Policy(데이터 손실 방지 정책)로 이동합니다

2.2단계. Add Rule을 클릭하고 Real Time Rule을 선택합니다.



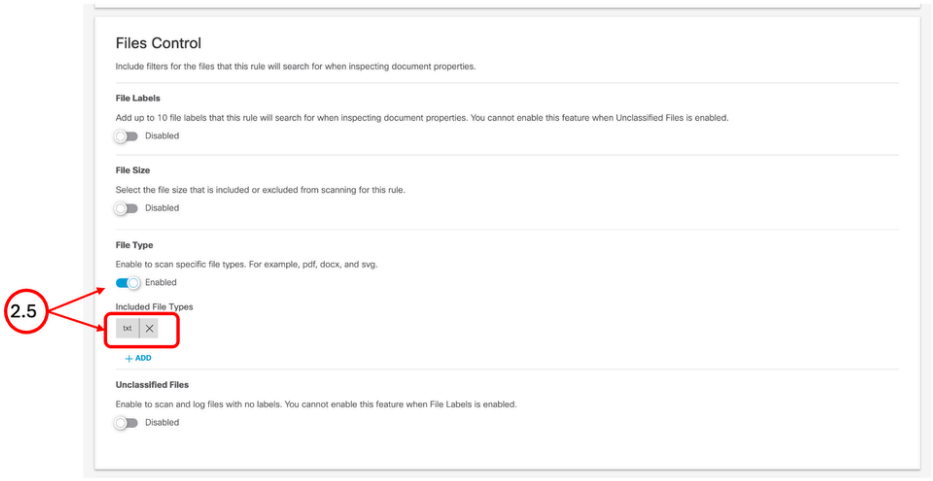
이미지 - 새 실시간 DLP 정책 생성

2.3단계. 정책 이름을 정의합니다.

2.4단계. [데이터 분류] 섹션에서 1단계에서 생성한 데이터 분류를 선택합니다.

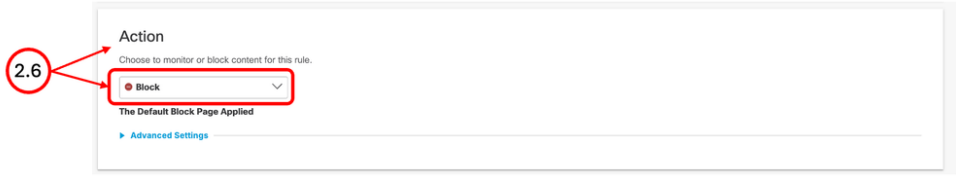
참고: 새로 생성된 데이터 분류가 DLP 정책 목록에 표시될 때까지 최대 5분 정도 기다립니다.

2.5단계. Files Control(파일 제어) 섹션에서 File Type(파일 유형)을 활성화하고 TXT를 선택합니다.
</td>
</tr>
</table>



이미지 - 파일 유형 구성

2.6단계. Action(작업) 섹션에서 Block(차단)을 선택합니다.



이미지 - 작업을 차단으로 설정

2.7단계. 변경 사항을 저장합니다.

모니터링

DLP 활동 및 관련 로그를 확인하려면 Monitor(모니터링) > Data Loss Prevention(데이터 손실 방지)으로 이동합니다. 사용 가능한 필터를 사용하여 결과를 좁히고 관련 DLP 이벤트를 식별합니다.

샘플 정규식

일본어 히라가나, 가타카나 및 간지 문자와 일치합니다.

```
[ぁ-けァ-ヲー-□]{1,}
```

대문자 라틴 문자와 일치:

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

소문자 라틴 문자 및 숫자와 일치합니다.

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

일반 구두점 문자와 일치:

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

작은따옴표, 큰따옴표 및 백틱과 일치합니다.

```
['"`]
```

괄호, 대괄호 및 중괄호와 일치:

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

공통 기호 및 특수 문자와 일치합니다.

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

À-esa 유니코드 범위의 라틴 문자와 일치합니다.

```
[À-ÿ]
```

Cyrillic 문자와 일치:

```
[È-ж]
```

그리스어 및 콥트 문자와 일치:

```
[ـ-ۓ]
```

아랍어 스크립트 문자와 일치:

```
[-ۿ]
```

한중일 통합 한자 일치:

```
[丄-□]
```

선택한 폴란드 문자와 분음 부호 일치:

```
[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]
```

한글 음절 일치:

```
[가-힣]
```

관련 정보

Cisco Secure Access DLP 지원 파일 유형의 전체 목록:
https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Cisco Secure Access DLP 지원 파일 유형 — Cisco 커뮤니티:
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 구성 및 정책 참조:
https://securitydocs.cisco.com/docs/csa/olh/161419.dita

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.