

Blokkeer het uploaden van TXT via DLP in Secure Access

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Voordat u begint](#)

[Configuratiestappen](#)

[Stap 1. Gegevensclassificatie maken](#)

[Stap 2. Het DLP-beleid configureren](#)

[controle](#)

[Voorbeelden van reguliere expressies](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven voor het blokkeren van het uploaden van .TXT-bestanden in Cisco Secure Access met DLP.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beheer van Cisco Secure Access.
- Data Loss Prevention (DLP).

Cisco raadt u aan om:

- Administratieve toegang tot Cisco Secure Access.

Gebruikte componenten

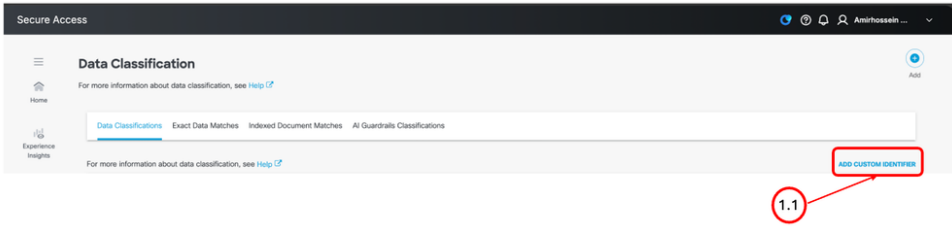
Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Voordat u begint

1. Gebruik deze stappen met voorzichtigheid, omdat ze extra belasting toevoegen aan het DLP-proces en prestatieverlies kunnen veroorzaken. Totdat TXT-bestandsblokkering beschikbaar is, kunt u naar deze link verwijzen voor de momenteel ondersteunde bestandstypen: [Cisco Secure Access - Ondersteunde bestandstypen](#)
2. Dit artikel bevat voorbeelden van reguliere expressies die als referentie kunnen worden gebruikt. Voordat u een van de voorbeelden gebruikt, moet u ervoor zorgen dat u de bijpassende voorwaarden en de patronen die ze zijn ontworpen om te identificeren volledig begrijpt. U kunt ook uw eigen reguliere expressies maken wanneer dat nodig is. Valideer de expressie in alle gevallen zorgvuldig om ervoor te zorgen dat deze correct alle beoogde matchingvoorwaarden en mogelijke variaties dekt.
3. Zorg ervoor dat het verkeer wordt ontsleuteld voordat u DLP-beleid toepast. DLP-inspectie vereist toegang tot de gedecodeerde inhoud; gecodeerd verkeer kan niet worden gescand op DLP-matches.

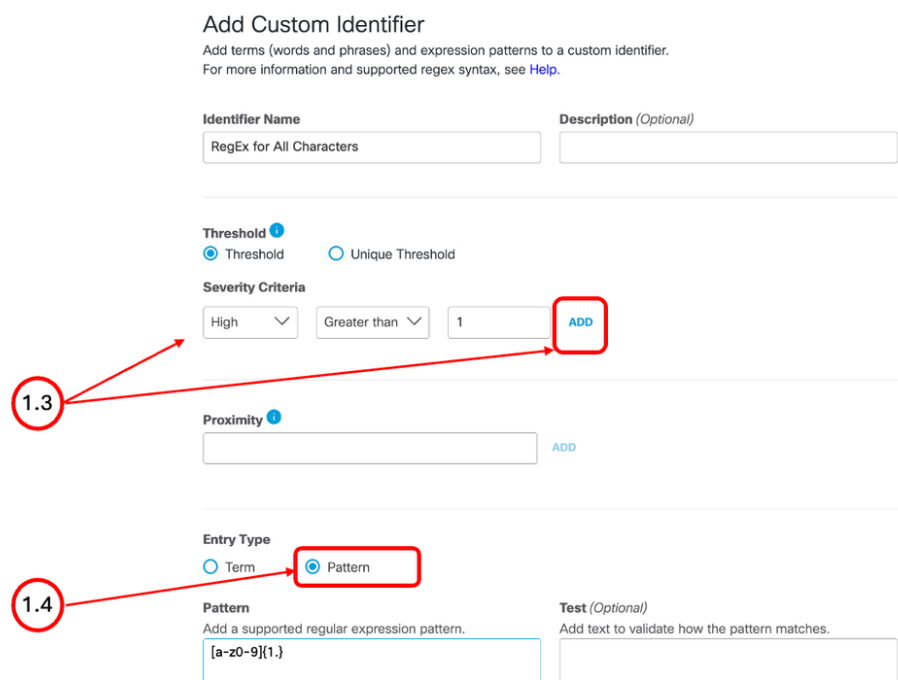
Configuratiestappen

categorie	Stappen
Stap 1. Gegevensclassificatie maken	Stap 1.1. Navigeer vanuit het Cisco Secure Access-beheerportaal naar Veilig > Gegevensclassificatie en klik op de Aangepaste ID toevoegen.  Afbeelding - Een nieuwe aangepaste id maken Stap 1.2. Definieer een naam voor de nieuwe ID

Stap 1.3. Configureer in het gedeelte Drempelwaarde de prioriteitscriteria en klik op Toevoegen.

Stap 1.4. Definieer elke reguliere expressie afzonderlijk en klik op Toevoegen.

 **Tip:** De reguliere uitdrukkingen in dit artikel zijn slechts voorbeelden. Controleer voordat u ze gebruikt of de expressie correct alle vereiste overeenkomende voorwaarden en mogelijke variaties dekt.



The screenshot shows the 'Add Custom Identifier' form. Step 1.3 points to the 'Severity Criteria' section, specifically the 'High' dropdown, the 'Greater than' dropdown, the '1' input field, and the 'ADD' button. Step 1.4 points to the 'Entry Type' section, specifically the 'Pattern' radio button. The 'Pattern' input field contains the regular expression '[a-z0-9]{1,}'.

Add Custom Identifier
Add terms (words and phrases) and expression patterns to a custom identifier.
For more information and supported regex syntax, see [Help](#).

Identifier Name: RegEx for All Characters
Description (Optional):

Threshold 
☒ Threshold ☐ Unique Threshold

Severity Criteria
High Greater than 1 **ADD**

Proximity 
 ADD

Entry Type
☐ Term ☒ **Pattern**

Pattern
Add a supported regular expression pattern.

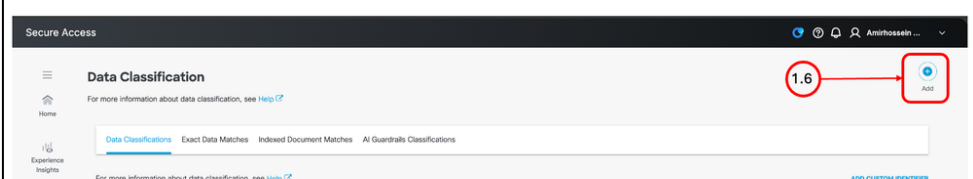
Test (Optional)
Add text to validate how the pattern matches.

Afbeelding - Aangepaste id toevoegen

 **Opmerking:** als er meer dan 10 reguliere expressies zijn, moet u dezelfde stappen gebruiken om een andere aangepaste id te maken.

Stap 1.5. Klik op Save (Opslaan).

Stap 1.6. Klik op het pictogram Toevoegen om een nieuwe gegevensclassificatie te maken



The screenshot shows the 'Data Classification' page. Step 1.6 points to the 'ADD' button in the top right corner.

Secure Access    AmrHossain ...

Data Classification
For more information about data classification, see [Help](#)

Home

 Data Classifications  Exact Data Matches  Indexed Document Matches  AI Guardrails Classifications

Experience Insights
For more information about data classification, see [Help](#)

ADD

Afbeelding - Een nieuwe gegevensclassificatie maken

Stap 1.7. Definieer een naam.

Stap 1.8. Klik in het gedeelte Inclusief gegevens op Aangepaste identificator en kies de identificator(en) die u in de vorige stappen hebt gemaakt.

Add New Data Classification

Data Classification Name: Block TXT file Upload

Description (Optional):

Include Data Identifiers

Select Boolean Operator: ☒ OR ☐ AND

Built-in Data Identifiers

Custom Identifiers

Exclude Data Identifiers

Built-in Data Identifiers

Custom Identifiers

CANCEL SAVE

Afbeelding - De gegevensclassificatie configureren

Stap 1.9. Klik op Save (Opslaan).

Stap 2.1. Navigeer vanuit het Cisco Secure Access-beheerportaal naar Veilig > Beleid voor preventie van gegevensverlies

Stap 2.2. Klik op Regel toevoegen en selecteer Regeltijd.

Secure Access

Data Loss Prevention Policy

When enabled through its rules, the Data Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications. Help

Search rules by name CLEAR

1 DLP Rule

ADD RULE

Real Time Rule

SaaS API Rule

Email DLP Rule

AI Guardrails Rule

Afbeelding - Een nieuw realtime DLP-beleid maken

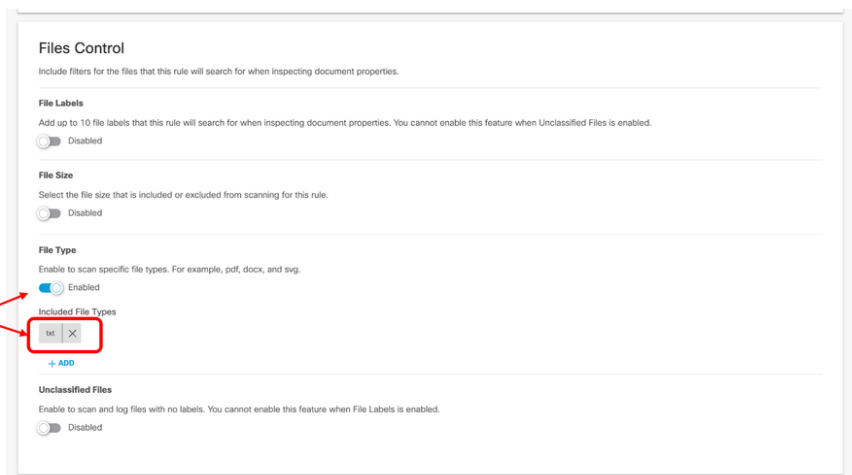
Stap 2. Het DLP-beleid configureren

Stap 2.3. Definieer de naam van het beleid.

Stap 2.4. Selecteer in het gedeelte Gegevensclassificaties de gegevensclassificatie die u in stap 1 hebt gemaakt.

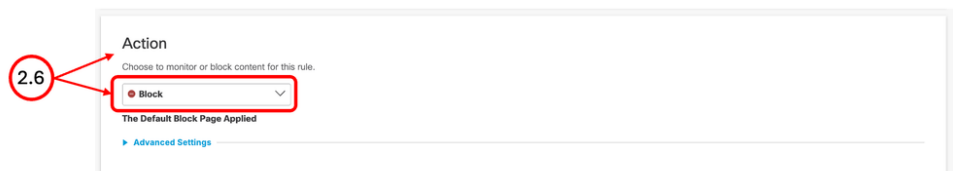
 Opmerking: Laat maximaal 5 minuten voor nieuw gemaakte gegevensclassificaties verschijnen in de DLP-beleidslijst.

Stap 2.5. Schakel in het gedeelte Bestandsbeheer het bestandstype in en selecteer TXT.



Afbeelding - Bestandstype configureren

Stap 2.6. Kies in het gedeelte Actie de optie Blokkeren.



Afbeelding - De actie op Blokkeren instellen

Stap 2.7. Sla de wijzigingen op.

controle

Ga naar Monitor > Preventie van gegevensverlies om de DLP-activiteit en gerelateerde logboeken te controleren. Gebruik de beschikbare filters om de resultaten te verfijnen en de relevante DLP-gebeurtenissen te identificeren.

Voorbeelden van reguliere expressies

Komt overeen met Japanse Hiragana-, Katakana- en Kanji-tekenen:

[あ-け ァ-ゾー-□]{1,}

Komt overeen met hoofdletters Latijnse letters:

[A-Z]{1,}

Komt overeen met kleine letters en cijfers in het Latijn:

[a-z0-9]{1,}

Komt overeen met veelgebruikte interpunctietekens:

[.,;:!?]

Komt overeen met enkele quotes, dubbele quotes en backticks:

['"``]

Komt overeen met haakjes, vierkante haakjes en gekrulde haakjes:

[(){}[]]

Komt overeen met gemeenschappelijke symbolen en speciale tekens:

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

Komt overeen met Latijnse tekens in het À-ÿ Unicode-bereik:

[À-ÿ]

Komt overeen met Cyrillische tekens:

[Ё-ѣ]

Komt overeen met Griekse en Koptische tekens:

[Ⲁ-Ϡ]

Komt overeen met tekens in Arabisch schrift:

[ﺀ-ﻻ]

Komt overeen met CJK Unified Ideographs:

[𠀤-𠬪]

Komt overeen met geselecteerde Poolse tekens met diakritische tekens:

[ĄąĆćĘęŁłŃńÓóŚśŻżŹź]

Komt overeen met Koreaanse Hangul lettergrepen:

[가-힣]

Gerelateerde informatie

Cisco Secure Access complete lijst met door DLP ondersteunde bestandstypen:

<https://securitydocs.cisco.com/docs/csa/olh/120218.dita>

Door Cisco Secure Access DLP ondersteunde bestandstypen — 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-configuratie en beleidsreferentie:

<https://securitydocs.cisco.com/docs/csa/olh/161419.dita>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.