Gegevensverliespreventie - misclassificaties en scanfouten voor probleemoplossing

Inhoud

Inleiding

Dit document beschrijft gemeenschappelijke methoden voor het oplossen van fouten en scanfouten (of fouten) die te maken hebben met betrekking tot Data Loss Prevention (DLP) op de e-mail security applicatie (ESA).

Voorwaarden

- ESA met AsyncOS 11.x of nieuwer.
- DLP-toets is geïnstalleerd en in gebruik.

Belangrijke informatie

Het is van cruciaal belang op te merken dat DLP op het ESA plug-and-play is in de zin dat u het in staat stelt, een beleid maakt en begint te scannen voor gevoelige gegevens. U dient er zich echter ook van bewust te zijn dat de beste resultaten pas zullen worden behaald nadat DLP is afgestemd op uw bedrijfsspecifieke vereisten. Dit zou dingen omvatten zoals types van DLP beleid, beleid dat details matching, het aanpassen van de ernst van schaal, het filteren en extra aanpassingen.

Schending vs. Geen geweld Meld Voorbeelden

Hier zijn een paar voorbeelden van schendingen van DLP die u kunt zien in de maillogbestanden en/of Berichttracering. De loglijn zal een tijdstempel, houtkapniveau, MID #, schending of geen schending, ernst en risicofactor bevatten, en het beleid dat is afgestemd.

```
Thu Jul 11 16:05:28 2019 Info: MID 40 DLP violation. Severity: CRITICAL (Risk Factor: 96). DLP
```

```
policy match: 'US HIPAA and HITECH'.

Thu Jul 11 16:41:50 2019 Info: MID 46 DLP violation. Severity: LOW (Risk Factor: 24). DLP policy
match: 'US State Regulations (Indiana HB 1101)'.
```

Wanneer er geen overtreding is gevonden, worden de e-maillogbestanden en/of Berichttracering *bij DLP* automatisch *geregistreerd*.

```
Mon Jan 20 12:59:01 2020 Info: MID 26245883 DLP no violation
```

Selectieknop voor probleemoplossing

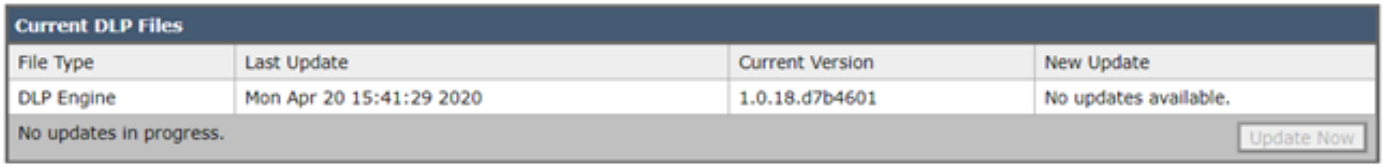
Hieronder vermelde algemene items zijn gebruikelijk die kunnen worden herzien bij de behandeling van DLP-verkeerde indelingen of scanfouten/missen.

> Opmerking: Dit is geen volledige lijst. Neem contact op met Cisco TAC als u iets hebt dat u inclusief wilt zien.

De versie van de DLP-motor bevestigen

DLP motor updates zijn standaard niet automatisch, dus is het van cruciaal belang om te zorgen dat u de nieuwste versie draait die recente verbeteringen of bug fixes bevat.

U kunt onder *Beveiligingsservices* in de GUI navigeren naar *gegevensverloren preventie* om de huidige versie van de motor te bevestigen en om te zien of er updates beschikbaar zijn. Als een update beschikbaar is, kunt u op *Nu bijwerken* klikken om de update uit te voeren.

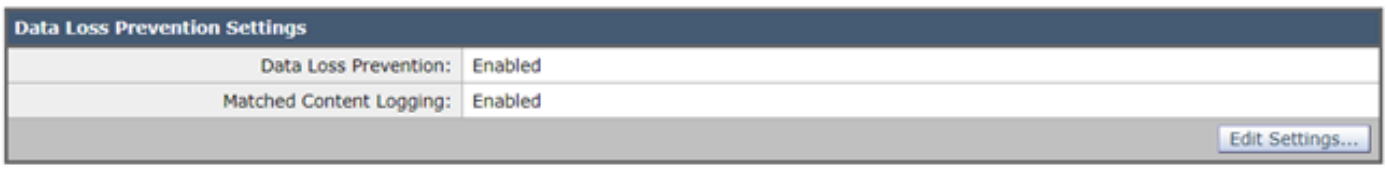


Aangepaste contentvastlegging inschakelen

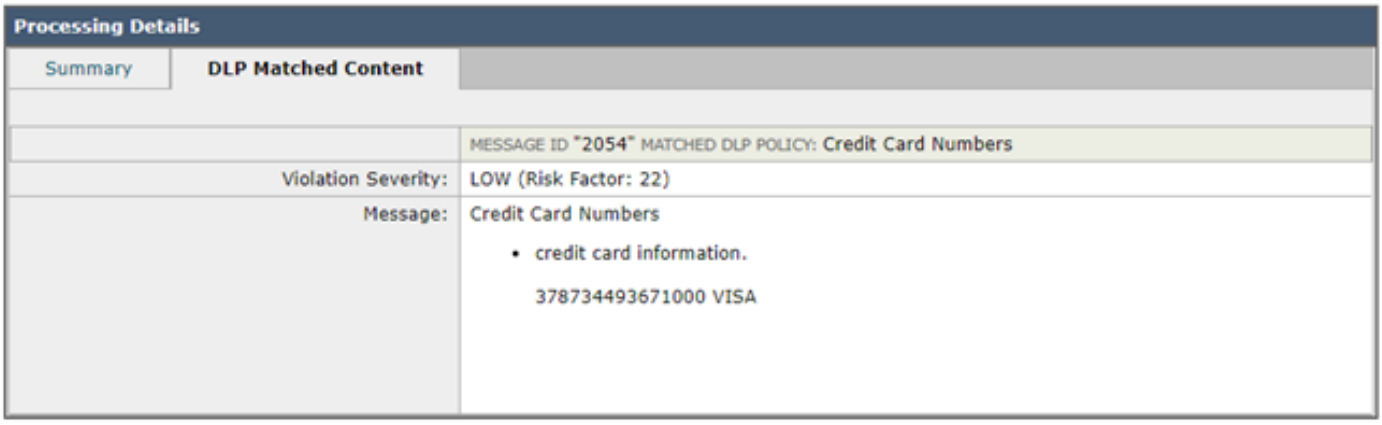
DLP biedt de optie om de inhoud te loggen die uw DLP-beleid schendt, evenals de omliggende inhoud. Deze gegevens kunnen dan in *Message Tracking* worden bekeken om te helpen bij het opsporen van de inhoud van een e-mail die een bepaalde schending kan veroorzaken.

> **Voorzichtig:** Het is belangrijk om te weten dat indien mogelijk, deze inhoud gevoelige gegevens kan omvatten zoals kredietkaartnummers en socialezekerheidsnummers, enz.

U kunt onder *Beveiligingsservices* in de GUI naar *gegevensverliespreventie* navigeren om te zien of *Aangepaste contentvastlegging* is ingeschakeld.



Voorbeeld van aangepaste contentvastlegging gezien in Berichttracering

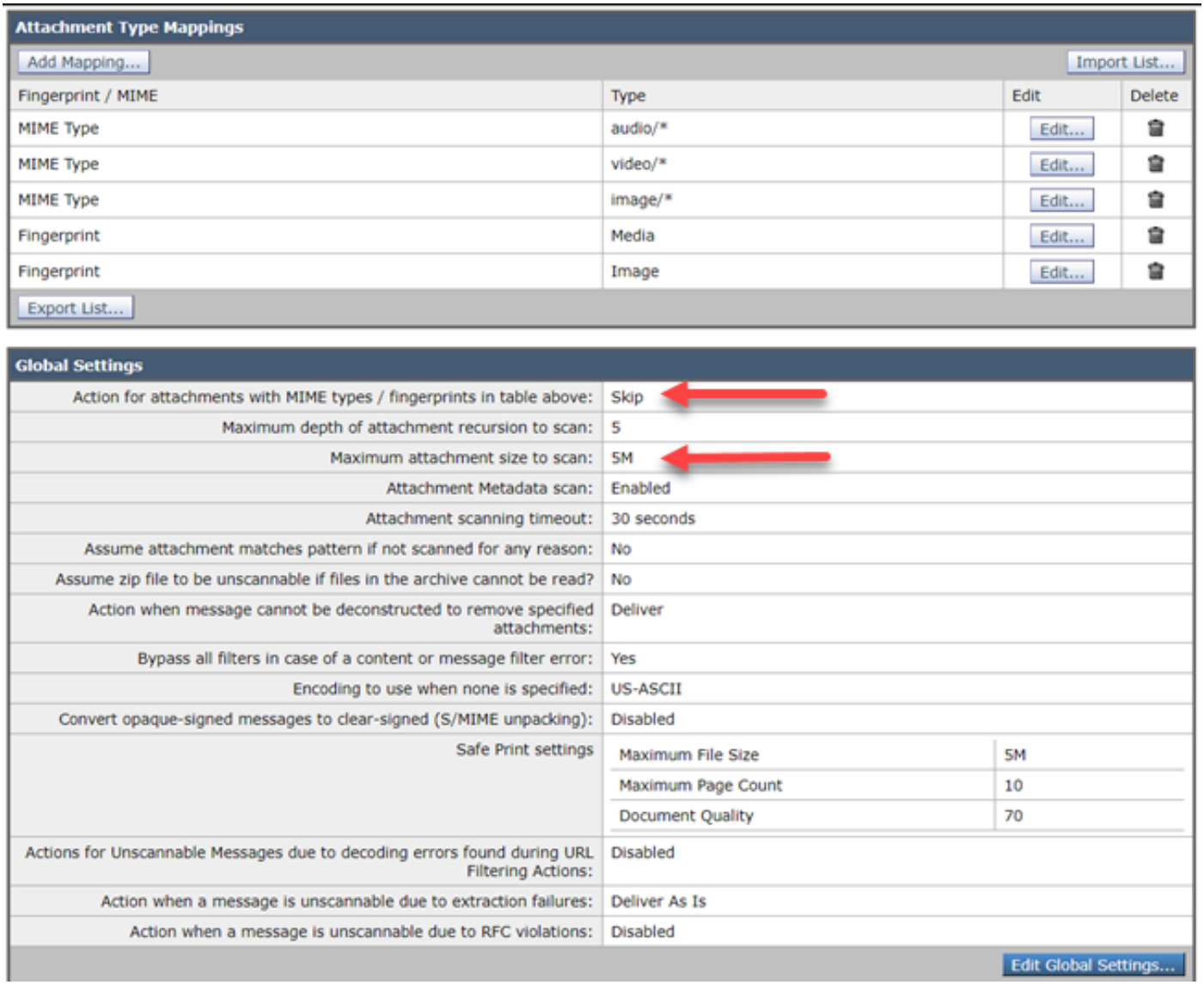


De configuratie van het scangedrag bekijken

De configuratie van het Scannen gedrag op de ESA zal ook van invloed zijn op de functionaliteit achter het DLP-scannen. Als u het hieronder weergegeven scherm bekijkt, zie u een voorbeeld met een ingesteld **maximale** scangrootte van **5 M**, zodat **het** scannen van DLP gemist wordt. Tevens is de **actie voor bijlagen met MIME-**typen een ander veel voorkomend item dat u wilt bekijken. Dit moet worden ingesteld op de standaard van **Skip** zodat de aangegeven MIME-typen worden overgeslagen en alle andere typen worden gescand. Als deze optie ingesteld is op Scannen, *scannen* we *alleen de* in de tabel opgenomen *MIME-typen*.

Op dezelfde manier kunnen andere hier genoemde instellingen invloed hebben op het DLP-scannen en moeten ze in aanmerking worden genomen, afhankelijk van de inhoud van de bijlage/e-mail.

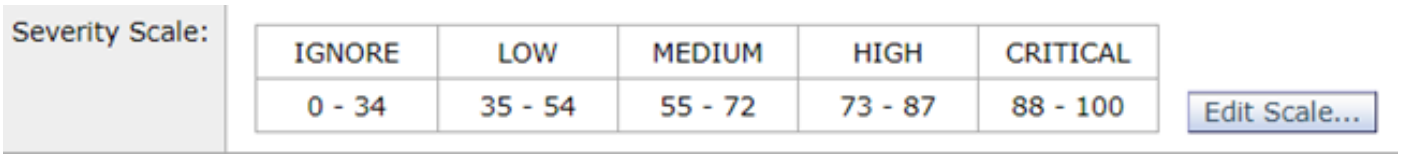
U kunt navigeren om *gedrag te scannen* onder *Beveiligingsservices* in de GUI, of door het **scanconfiguratie** opdracht binnen de CLI uit te voeren.



De configuratie van de prioriteitsschaal bekijken

De standaardinstellingen voor de ernst van de schade zullen voor de meeste omgevingen voldoende zijn; Als u deze echter moet wijzigen om te helpen met FN (FN) of Fse Positive (FP) bij elkaar te brengen, dan kunt u dit doen. U kunt ook bevestigen dat uw DLP-beleid de aanbevolen standaarddrempels gebruikt door een nieuw schijnbeleid te maken en ze vervolgens te vergelijken.

> **Opmerking**: ander vooraf bepaald beleid (bijvoorbeeld VS HIPAA vs. PCI-DSS) zal verschillende schaalgrootte hebben.



De e-mailadressen bekijken die toegevoegd zijn aan de velden van filteraars en -ontvangers

Controleer of een in een van deze velden ingevoerd bestand overeenkomt met het juiste geval van de verzendende en/of het ontvangende e-mailadres. Het veld Afbeeldingen en ontvangers van filter is **hoofdlettergevoelig**. Het DLP-beleid treedt niet op als het e-mailadres eruitziet als "TestEmail@mail.com" in de mailclient en als "testemail@mail.com" in deze velden is ingevoerd.

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Wat is gegevensverliespreventie?
- Trigger een DLP-overtreding om een HIPAA-beleid op de ESA te testen