Prevenzione della perdita di dati - Risoluzione dei problemi di classificazione errata e degli errori di scansione

Sommario

Introduzione

In questo documento vengono descritti i metodi più comuni per risolvere gli errori di classificazione e di scansione (o errori) relativi a Data Loss Prevention (DLP) su Email Security Appliance (ESA).

Prerequisiti

- ESA con AsyncOS 11.x o versione successiva.
- Chiave funzione DLP installata e in uso.

Informazioni importanti

Èfondamentale notare che il DLP sull'ESA è plug-and-play nel senso che è possibile abilitarlo, creare una politica e iniziare la scansione per i dati sensibili; tuttavia, devi anche essere consapevole che i migliori risultati saranno raggiunti solo dopo aver regolato il DLP per soddisfare i requisiti specifici della tua azienda. ad esempio tipi di criteri di prevenzione della perdita dei dati, dettagli sulla corrispondenza ai criteri, regolazione della scala di gravità, filtro e ulteriori personalizzazioni.

Esempi di log delle violazioni e violazioni assenti

Di seguito sono riportati alcuni esempi di violazioni dei criteri di prevenzione della perdita dei dati che possono essere visualizzati nei log di posta e/o nel monitoraggio dei messaggi. La linea di registrazione includerà un indicatore orario, il livello di registrazione, il numero MID, la violazione o nessuna violazione, la gravità e il fattore di rischio e la regola corrispondente.

```
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)'.
```

Quando non viene rilevata alcuna violazione, i log di posta e/o la verifica messaggi registrano semplicemente *DLP senza violazione*.

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

Elenco di controllo per la risoluzione dei problemi

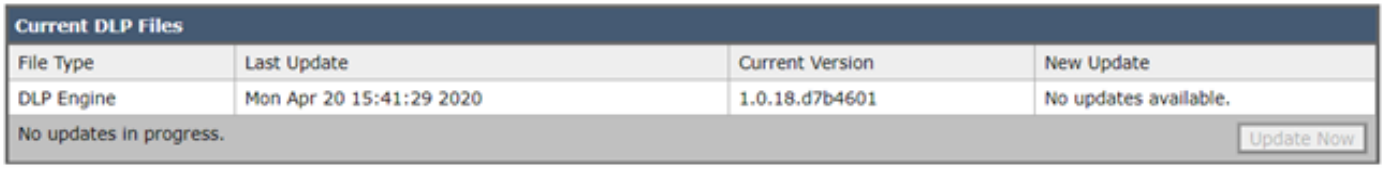
Di seguito sono riportati gli elementi comuni che è possibile esaminare quando si verificano errori o errori di classificazione o di analisi dei criteri di prevenzione della perdita dei dati.

> **Nota:** L'elenco non è esaustivo. Se si desidera includere qualcosa, contattare Cisco TAC.

Conferma della versione del motore DLP

Gli aggiornamenti del motore di prevenzione della perdita dei dati non sono automatici per impostazione predefinita, quindi è fondamentale verificare che sia in esecuzione la versione più recente che include eventuali miglioramenti recenti o correzioni di bug.

Èpossibile passare a *Data Loss Prevention* (Prevenzione perdita dati) in *Security Services* (Servizi di sicurezza) nella GUI per confermare la versione corrente del motore e verificare se sono disponibili aggiornamenti. Se è disponibile un aggiornamento, è possibile fare clic su *Aggiorna adesso* per eseguire l'aggiornamento.

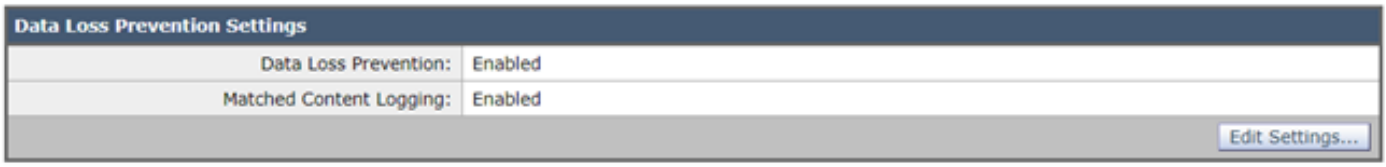


Abilitazione della registrazione del contenuto corrispondente

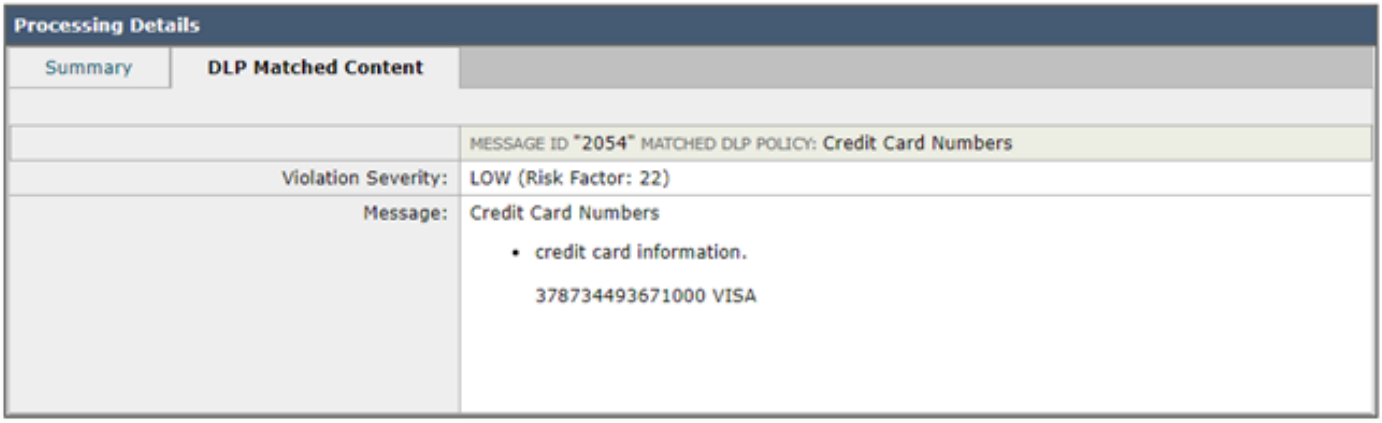
DLP offre la possibilità di registrare il contenuto che viola i criteri di prevenzione della perdita dei dati, insieme al contenuto circostante. Questi dati possono quindi essere visualizzati in *Message Tracking* (Verifica messaggi) per individuare il contenuto di un'e-mail che potrebbe causare una particolare violazione.

> **Attenzione:** È importante sapere che, se abilitato, questo contenuto può includere dati riservati come numeri di carta di credito e numeri di previdenza sociale, ecc.

Èpossibile passare a *Data Loss Prevention* (Prevenzione della perdita dei dati) in *Security Services* (Servizi di sicurezza) nella GUI per verificare se la *registrazione del contenuto corrispondente* è abilitata.



Esempio di log del contenuto corrispondente visualizzato in Message Tracking

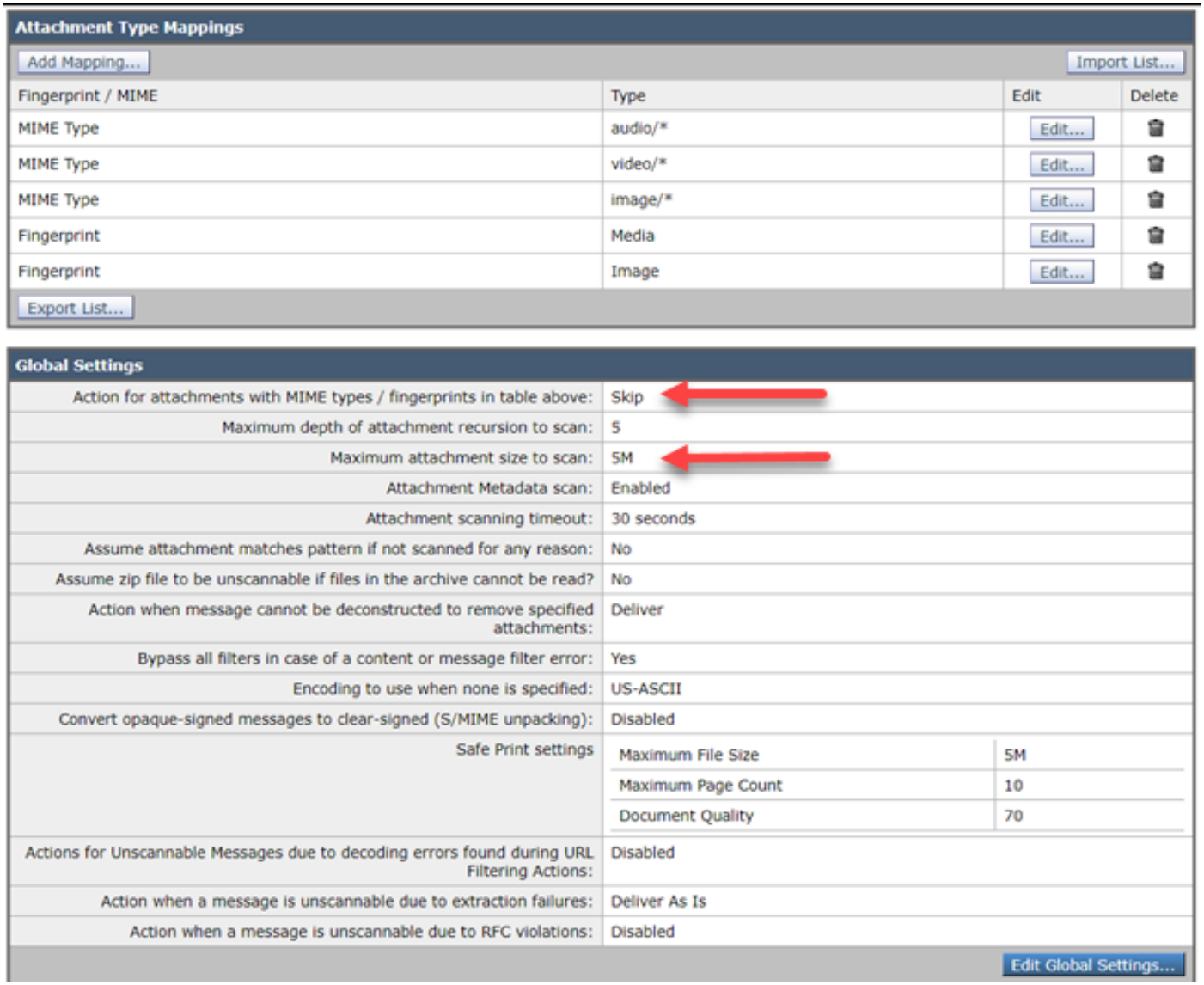


Esame della configurazione del comportamento di scansione

La configurazione del comportamento di scansione sull'ESA influisce anche sulla funzionalità di scansione DLP. Osservando lo screenshot seguente come esempio, che ha una **dimensione massima configurata** di **scansione** degli **allegati** di **5M**, un valore maggiore potrebbe causare la mancata scansione del DLP. L'**azione per gli allegati con l'**impostazione **dei tipi MIME** è un altro elemento comune che si desidera esaminare. È necessario impostare il valore predefinito **Skip** in modo che i tipi MIME elencati vengano ignorati e tutti gli altri vengano analizzati. Se invece è impostato su Scan, verranno *analizzati solo i tipi MIME* elencati nella tabella.

Analogamente, altre impostazioni qui elencate possono influire sulla scansione DLP e devono essere prese in considerazione a seconda del contenuto dell'allegato/e-mail.

Èpossibile passare a *Scan Behavior* (Comportamento analisi) in *Security Services* nella GUI o eseguendo il comando **scanconfig** nella CLI.



Attachment Type Mappings

Add Mapping... | Import List...

Fingerprint / MIME	Type	Edit	Delete
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	
MIME Type	image/*	Edit...	
Fingerprint	Media	Edit...	
Fingerprint	Image	Edit...	

Export List...

Global Settings

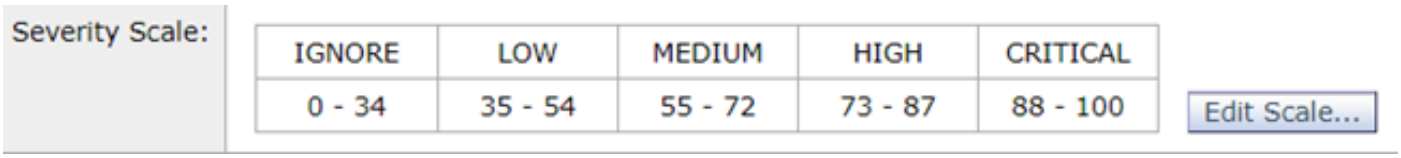
Action for attachments with MIME types / fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	5M
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Safe Print settings	Maximum File Size: 5M; Maximum Page Count: 10; Document Quality: 70
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled

Edit Global Settings...

Esame della configurazione della scala di gravità

Le soglie predefinite della scala di gravità saranno sufficienti per la maggior parte degli ambienti; tuttavia, se è necessario modificarli per supportare la corrispondenza con i valori FN (False Negative) o FP (False Positive), è possibile eseguire questa operazione. È inoltre possibile verificare che i criteri di prevenzione della perdita dei dati utilizzino le soglie predefinite consigliate creando un nuovo criterio fittizio e quindi confrontandoli.

> **Nota**: i diversi criteri predefiniti (ad esempio HIPAA USA e PCI-DSS) hanno una diversa scala.



Severity Scale:

IGNORE	LOW	MEDIUM	HIGH	CRITICAL
0 - 34	35 - 54	55 - 72	73 - 87	88 - 100

Edit Scale...

Esame degli indirizzi e-mail aggiunti ai campi Filtra mittenti e destinatari

Verificare che le voci immesse in uno di questi campi corrispondano alla corrispondenza tra maiuscole e minuscole degli indirizzi e-mail del mittente e/o del destinatario. Il campo Filtra mittenti e destinatari **rileva la distinzione tra maiuscole** e **minuscole**. I criteri di prevenzione della perdita dei dati non verranno attivati se l'indirizzo e-mail nel client di posta assomiglia a

"TestEmail@mail.com" e viene immesso come "testemail@mail.com" in questi campi.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Cos'è la prevenzione della perdita dei dati?
- Attivare una violazione del DLP per testare una politica HIPAA sull'ESA