Prevención de pérdida de datos: resolución de problemas de clasificaciones erróneas y fallas de escaneo

Contenido

Introducción

Este documento describe métodos comunes para solucionar errores de clasificación y escanear fallas (o pérdidas) relacionadas con la prevención de pérdida de datos (DLP) en el dispositivo de seguridad de correo electrónico (ESA).

Prerequisites

- ESA que ejecuta AsyncOS 11.x o posterior.
- Clave de característica DLP instalada y en uso.

Información importante

Es fundamental tener en cuenta que DLP en el ESA es plug-and-play en el sentido de que puede habilitarlo, crear una política y comenzar a buscar datos confidenciales; sin embargo, también debe ser consciente de que los mejores resultados sólo se obtendrán después de ajustar DLP para adaptarlos a los requisitos específicos de su empresa. Esto incluiría elementos como tipos de políticas de DLP, detalles de coincidencia de políticas, ajuste de la escala de gravedad, filtrado y personalizaciones adicionales.

Ejemplos de Violación vs. No Violación de Registro

A continuación se muestran algunos ejemplos de violaciones de DLP que puede ver en los registros de correo o en el Rastreo de mensajes. La línea de registro incluirá una marca de

tiempo, el nivel de registro, el número de IDm, la violación o ausencia de infracción, el factor de gravedad y riesgo y la política coincidente.

```
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)'.
```

Cuando no se encuentra ninguna violación, los registros de correo y/o el Rastreo de mensajes simplemente registrarán *DLP sin infracción*.

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

Lista de comprobación de resolución de problemas

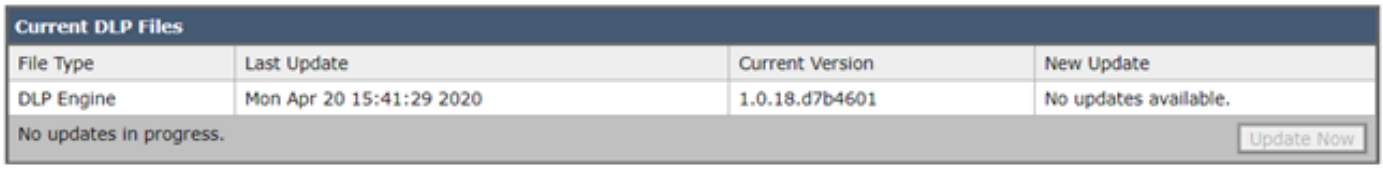
A continuación, se proporcionan los elementos comunes que se pueden revisar cuando se trata de clasificaciones erróneas de DLP o errores/errores de escaneo.

> **Nota:** Esta es una lista exhaustiva. Póngase en contacto con el TAC de Cisco si desea que se le incluya algo.

Confirmación de la versión del motor DLP

Las actualizaciones del motor DLP no son automáticas de forma predeterminada, por lo que es fundamental asegurarse de que está ejecutando la versión más reciente que incluye mejoras o correcciones de errores recientes.

Puede navegar hasta *Prevención de pérdida de datos* en *Servicios de seguridad* en la GUI para confirmar la versión actual del motor y ver si hay actualizaciones disponibles. Si hay una actualización disponible, puede hacer clic en *Actualizar ahora* para realizar la actualización.



Current DLP Files

File Type	Last Update	Current Version	New Update
DLP Engine	Mon Apr 20 15:41:29 2020	1.0.18.d7b4601	No updates available.

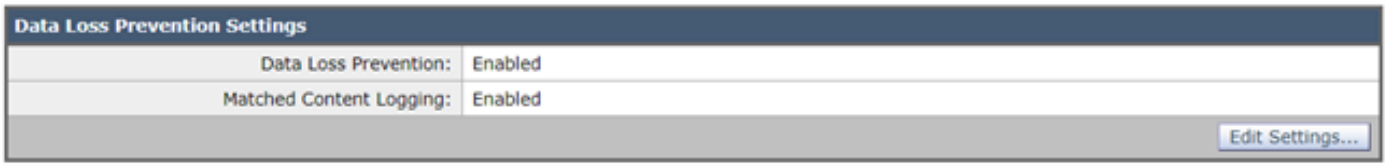
No updates in progress. Update Now

Habilitación del Registro de Contenido Coincidente

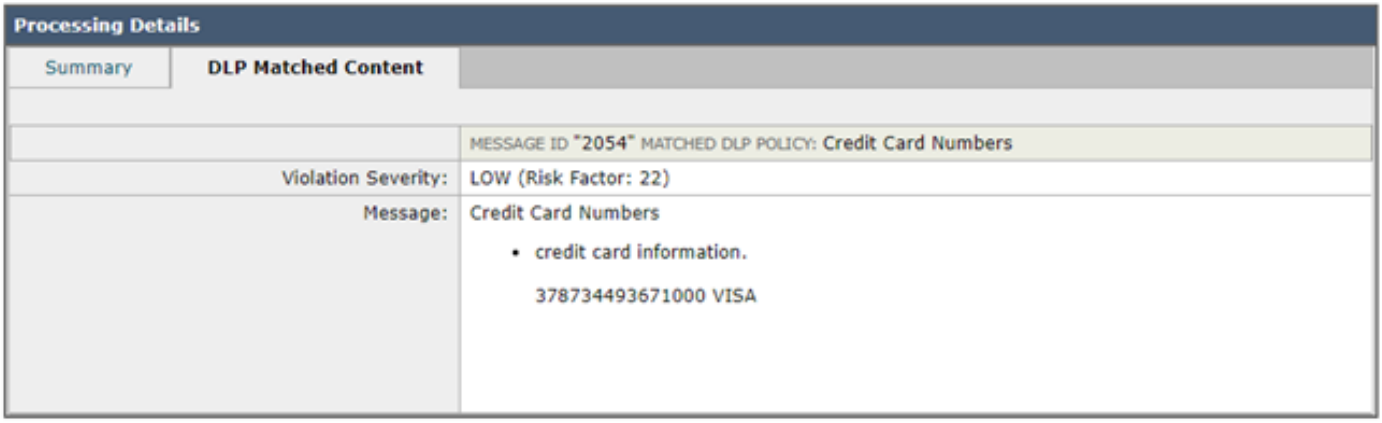
DLP ofrece la opción de registrar el contenido que infringe las políticas de DLP, junto con el contenido que lo rodea. Estos datos se pueden ver luego en *Rastreo de mensajes* para ayudar con el rastreo de qué contenido dentro de un correo electrónico puede estar causando una violación en particular.

> **Precaución:** Es importante saber que, si se activa, este contenido puede incluir datos confidenciales como números de tarjetas de crédito y números de la seguridad social, etc.

Puede navegar hasta *Prevención de pérdida de datos* en *Servicios de seguridad* en la GUI para ver si *Registro de contenido coincidente* está habilitado.



Ejemplo de registro de contenido coincidente visto en el rastreo de mensajes

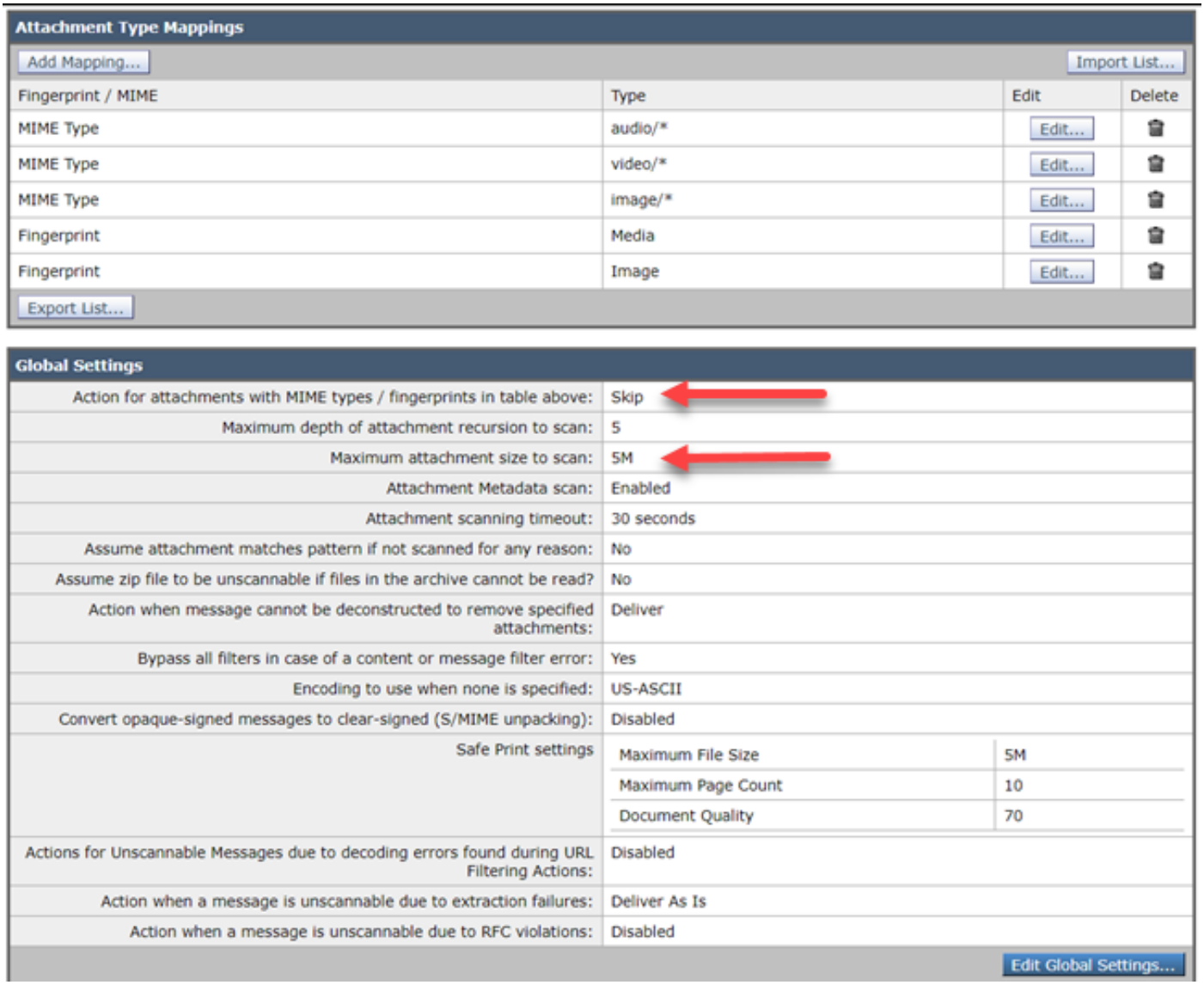


Revisión de la configuración del comportamiento de escaneo

La configuración de comportamiento de escaneo en el ESA también afectará a la funcionalidad detrás del escaneo de DLP. Al observar la captura de pantalla siguiente como ejemplo, que tiene un **tamaño máximo de escaneo** de archivos adjuntos **configurado** de **5M**, cualquier tamaño puede hacer que se pierda el escaneo de DLP. Además, la **acción para los archivos adjuntos con la** configuración de **tipos MIME** es otro elemento común que desea revisar. Esto se debe establecer en el valor predeterminado de **Skip** para que los tipos MIME enumerados se omitan y se escanee todo lo demás. Si en su lugar está configurado en Scan (Escanear), entonces *sólo analizamos los tipos MIME* enumerados en la tabla.

Asimismo, otras configuraciones enumeradas aquí pueden afectar al escaneo de DLP y deben tenerse en cuenta en función del contenido del archivo adjunto/correo electrónico.

Puede navegar hasta *Scan Behavior* en *Security Services* en la GUI, o ejecutando el comando **scanconfig** dentro de la 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

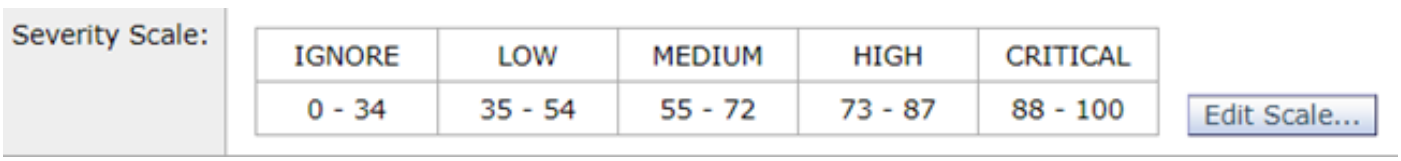
Action for attachments with MIME types / fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	5M
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
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...

Revisión de la Configuración de Escala de Gravedad

Los umbrales de escala de gravedad predeterminados serán suficientes para la mayoría de los entornos; sin embargo, si necesita modificarlos para ayudar con la coincidencia de FN (False Negative) o Falso Positive (FP), puede hacerlo. También puede confirmar que su política de DLP utiliza los umbrales predeterminados recomendados creando una nueva política falsa y después comparándolos.

> **Nota**: Las diferentes políticas predefinidas (p. ej., HIPAA de EE. UU. frente a PCI-DSS) tendrán un escalado diferente.



Severity Scale:

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

Edit Scale...

Revisión de las direcciones de correo electrónico agregadas a los campos Filtrar remitentes y destinatarios

Compruebe que las entradas introducidas en cualquiera de estos campos coincidan con el caso correcto de las direcciones de correo electrónico del remitente o del destinatario. El campo Filtrar remitentes y destinatarios distingue **entre mayúsculas y minúsculas**. La política de DLP no se activará si la dirección de correo electrónico se muestra como "TestEmail@mail.com" en el cliente

de correo y se introduce como "testemail@mail.com" en estos campos.

Información Relacionada

- Dispositivo de seguridad Cisco Email Security Appliance - Guías de usuario final
- ¿Qué es la prevención de la pérdida de datos?
- Desencadenar una violación de DLP para probar una política HIPAA en ESA