

Guía de prácticas recomendadas para protección frente a malware avanzado (AMP) en Cisco Email Security

Contenido

[Introducción](#)

[Verificar claves de característica](#)

[Habilitar protección frente a malware avanzado \(AMP\)](#)

[Personalización de la configuración global de protección frente a malware avanzado \(AMP\)](#)

[Configuración del umbral de Análisis de archivos](#)

[Integre ESA con AMP para la consola de terminales](#)

[Habilitar la remediación automática del buzón \(MAR\)](#)

[Configuración de la protección frente a malware avanzado \(AMP\) en la política de correo](#)

[Integración de SMA con Cisco Threat Response \(CTR\)](#)

[Conclusión](#)

Introducción

La protección frente a malware avanzado (AMP) es una solución completa que permite la detección y el bloqueo de malware, el análisis continuo y las alertas retrospectivas. El aprovechamiento de AMP con Cisco Email Security ofrece una protección superior a lo largo de todo el ciclo de ataque: antes, durante y después de un ataque con el enfoque de defensa frente a malware avanzado más rentable y fácil de implementar.

Este documento de prácticas recomendadas tratará las características clave de AMP en Cisco Email Security Appliance (ESA) como se indica a continuación:

- **Reputación de archivos** - captura una huella digital de cada archivo a medida que atraviesa el ESA y la envía a la red de inteligencia basada en la nube de AMP para emitir un veredicto de reputación. Teniendo en cuenta estos resultados, puede bloquear automáticamente los archivos malintencionados y aplicar la política definida por el administrador.
- **Análisis de archivos:** proporciona la capacidad de analizar los archivos desconocidos que atraviesan el ESA. Un entorno de espacio aislado altamente seguro permite a AMP obtener detalles precisos sobre el comportamiento del archivo y combinar esos datos con análisis humanos y automatizados detallados para determinar el nivel de amenaza del archivo. A continuación, esta disposición se introduce en la red de inteligencia basada en la nube de AMP y se utiliza para actualizar y ampliar de forma dinámica el conjunto de datos de la nube de AMP con el fin de mejorar la protección.
- **Remediación automática de buzón de correo (MAR):** para Microsoft Office 365 y Exchange 2013/2016 automatiza la eliminación de correos electrónicos con archivos que se vuelven maliciosos después del punto de inspección inicial. Esto ahorra a los administradores horas de trabajo y ayuda a contener el impacto de una amenaza.
- **Cisco AMP Unity:** es la capacidad que permite a una organización registrar su dispositivo habilitado para AMP, incluido el ESA con suscripción a AMP en AMP para terminales

Console. Con esta integración, Cisco Email Security se puede ver y consultar para obtener observaciones de ejemplo de la misma manera que la consola de AMP para terminales ya ofrece para terminales y permite correlacionar los datos de propagación de archivos en todos los vectores de amenazas en una única interfaz de usuario.

- **Cisco Threat Response:** es una plataforma de orquestación que reúne información relacionada con la seguridad de fuentes de Cisco y de terceros en una única consola de respuesta e investigación intuitiva. Lo hace a través de un diseño modular que sirve como marco de integración para los registros de eventos y la inteligencia de amenazas. Los módulos permiten una correlación rápida de los datos mediante la creación de gráficos de relaciones que, a su vez, permiten a los equipos de seguridad obtener una visión clara del ataque, así como realizar acciones de respuesta eficaces rápidamente.

Verificar claves de característica

- En el ESA, vaya a **Administración del sistema > Claves de funciones**
- Busque las teclas de función **Reputación de archivos** y **Análisis de archivos** y asegúrese de que los estados son **Activo**

Habilitar protección frente a malware avanzado (AMP)

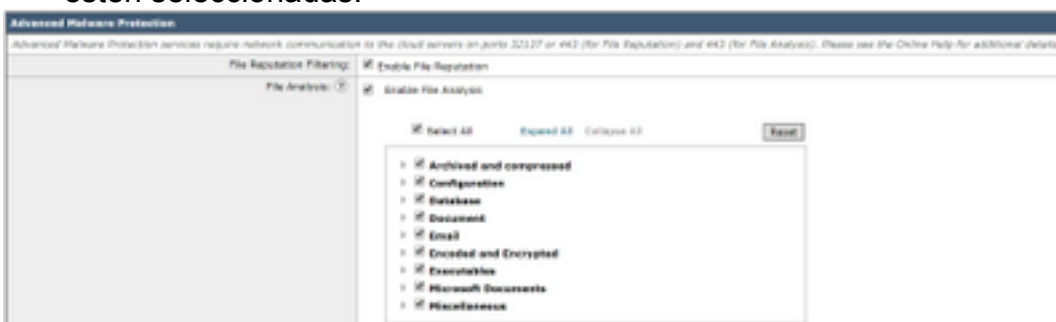
- En ESA, navegue hasta **Servicios de seguridad > Protección frente a malware avanzado - Reputación y análisis de archivos**
- Haga clic en el botón **Enable** en **Advanced Malware Protection Global Settings**:



- **Confirme** sus cambios.

Personalización de la configuración global de protección frente a malware avanzado (AMP)

- AMP está ahora habilitado, haga clic en **Editar configuración global** para personalizar la configuración global.
- La lista de extensiones de archivo se actualizará automáticamente de vez en cuando, por lo que siempre visite esta configuración y asegúrese de que todas las extensiones de archivo estén seleccionadas:



- Expandir la configuración avanzada para **Reputación de archivos**

- La selección predeterminada para File Reputation Server es **AMERICA (cloud-sa.amp.cisco.com)**
- Haga clic en el menú desplegable y seleccione los servidores de reputación de archivos más cercanos (especialmente para los clientes de APJC y EUROPE):



- Expandir la configuración avanzada para el análisis de archivos
- La selección predeterminada para la URL de File Analysis Server es **AMERICAS (https://panacea.threatgrid.com)**
- Haga clic en el menú desplegable y seleccione los servidores de reputación de archivos más cercanos (especialmente para los clientes de EUROPA):



Configuración del umbral de Análisis de archivos

(Opcional) Se le permite establecer el límite superior del umbral para la puntuación de análisis de archivos aceptable. Los archivos bloqueados en función de la configuración de umbral se muestran como Umbral personalizado en la sección Archivos de amenazas de malware entrantes del informe Protección frente a malware avanzado.

- En la página de configuración global de AMP, expanda **Threshold Settings**.
- El valor predeterminado del servicio en la nube es **95**.
- Elija el botón de opción de **Introducir valor personalizado** y cambie el valor (por ejemplo, 70):



- Haga clic en **Enviar** y confirme sus cambios

Integre ESA con AMP para la consola de terminales

(Solo para el cliente de AMP para terminales) Se puede crear una lista de bloqueo de archivos personalizada unificada (o una lista de archivos permitidos) a través de la consola de AMP para terminales y distribuir sin problemas la estrategia de contención a través de la arquitectura de seguridad, incluido el ESA.

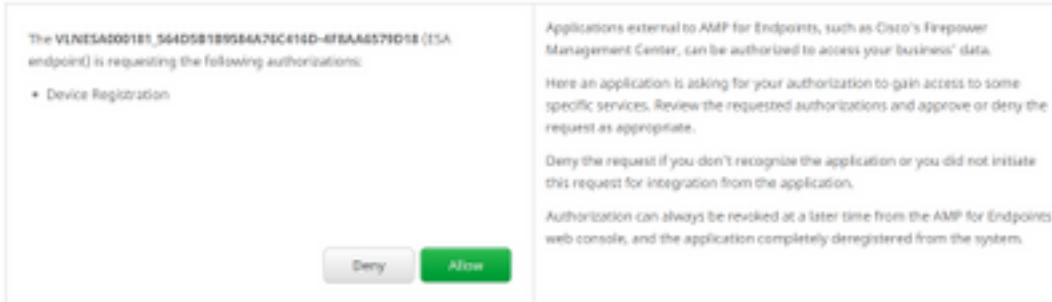
- En la página de configuración global de AMP, expanda **Configuración avanzada para Reputación de archivos**
- Al hacer clic en el botón - **Registrar dispositivo con AMP para terminales**:



- Haga clic en **Aceptar** para redirigir al sitio de la consola de AMP para terminales para

completar el registro.

- Inicie sesión en la consola de AMP para terminales con sus credenciales de usuario
- Haga clic en **Permitir** autorización del registro ESA:



- La consola de AMP para terminales mueve automáticamente la página de nuevo a ESA.
- Asegúrese de que el estado del registro se muestra como **SUCCESS**:



- Haga clic en **Enviar** y **Registrar** los cambios

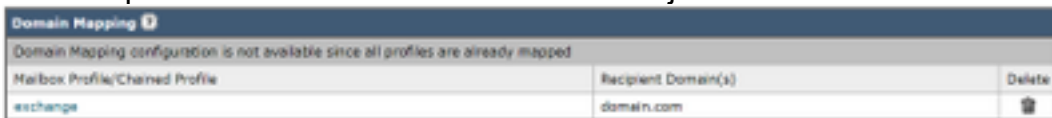
Habilitar la remediación automática del buzón (MAR)

Si tiene buzones O365 o Microsoft Exchange 2013/2016, la función de remediación automática de buzón (MAR) permitirá que se realice la acción cuando el veredicto de reputación de archivo cambie de Limpio/Desconocido a Malintencionado.

- Vaya a **Administración del sistema > Configuración de cuenta**
- En **Perfil de cuenta**, haga clic en **Crear perfil de cuenta** para crear un perfil de conexión de API con su Office 365 o los buzones de correo de Microsoft Exchange:



- Haga clic en **Enviar** y **Registrar** los cambios
- **(Opcional)** El perfil en cadena es una colección de perfiles, sólo se configura el perfil en cadena cuando las cuentas a las que se accede residen en diferentes arrendatarios de diferentes tipos de implementaciones.
- Haga clic en el botón **Crear asignación de dominio** para asignar su perfil de cuenta al dominio receptor. A continuación se muestran los ajustes recomendados:



- Haga clic en **Enviar** y **Registrar** los cambios

Configuración de la protección frente a malware avanzado (AMP) en la política de correo

Una vez que AMP y MAR se han configurado globalmente, ahora puede habilitar los servicios

para las políticas de correo.

- Vaya a **Políticas de correo > Políticas de correo entrante**
- Personalice la configuración de **protección frente a malware avanzado** para una política de correo entrante haciendo clic en el enlace azul en **Protección frente a malware avanzado** para la política que desea personalizar.
- A los efectos de este documento de prácticas recomendadas, haga clic en el botón de opción situado junto a **Habilitar Reputación de Archivos** y seleccione **Habilitar Análisis de Archivos**:



- Se recomienda **incluir un encabezado X con el resultado de AMP en un mensaje**.
- Las tres secciones siguientes le permiten seleccionar la acción que debe realizar el ESA si un adjunto se considera no escaneable debido a errores de mensaje, límite de velocidad o si el servicio AMP no está disponible. La acción recomendada es **Entregar tal cual** con un **texto de advertencia precedido del asunto del mensaje**:

Unscannable Actions on Message Errors	
Action Applied to Message:	Deliver As Is ▼
▼ Advanced	Archive Original Message: <input type="radio"/> No <input checked="" type="radio"/> Yes Modify Message Subject: <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>
Unscannable Actions on Rate Limit	
Action Applied to Message:	Deliver As Is ▼
▼ Advanced	Archive Original Message: <input type="radio"/> No <input checked="" type="radio"/> Yes Modify Message Subject: <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>
Unscannable Actions on AMP Service Not Available	
Action Applied to Message:	Deliver As Is ▼
▼ Advanced	Archive Original Message: <input type="radio"/> No <input checked="" type="radio"/> Yes Modify Message Subject: <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>

- La siguiente sección configurará el ESA para que descarte el mensaje si un adjunto se considera malicioso:

Messages with Malware Attachments:	
Action Applied to Message:	Drop Message ▼
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: MALWARE DETECTED]
▶ Advanced	Optional settings.

- La acción recomendada es poner en cuarentena el mensaje si se envía el archivo adjunto para Análisis de archivos:

Messages with File Analysis Pending:	
Action Applied to Message:	Quarantine ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
<input type="checkbox"/> Advanced Optional settings.	

- (Sólo para la política de correo entrante) Configure las acciones correctivas que se realizarán en el mensaje enviado a los usuarios finales cuando el veredicto de amenaza cambie a malicioso. A continuación se muestran los ajustes recomendados:


Enable Mailbox Auto Remediation (MAR)	
Mailbox Auto Remediation Actions apply only if Account Settings are configured. See System Administrator > Account Settings.	
Action to be taken on message(s) in user's mailbox:	<input type="radio"/> Forward to: <input type="text"/>
	<input checked="" type="radio"/> Delete
	<input type="radio"/> Forward to: <input type="text"/> and Delete

- Haga clic en **Enviar** y **Registrar** los cambios

Integración de SMA con Cisco Threat Response (CTR)

La integración de un módulo de correo electrónico SMA requiere el uso de Security Services Exchange (SSE) a través de CTR. SSE permite que un SMA se registre en Exchange y proporciona permiso explícito para que Cisco Threat Response acceda a los dispositivos registrados. El proceso implica vincular su SMA a SSE a través de un token que se genera cuando está listo para vincularlo.

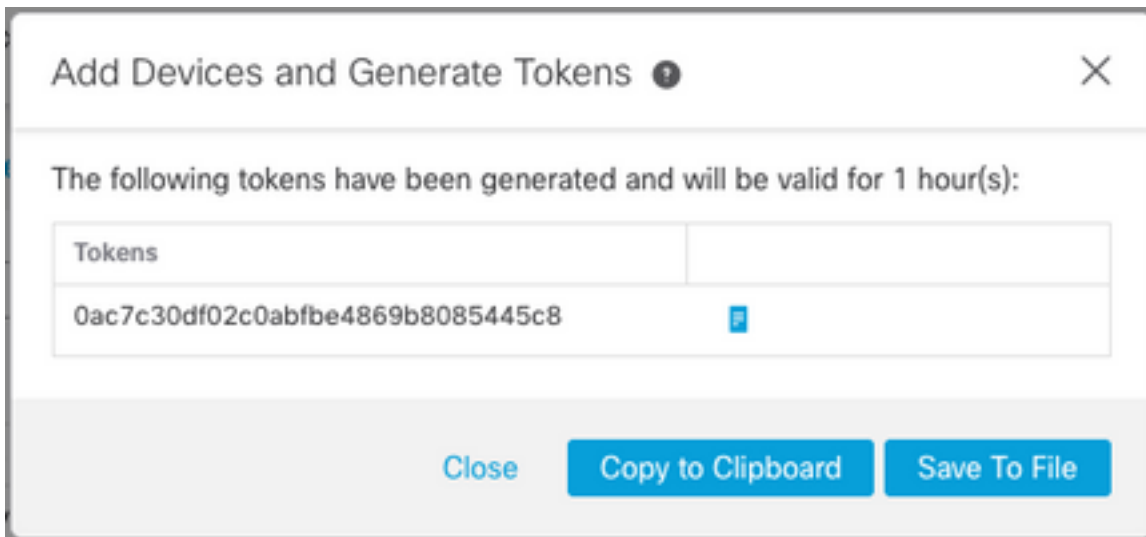
- En el portal CTR (<https://visibility.amp.cisco.com>), inicie sesión con sus credenciales de usuario.
- CTR utiliza un módulo para integrarse con otros productos de seguridad de Cisco, incluido ESA. Haga clic en la pestaña **Módulos**.
- Elija **Devices** y haga clic en **Manage Devices**:


Threat Response
Investigate
Snapshots
Incidents
Beta
Intelligence
Modules

Settings > Devices

Settings Your Account Devices API Clients	<h3>Devices</h3> <div style="display: flex; justify-content: space-around; margin-top: 20px;"> Manage Devices Reload Devices </div>
--	---

- CTR girará la página a SSE.
- Haga clic en el icono **+** para generar un nuevo token y haga clic en **Continuar**.
- Copie el nuevo token antes de cerrar el cuadro:



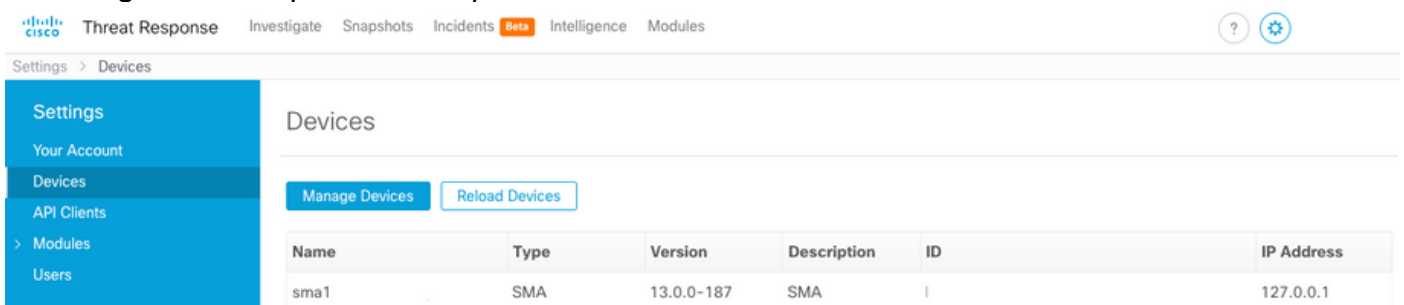
- En su SMA, navegue hasta la pestaña **Dispositivos de administración > Red > Configuración del servicio en la nube**
- Haga clic en **Edit Setting** y asegúrese de que la opción Threat Response esté **Enable**.
- La selección predeterminada para la URL de Threat Response Server es **AMERICAS (api-sse.cisco.com)**. Para los clientes de EUROPA, haga clic en el menú desplegable y elija **EUROPE (api.eu.sse.itd.cisco.com)**:



- Haga clic en **Enviar y Registrar** los cambios
- Pegue la clave token (que ha generado desde el portal CTR) en la configuración de servicios en la nube y haga clic en **Registrar**:



- Se tardará un tiempo en completar el proceso de registro. Vuelva a esta página después de unos minutos para volver a comprobar el estado.
- Vuelva a **CTR > Modules > Device** y haga clic en el botón **Recargar dispositivo** para asegurarse de que el SMA aparezca en la lista:



Conclusión

Este documento tenía por objeto describir las configuraciones predeterminadas o prácticas recomendadas para la protección frente a malware avanzado (AMP) de Cisco en el dispositivo de

seguridad Email Security Appliance. La mayoría de estos ajustes están disponibles tanto en las políticas de correo electrónico entrante como saliente, y se recomienda la configuración y el filtrado en ambas direcciones.