Solución de problemas de integración de XDR y Secure Email Appliance (antes ESA)

Contenido

Introducción

Este documento describe los pasos para realizar un análisis básico y cómo resolver problemas del módulo de integración de XDR y Insights and Secure Email Appliance.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- XDR
- Intercambio de servicios de seguridad
- Correo electrónico seguro

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Intercambio de servicios de seguridad
- XDR
- Secure Email C100V en la versión de software 13.0.0-392

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco Secure Email Appliance (anteriormente conocido como Email Security Appliance) proporciona funciones de protección frente a amenazas avanzadas para detectar, bloquear y remediar las amenazas más rápidamente, evitar la pérdida de datos y proteger la información importante en tránsito con cifrado de extremo a extremo. Una vez configurado, el módulo Secure Email Appliance proporciona detalles asociados con elementos observables. Puede realizar lo siguiente:

- Ver los informes de correo electrónico y los datos de seguimiento de mensajes de varios dispositivos de su organización

- Identificar, investigar y remediar las amenazas observadas en los informes de correo electrónico y las pistas de mensajes
- Resolver las amenazas identificadas rápidamente y proporcionar acciones recomendadas para actuar frente a las amenazas identificadas
- Documentar las amenazas para salvar la investigación y permitir la colaboración de información entre otros dispositivos.

La integración de un módulo Secure Email Appliance requiere el uso de Security Services Exchange (SSE). SSE permite que un dispositivo de correo electrónico seguro se registre en Exchange y usted proporciona permiso explícito para acceder a los dispositivos registrados.

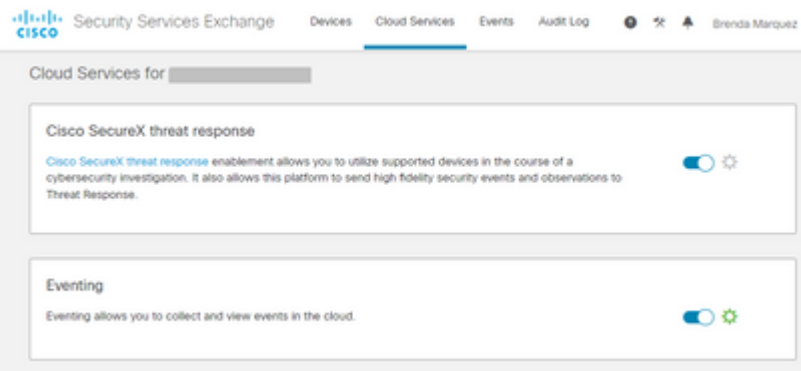
Si desea obtener más información sobre la configuración, consulte este artículo aquí para obtener los detalles del módulo de integración.

Troubleshoot

Para solucionar problemas comunes con la integración de XDR y Secure Email Appliance, puede verificar estos pasos.

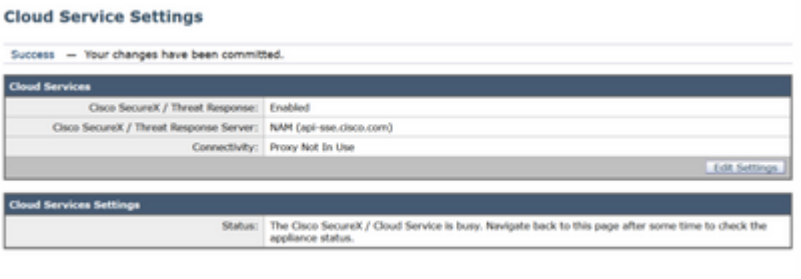
El dispositivo de correo electrónico seguro no se muestra en el XDR ni en el portal de intercambio de servicios de seguridad

Si su dispositivo no se muestra en el portal de SSE, asegúrese de haber habilitado los servicios **XDR Threat Response** y **Event** en el portal de SSE, navegue hasta **Cloud Services** y habilite los servicios, como se muestra en la siguiente imagen:



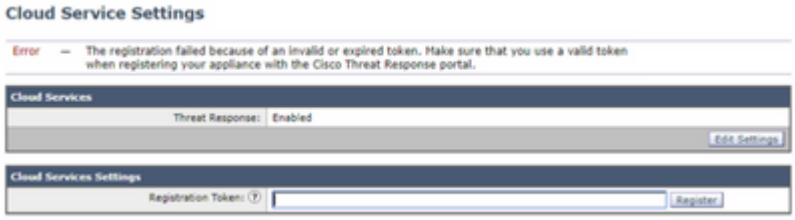
Secure Email no solicita el token de registro

Asegúrese de aplicar los cambios una vez que se haya habilitado el servicio Cisco XDR / Threat Response; de lo contrario, los cambios no se aplicarán a la sección Servicio en la nube del mensaje de correo electrónico seguro. Consulte la imagen que aparece a continuación.



Error de registro debido a un token no válido o caducado

Si ve el mensaje de error: "Error en el registro debido a un token no válido o caducado. Asegúrese de utilizar un token válido para su dispositivo con "Cisco XDR Threat Response portal" en la GUI de Secure Email, como se muestra en la imagen siguiente:



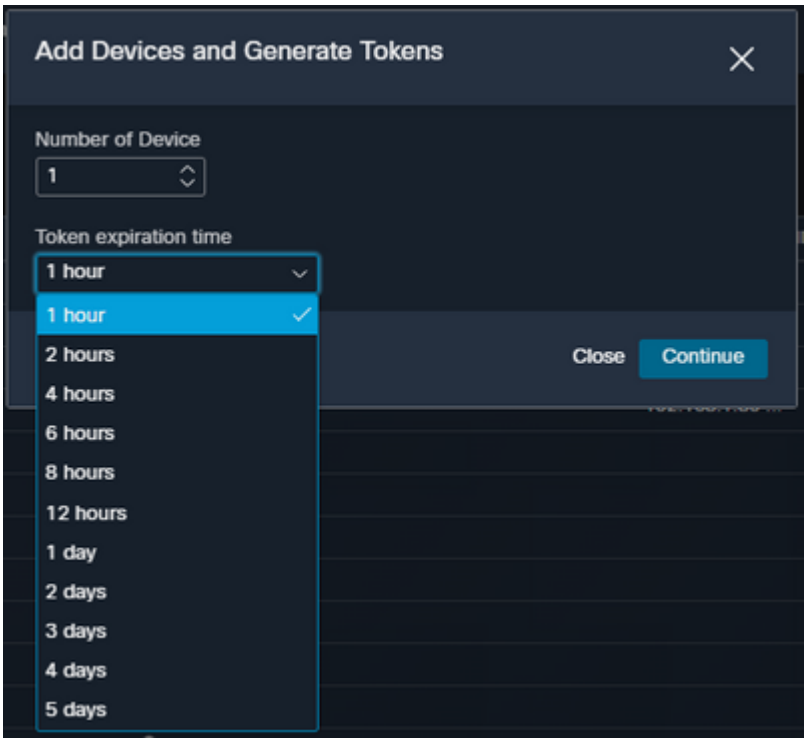
Asegúrese de que el token se genere desde la nube correcta:

Si utiliza la nube de Europa (UE) para el correo electrónico seguro, genere el token de https://admin.eu.sse.itd.cisco.com/

Si utiliza la nube de América (NAM) para correo electrónico seguro, genere el token desde https://admin.sse.itd.cisco.com/

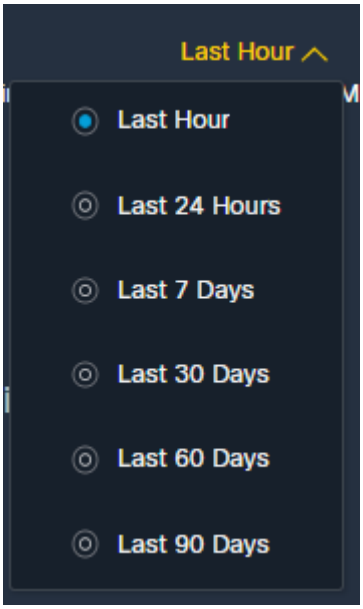
Portal Security Services Exchange (SSE):	NAM: https://admin.sse.itd.cisco.com/ UE: https://admin.eu.sse.itd.cisco.com/
Portal XDR de Cisco	NAM: https://XDR.us.security.cisco.com/ UE: https://XDR.eu.security.cisco.com/
Secure Email Cisco XDR/Servidor de respuesta ante amenazas:	NOMBRE: api-sse.cisco.com UE: api.eu.sse.itd.cisco.com

Además, recuerde que el token de registro tiene una hora de vencimiento (seleccione la hora más conveniente para completar la integración a tiempo), como se muestra en la imagen.



El panel de XDR no muestra información sobre el módulo Secure Email

Puede seleccionar un rango de tiempo más amplio en los cuadros disponibles, desde **Última hora** hasta **Últimos 90 días**, como se muestra en la imagen siguiente.

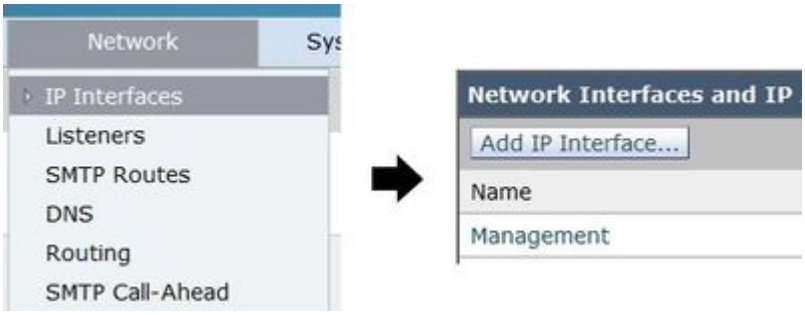


Otros ejemplos podrían ser que vemos el mensaje "Hubo un problema. Inténtelo de nuevo más tarde". o incluso el mensaje de error "Error de cliente en el módulo de correo electrónico seguro: E4017: El dispositivo está desconectado [409]". Verifique si el dispositivo sigue mostrándose como registrado en el portal SSE, probablemente el dispositivo fue dado de baja y ya no está visible. Intente agregar un nuevo módulo al portal XDR.

El módulo de mosaico de Secure Email de XDR muestra el error "Error inesperado en el módulo de Secure Email"

Secure Email requiere la configuración HTTP y HTTPS de la API AsyncOS habilitada en la interfaz de

gestión para comunicarse con el portal XDR/CTR. Para un correo electrónico seguro en las instalaciones, configure esta función desde la GUI del portal de correo electrónico seguro, navegue hasta **Red > Interfaces IP > Interfaz de administración > API AsyncOS** y habilite HTTP y HTTPS, como se muestra en la imagen.

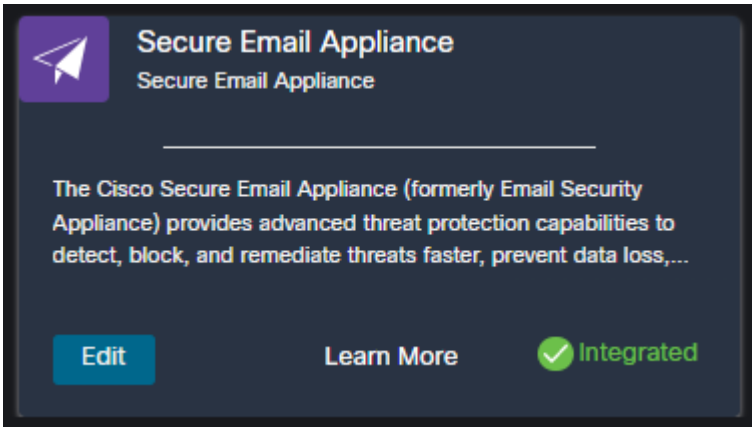


Para un CES (correo electrónico seguro basado en la nube), esta configuración debe realizarla desde el back-end un ingeniero del TAC de correo electrónico seguro; requiere acceso al túnel de asistencia del CES afectado.

Verificación

Una vez que se agrega Secure Email como fuente a Device Insights, puede ver un estado de conexión **API REST** exitoso.

- Puede ver la conexión **API REST** con un estado verde
- Presione en **SYNC NOW** para activar la sincronización completa inicial, como se muestra en la imagen



En caso de que el problema persista con la integración de XDR y Secure Email Appliance, consulte este artículo para recopilar los registros HAR del navegador y póngase en contacto con el servicio de asistencia del TAC para realizar un análisis más profundo.

Información Relacionada

- **Puede encontrar la información de este artículo en este vídeo de integración de XDR y correo electrónico seguro.**
- **Puede encontrar vídeos sobre cómo configurar las integraciones de productos aquí**
- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).