Solução de problemas de XDR e integração do Secure Email Appliance (anteriormente ESA)

Contents

Introdução

Este documento descreve as etapas para executar uma análise básica e como solucionar problemas do módulo de integração do XDR, Insights e Secure Email Appliance.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- XDR
- Security Services Exchange (Troca de serviços de segurança)
- E-mail seguro

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Security Services Exchange (Troca de serviços de segurança)
- XDR
- Secure Email C100V no software versão 13.0.0-392

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Secure Email Appliance (anteriormente conhecido como Email Security Appliance) oferece recursos avançados de proteção contra ameaças para detectar, bloquear e corrigir ameaças mais rapidamente, evitar a perda de dados e proteger informações importantes em trânsito com criptografia de ponta a ponta. Depois de configurado, o módulo Secure Email Appliance fornece detalhes associados aos itens observáveis. Você pode:

- Visualize os relatórios de e-mail e os dados de monitoramento de mensagens de vários dispositivos na sua organização

- Identifique, investigue e corrija as ameaças observadas nos relatórios de e-mail e nos controles de mensagens
- Resolver as ameaças identificadas rapidamente e fornecer ações recomendadas para tomar contra as ameaças identificadas
- Documentar as ameaças para salvar a investigação e permitir a colaboração de informações entre outros dispositivos

A integração de um módulo Secure Email Appliance requer o uso do Security Services Exchange (SSE). O SSE permite que um Secure Email Appliance registre-se no Exchange e você fornece permissão explícita para acessar os dispositivos registrados.

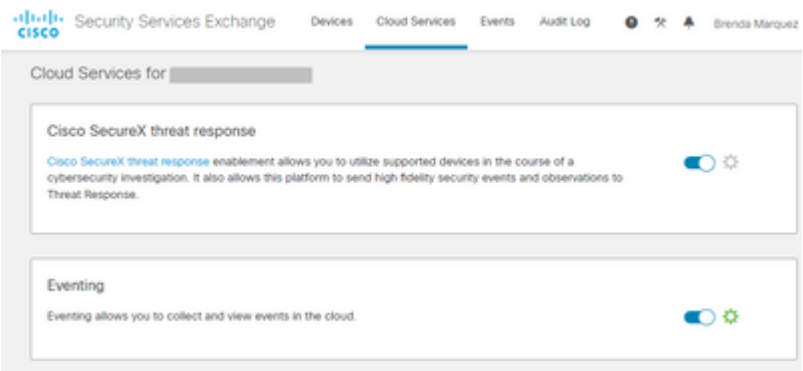
Se você quiser saber mais sobre a configuração, leia este artigo aqui para obter os detalhes do módulo de integração.

Troubleshooting

Para solucionar problemas comuns com a integração do XDR e do Secure Email Appliance, você pode verificar essas etapas.

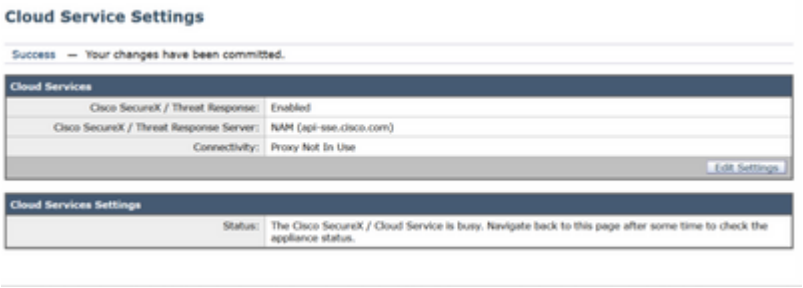
O dispositivo Secure Email não é mostrado no XDR nem no portal Security Services Exchange

Se o seu dispositivo não for mostrado no portal SSE, certifique-se de ter habilitado os serviços **Resposta a ameaças XDR** e **Evento** no portal SSE, navegue até **Serviços em nuvem** e habilite os serviços, como a imagem abaixo:



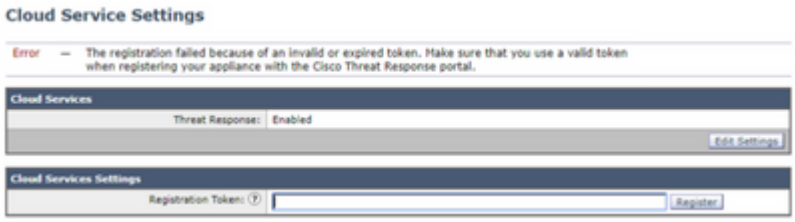
O Secure Email não solicita o token de Registro

Certifique-se de confirmar as alterações, depois que o serviço Cisco XDR / Threat Response tiver sido habilitado; caso contrário, as alterações não serão aplicadas à seção Cloud Service no e-mail seguro, veja a imagem abaixo.



Falha no registro devido a um token inválido ou expirado

Se você vir a mensagem de erro: "The registration failed due of an invalid or expiry token (Falha no registro devido a um token inválido ou expirado). Certifique-se de usar um token válido para o seu dispositivo com o "portal de resposta a ameaças do Cisco XDR" na GUI de e-mail seguro, como na imagem abaixo:



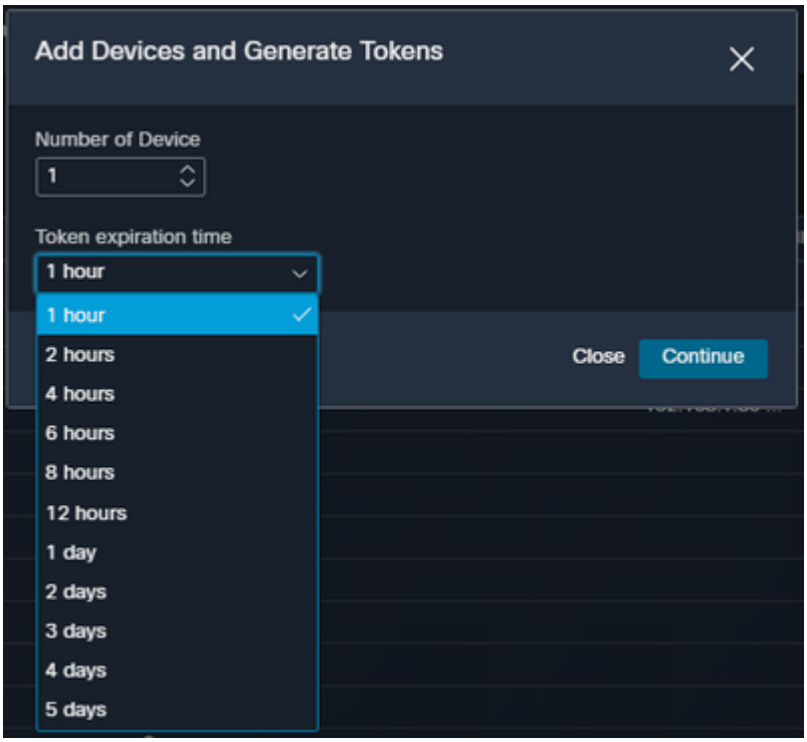
Certifique-se de que o token seja gerado a partir da nuvem correta:

Se você usa a nuvem da Europa (EU) para e-mail seguro, gere o token de https://admin.eu.sse.itd.cisco.com/

Se você usa a nuvem das Américas (NAM) para e-mail seguro, gere o token de https://admin.sse.itd.cisco.com/

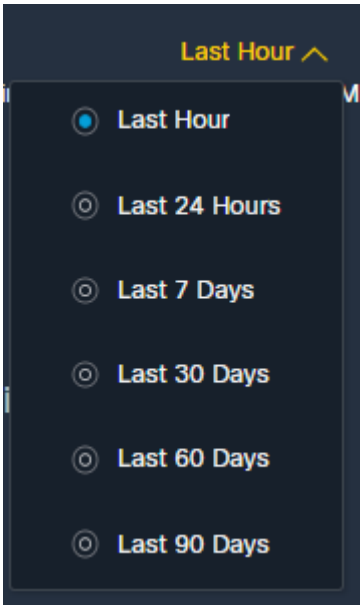
Portal Security Services Exchange (SSE):	NOME: https://admin.sse.itd.cisco.com/ UE: https://admin.eu.sse.itd.cisco.com/
Portal Cisco XDR	NOME: https://XDR.us.security.cisco.com/ UE: https://XDR.eu.security.cisco.com/
E-mail seguro Cisco XDR / Servidor de resposta a ameaças:	NOME: api-sse.cisco.com UE: api.eu.sse.itd.cisco.com

Além disso, lembre-se de que o token de Registro tem um tempo de expiração (selecione o tempo mais conveniente para concluir a Integração em tempo), como mostrado na imagem.



O Painel XDR não exibe informações sobre o módulo Secure Email

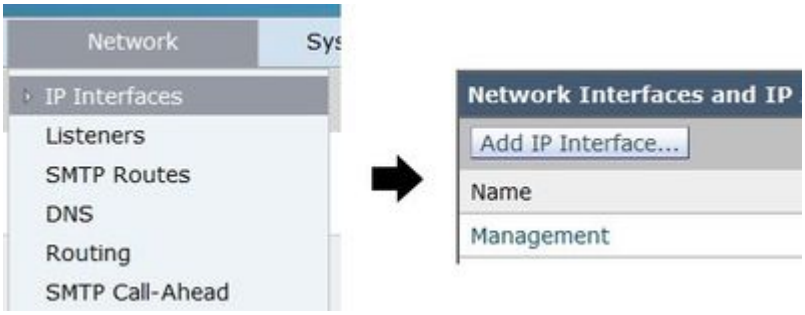
Você pode selecionar um intervalo de tempo mais amplo nos blocos disponíveis, de **Última Hora** a **Últimos 90 Dias**, como na imagem abaixo.



Outros exemplos podem ser a mensagem "Houve um problema. Tente novamente mais tarde." ou até mesmo a mensagem de erro "There was a client error in the Secure Email module: E4017: Device is offline [409]" (Houve um erro de cliente no módulo de e-mail seguro: E4017: o dispositivo está off-line [409]). Verifique se o dispositivo ainda é mostrado como registrado no portal SSE, provavelmente o dispositivo teve o registro cancelado e não está mais visível. Tente adicionar um novo módulo ao portal XDR.

O módulo lado a lado do Secure Email XDR exibe o erro "There was an expected Error on the Secure Email module" (Ocorreu um erro inesperado no módulo Secure Email)

O Secure Email requer a configuração HTTP e HTTPS da API do AsyncOS habilitada na interface de gerenciamento para se comunicar com o portal XDR/CTR. Para um Secure Email local, configure esse recurso na GUI do portal Secure Email, navegue para **Network > IP Interfaces > Management interface > AsyncOS API** e habilite HTTP e HTTPS, como mostrado na imagem.

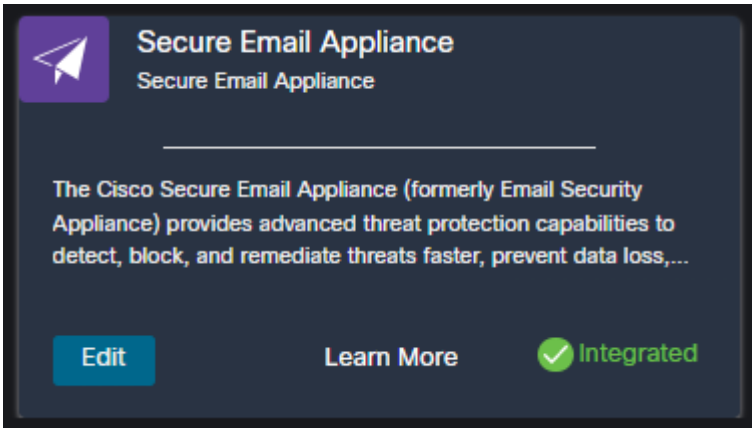


Para um CES (Cloud-Based Secure Email, e-mail seguro baseado em nuvem), essa configuração precisa ser feita no back-end por um engenheiro do Secure Email TAC; ela requer acesso ao túnel de suporte do CES afetado.

Verificar

Depois que o Secure Email for adicionado como uma fonte para o Device Insights, você poderá ver um status de conexão da **API REST** bem-sucedida.

- Você pode ver a conexão da **API REST** com um status verde
- Pressione **SYNC NOW** para acionar a sincronização completa inicial, como mostrado na imagem



Caso o problema persista com a integração do XDR e do Secure Email Appliance, consulte este artigo para coletar registros HAR do navegador e entre em contato com o suporte TAC para executar uma análise mais profunda.

Informações Relacionadas

- **Você pode encontrar as informações neste artigo neste vídeo XDR e Secure Email Integration.**
- **Você pode encontrar vídeos sobre como configurar suas integrações de produtos aqui**
- **Suporte Técnico e Documentação - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.