Solução de problemas de integração do SecureX e 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 SecureX, Insights e Secure Email Appliance.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SecureX
- 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)
- SecureX 1.54
- 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.

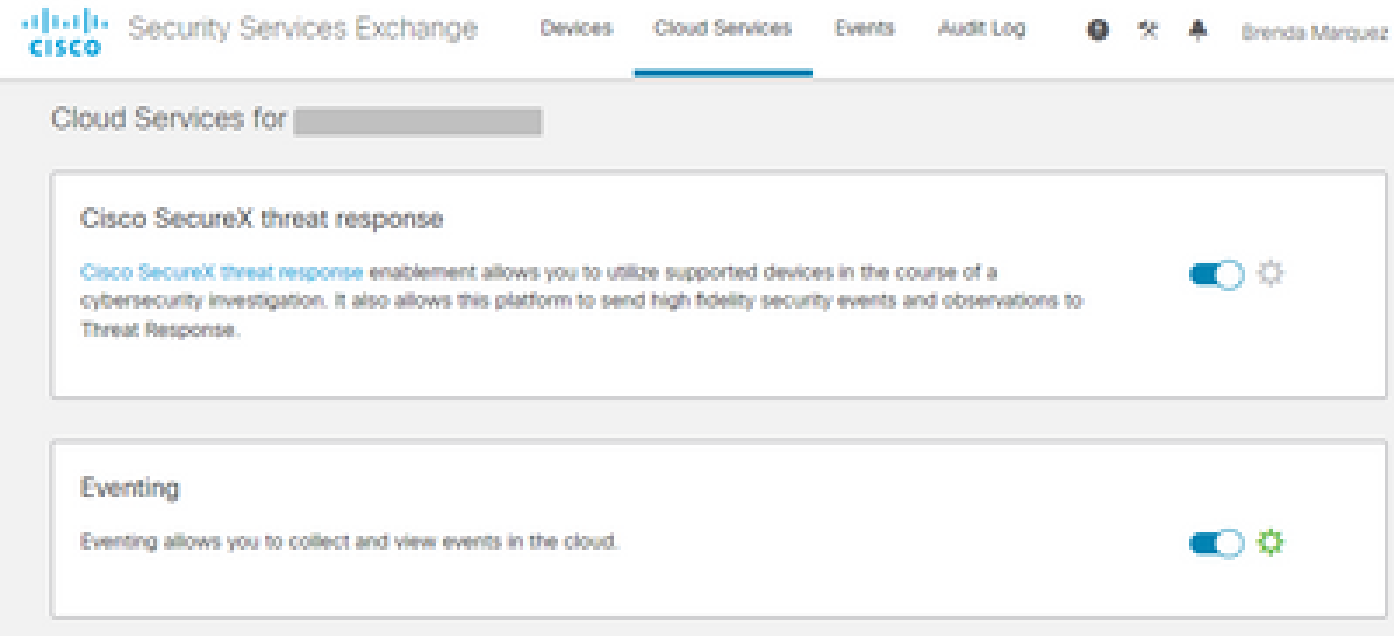
Se você quiser saber mais sobre a configuração, leia este artigo aqui para obter os detalhes do módulo de integração.

Troubleshooting

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

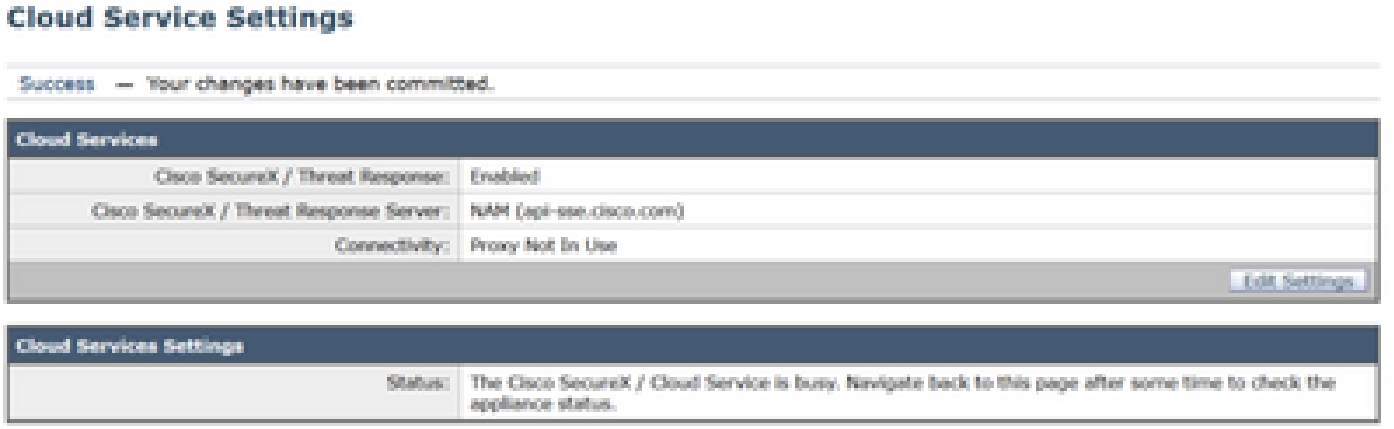
O dispositivo Secure Email não é mostrado no portal SecureX nem no portal Security Services Exchange

Se o seu dispositivo não for mostrado no portal SSE, certifique-se de ter habilitado os serviços SecureX Threat Response e Event no portal SSE, navegue até Cloud Services e habilite os serviços, como a imagem abaixo:



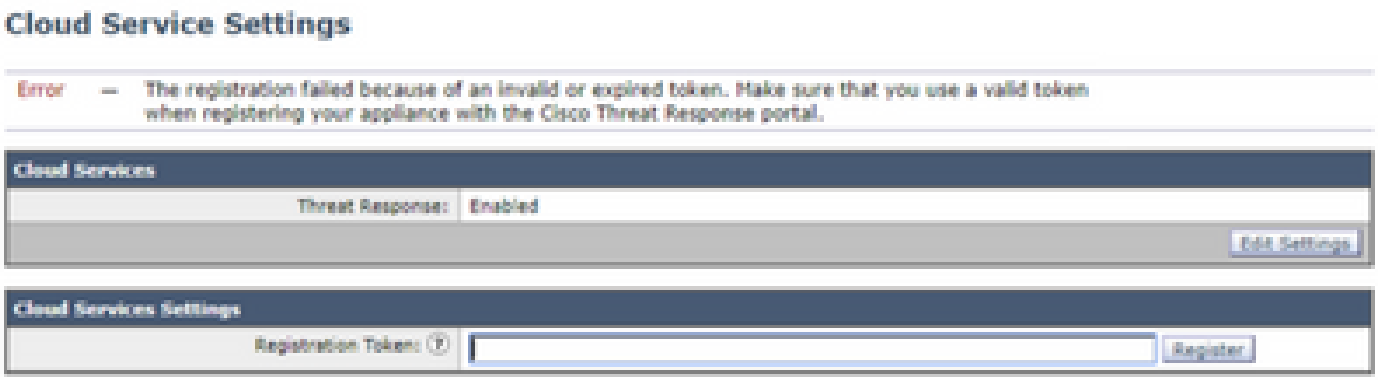
O Secure Email não solicita o token de Registro

Certifique-se de confirmar as alterações, depois que o serviço Cisco SecureX / 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 da Cisco" na GUI de e-mail seguro, como na imagem abaixo:



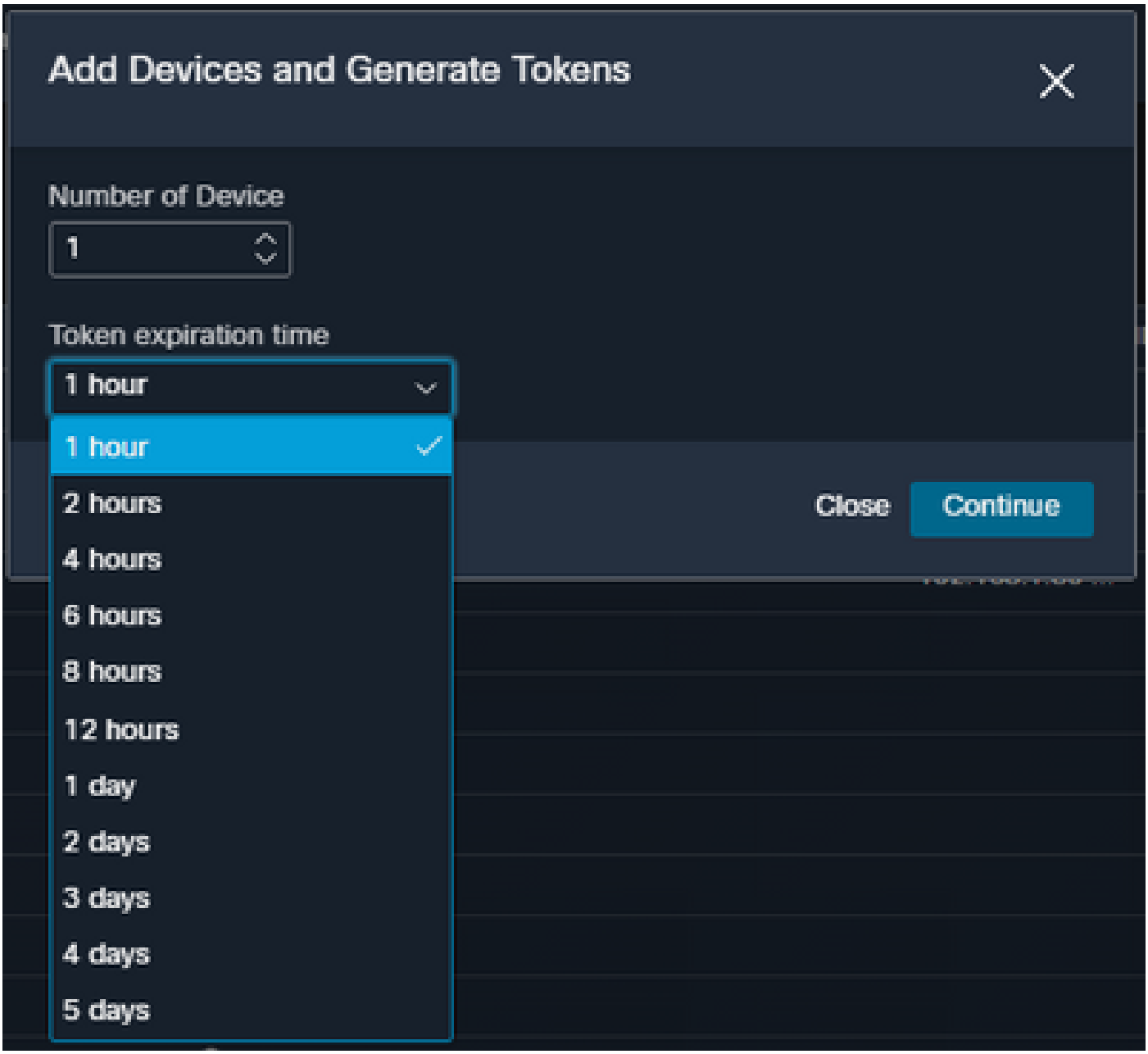
Certifique-se de que o token seja gerado a partir da nuvem correta:

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/

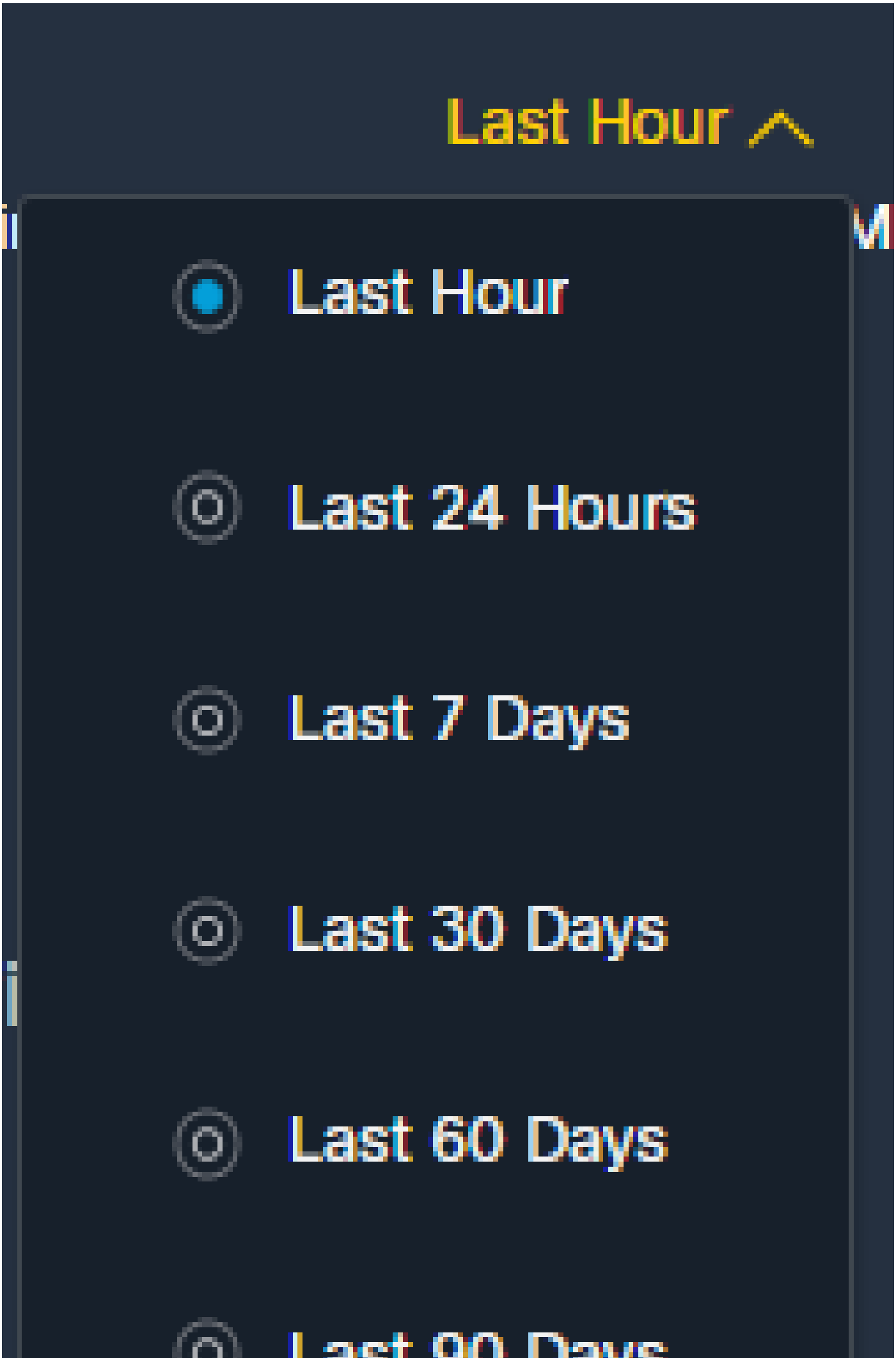
Portal Security Services Exchange (SSE):	NOME: https://admin.sse.itd.cisco.com/ UE: https://admin.eu.sse.itd.cisco.com/
Portal Cisco SecureX	NOME: https://securex.us.security.cisco.com/ UE: https://securex.eu.security.cisco.com/
Secure Email Cisco SecureX / Servidor de resposta a ameaças:	NOME: api-sse.cisco.com 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 SecureX Dashboard não exibe informações do 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.


Last Hour
Last Hour
Last 24 Hours
Last 7 Days
Last 30 Days
Last 60 Days

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 SecureX and 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.