XDRとSecure Email Appliance（旧称ESA）の統合のトラブルシューティング

内容

概要

このドキュメントでは、基本的な分析を実行する手順と、XDRとInsightsおよびSecure Email Appliance統合モジュールのトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- XDR
- セキュリティサービス交換
- 安全な電子メール

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- セキュリティサービス交換
- XDR
- ソフトウェアバージョン13.0.0-392上のSecure Email C100V

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Secure Email Appliance（旧称Eメールセキュリティアプライアンス）は、エンドツーエン

ドの暗号化を使用して、脅威の検出、ブロック、修復を高速化し、データ損失を防止し、転送中の重要な情報を保護する高度な脅威保護機能を提供します。設定が完了すると、Secure Email Applianceモジュールが監視対象に関連する詳細情報を提供します。次の操作を実行できます。

- 組織内の複数のアプライアンスからのEメールレポートおよびメッセージトラックデータを表示する
- 電子メールレポートおよびメッセージトラックで見られる脅威を特定、調査、および修復する
- 特定された脅威を迅速に解決し、特定された脅威に対して推奨されるアクションを提供する
- 脅威を文書化して調査の手間を省き、他のデバイス間での情報のコラボレーションを可能にする

Secure Eメールアプライアンスモジュールを統合するには、Security Services Exchange(SSE)を使用する必要があります。SSEを使用すると、Secure Email ApplianceをExchangeに登録し、登録したデバイスにアクセスするための明示的な権限を付与できます。

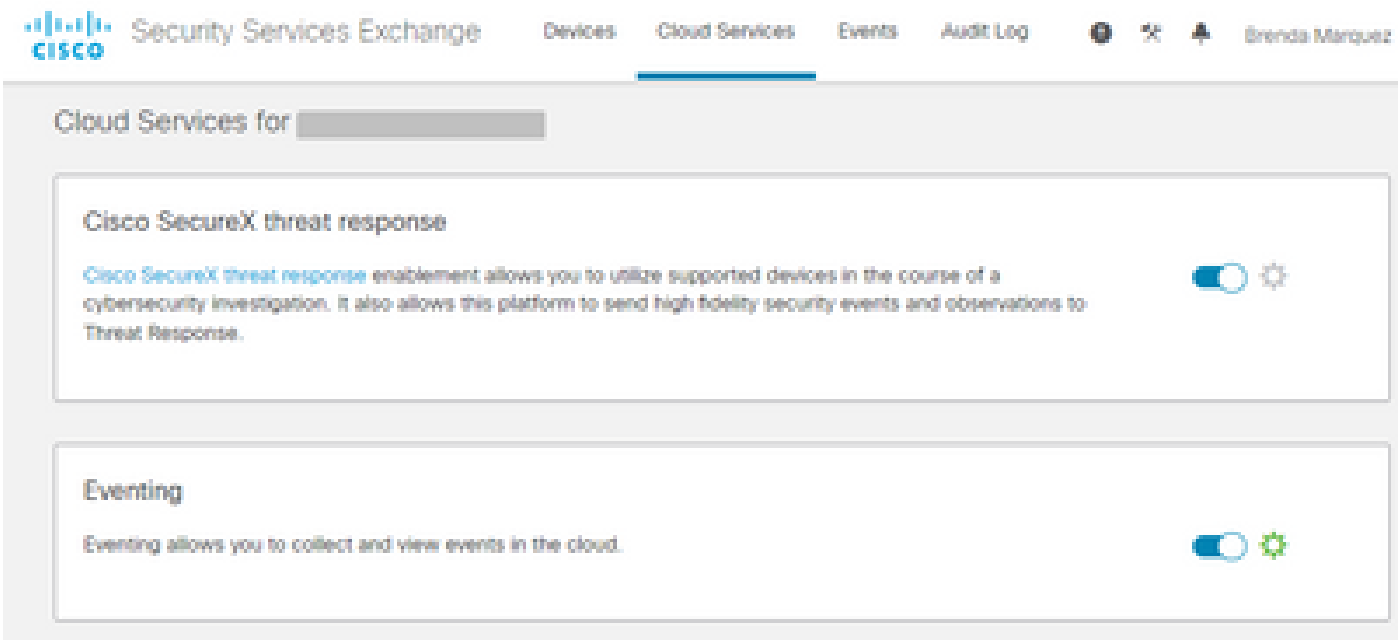
設定の詳細については、この記事の統合モジュールの詳細を参照してください。

トラブルシュート

XDRとセキュアEメールアプライアンス(SEA)の統合に関する一般的な問題をトラブルシューティングするには、次の手順を確認できます。

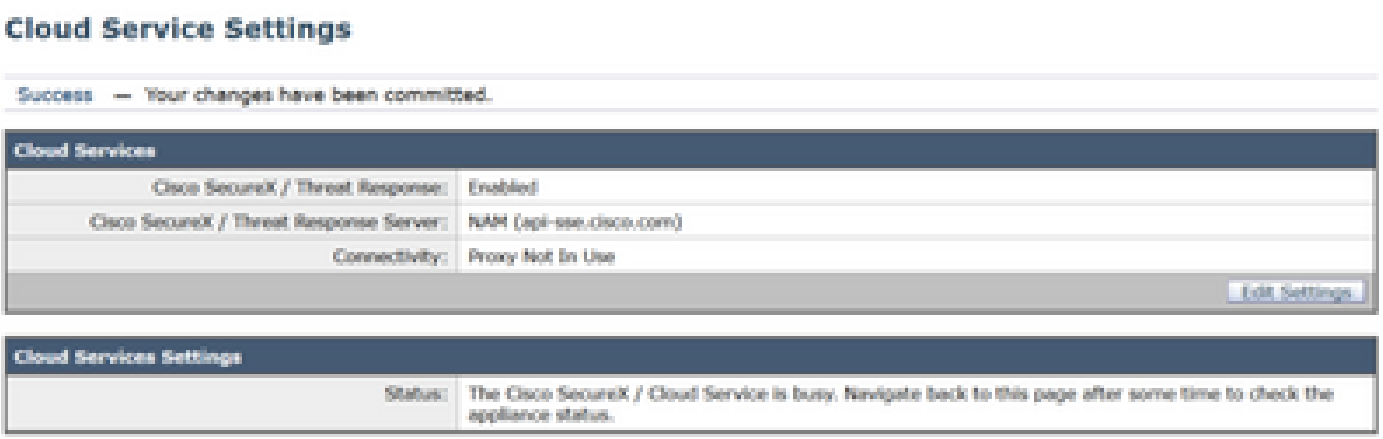
セキュアな電子メールデバイスがXDRまたはSecurity Services Exchangeポータルに表示されない

デバイスがSSEポータルに表示されない場合は、次の図のように、SSEポータルでXDR Threat ResponseおよびEventサービスを有効にし、Cloud Servicesに移動して、サービスを有効にしてください。



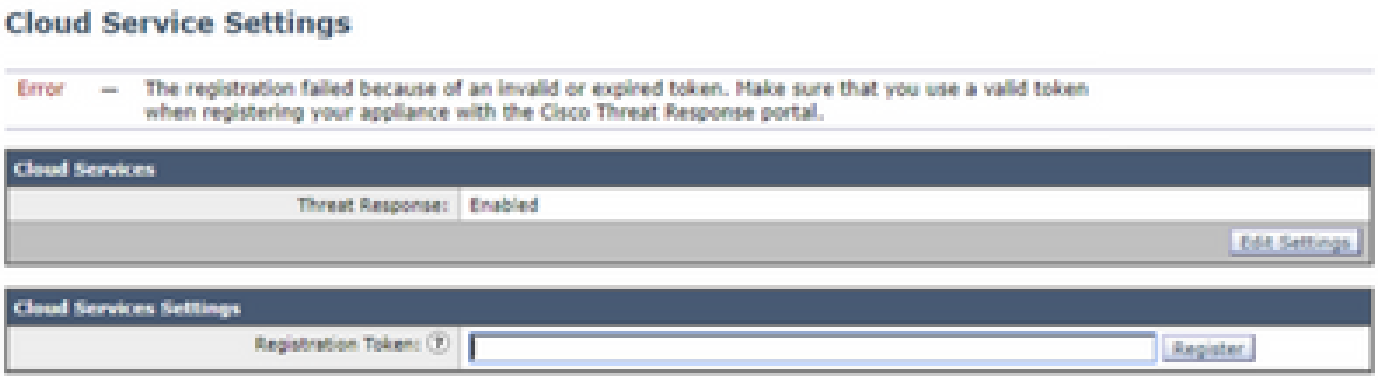
セキュリティで保護された電子メールが登録トークンを要求しない

Cisco XDR/Threat Responseサービスを有効にした後、変更を必ずコミットしてください。そうしないと、変更はセキュアEメールのCloud Serviceセクションに適用されません。次の図を参照してください。



トークンが無効または期限切れのため、登録できませんでした

エラーメッセージ「The registration failed because of an invalid or expired token.下図のように、Secure Email GUIでCisco XDR Threat Response portal」を使用して、アプライアンスに有効なトークンを使用していることを確認します。



トークンが正しいクラウドから生成されていることを確認してください。

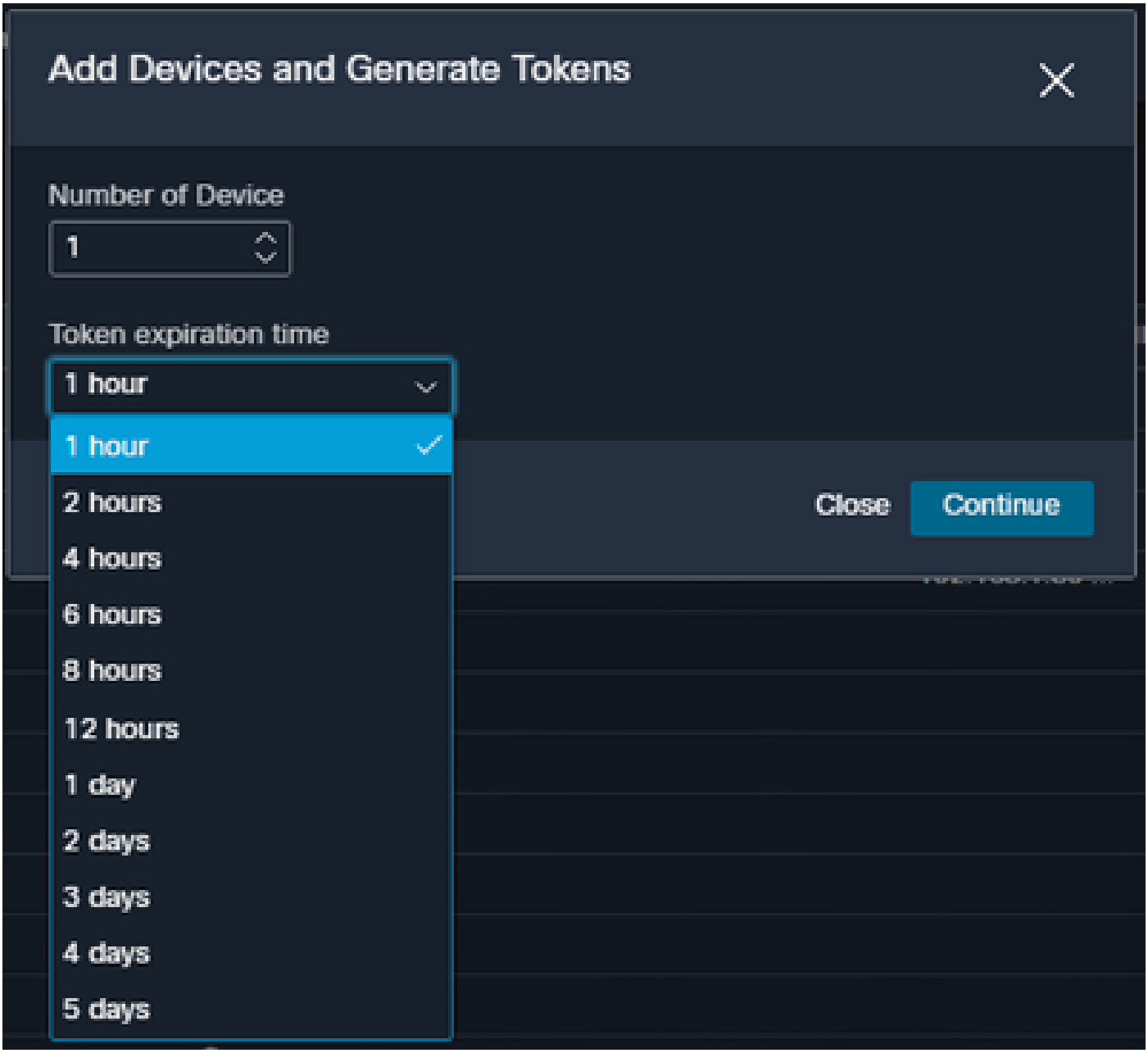
欧州(EU)のクラウドを使用してEメールを保護する場合は、https://admin.eu.sse.itd.cisco.com/からトークンを生成します。

セキュアメールに南・北・中央アメリカ(NAM)クラウドを使用する場合は、https://admin.sse.itd.cisco.com/からトークンを生成します。

Security Services Exchange(SSE)ポータル	NAM:https://admin.sse.itd.cisco.com/ EU:https://admin.eu.sse.itd.cisco.com/

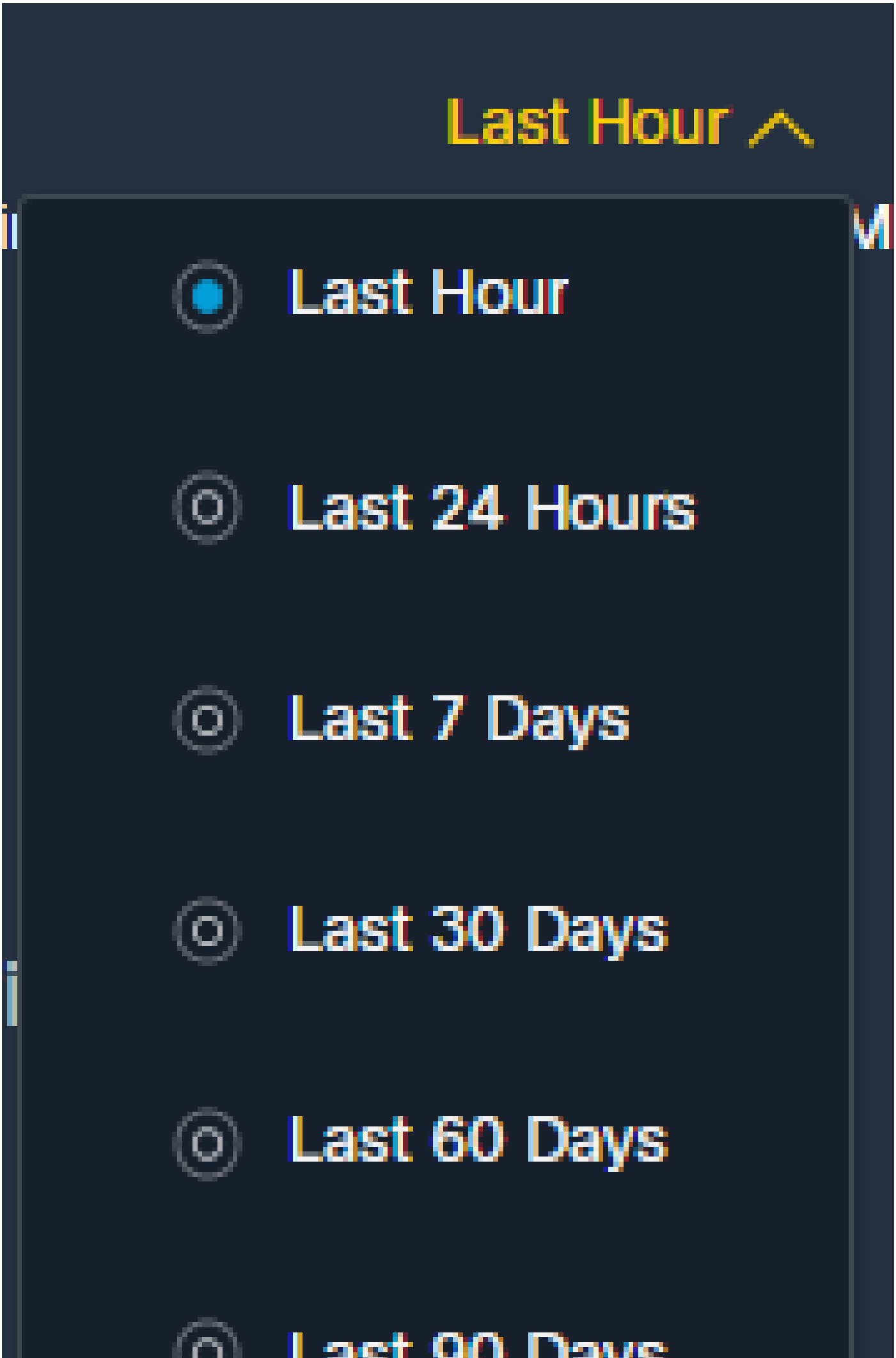
Cisco XDRポータル	NAM:https://XDR.us.security.cisco.com/ EU:https://XDR.eu.security.cisco.com/
セキュアな電子メールCisco XDR/Threat Response Server:	NAM:api-sse.cisco.com EU:api.eu.sse.itd.cisco.com

また、図に示すように、登録トークンには有効期限があります（統合を完了するのに最も便利な時間を選択してください）。



XDRダッシュボードに、セキュリティで保護された電子メールモジュールに関する情報が表示されない

次の図に示すように、使用可能なタイルで過去1時間から過去90日までの幅広い時間範囲を選択できます。


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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。