[Stealthwatch Management Console Secure X]リボンに認証エラーが表示される

内容

概要

このドキュメントでは、StealthWatch Management Center Secure Xリボンで工ラーが発生する理由と、この問題の解決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。

- Cisco Secure X
- Cisco Threat Response（CTR）
- Cisco StealthWatch 管理コンソール

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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、初期（デフォルト）設定の状態から起動しています。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。

問題

Secure X設定（Secure XおよびSSE）でSecure Xへの正しく設定された接続が表示されているにもかかわらず、SMCリボンにエラーが表示される

解決方法

リボンを使用するために必要な追加の特権があるため、APIクレデンシャルは、選択してSMCに適用した拡張スコープで再生成する必要があります。

ステップ1:https://visibility.amp.cisco.com/settings/apiClientsに移動します

ステップ2：プロンプトが表示されたら、CTR/Secure Xへのログインに使用するクレデンシャルでログインします

ステップ3:[**Generate API Client**]をクリックします

ステップ4：対応するフィールドに必要な情報を入力します。

Client Name：*任意の記述名*

範囲：*すべてのスコープが必要です*

説明:*オプションの詳細*

ステップ5:[**Add New Client**]をクリックします

ステップ6：生成されたクライアントAPI IDとキーを[SMC Secure X Settings]ページに入力します

https://
ステップ7:SMCダッシュボードに移動します。Secure X Dashboardは期待どおりに機能します。