設定

- 設定 （1 ページ）

設定

アプリケーションを設定するには、ナビゲーションメニューの [設定（Settings）] をクリックします。

- [Cisco SecureXの統合（Cisco SecureX Integration）]：SecureX アカウントのリージョンを選択し、[承認（Authorize）] をクリックして、SecureXアカウントにサインインすることで、SecureX との統合を有効にします。
- [デバイスアカウント（Device Accounts）] - 1 つ以上のソースプロキシデバイスから分析用グローバル脅威アラートシステムにログファイルのテレメトリデータをアップロードします。このサービスにアクセスするには、外部テレメトリ機能を有効にして、企業用にプロビジョニングする必要があります。外部テレメトリ機能がない場合は、Cisco Security アカウントチームにお問い合わせください。「プロキシデバイスのアップロード」を参照してください。
- [抑制されたネットワーク（Ignored Networks）]：無視する IPv4 アドレスとネットワーク範囲をリストしてアラートを非表示にします。これは、ゲストネットワークやその他の重要度の低いネットワークからのアラートなど、不要なアラートをフィルタ処理し抑制する場合に役立ちます。インシデントのリストから非表示にするホストの IPv4 アドレス、サブネット、または IPv4 アドレス範囲（例：10.100.10.1、10.100.10.0/24、10.100.10.1-10.100.10.254）を入力します。
- [Global Threat Alerts API] - REST API を使用して、さらなる分析、インシデント対応、およびデータアーカイブのために、グローバル脅威アラートで検出されたインシデントに関する情報を SIEM クライアントまでプルします。
- [電子メール通知（Email Notifications）] - 新規および更新された脅威のサマリーを送信する電子メール アドレスを 24 時間ごとに入力します。
- [リリースノート（Release Notes）]：機能の更新、変更、および修正の概要を示します（このガイドで後述）。

設定

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。