Cisco Secure Network Analytics

Cisco SecureX 統合ガイド 7.4.2

目次

はじめに 4
最新情報 4
7.3 から 7.4 へのアップグレード 4
SecureX 地域クラウド 5
地域クラウドの選択に関する注意事項と制約事項 5
Cisco Secure Network Analytics のデータと SecureX 6
SecureX リボンとメニューについて 6
SecureX リボン 6
SecureX メニュー 6
SecureX ダッシュボードの Secure Network Analytics タイルについて 7
Cisco SecureX Threat Response への Secure Network Analytics アラームの送信について 9
SecureX の Secure Network Analytics エンリッチメントデータについて 10
Cisco Threat Intel モデルについて 10
Secure Network Analytics アラームの CTIM オブジェクトへの変換について 11
Secure Network Analytics セキュリティイベントの CTIM オブジェクトへの変換について 11
Cisco Cloud アカウント 12
SecureX へのアクセスに必要なアカウント 12
SecureX にアクセスするためのアカウントの作成 12
組織のシスコ セキュリティアカウントへのアクセスの管理 12
Cisco Secure Network Analytics と SecureX の設定 13
SecureX 統合の設定 13
前提条件 13
手順 14
SecureX のリボンとメニューの承認 17
SecureX のリボンからの承認 17
[SecureXの設定(SecureX Configuration)] ページからの承認 18
現在の SecureX リボンの承認解除 18
Threat Response インシデントアクションの設定 18
検証 19
Cisco Cloud での Manager の登録 20
自動登録手順 21
アカウントのリンク 21
手動登録手順 22

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

SecureX での Cisco Secure Network Analytics 統合モジュールの設定 24
前提条件 24
手順 24
Secure Network Analytics タイルを使用した SecureX ダッシュボードの設定 26
既知の問題と制限事項 **28**
サポートへの問い合わせ **29**
変更履歴 **30**

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

はじめに

Cisco SecureX は、複数の製品やソースから集約されたデータを使用して、脅威の検出、調査、分析、対応を行うのに役立つ Cisco Cloud のプラットフォームです。

このような統合により、Secure Network Analytics（旧 Stealthwatch）で次のことが可能になります。

- SecureX ダッシュボードの（Stealthwatch と表示されている）Secure Network Analytics タイルを使用して、主要な業務メトリクスをモニターする。
- SecureX のメニューを使用して、他のシスコセキュリティおよびサードパーティの統合にピボットする。
- SecureX のリボンへのアクセスを提供する。
- Cisco SecureX Threat Response（旧 [Cisco Threat Response]）プライベート インテリジェンス ストアに Secure Network Analytics アラームを送信する。
- Threat Response ワークフローの調査コンテキストを強化するために、SecureX で Secure Network Analytics からのセキュリティイベントを要求できるようにする。

SecureX の詳細については、次のリンクを参照してください。

- SecureX Web サイト
- SecureX マニュアル

最新情報

v7.4.0 では、Cisco Stealthwatch Enterprise 製品のブランド名を Cisco Secure Network Analytics に変更しました。詳細なリストについては、リリース ノート を参照してください。このガイドでは、以前の製品名である Stealthwatch が必要に応じて明確さを維持するために使用され、Stealthwatch Management Console や SMC などの用語も使用されています。

現在、SecureX では Secure Network Analytics は Stealthwatch Enterprise と表示されていることに注意してください。

7.3 から 7.4 へのアップグレード

7.3 の SecureX の設定で Cisco SecureX Threat Response に Secure Network Analytics アラームを送信するオプションが有効になっている場合は、アラームを送信し続けるように Threat Response Incident のアクションが自動的に設定されます。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

SecureX 地域クラウド

地域	リンク	サポートされる Secure Network Analytics の統合
北米	• Threat Response Web コンソール：https://visibility.amp.cisco.com • SecureX ポータル：https://securex.us.security.cisco.com	• SecureX メニュー • SecureX リボン • Cisco SecureX Threat Response への Secure Network Analytics アラームの送信 • Secure Network Analytics セキュリティイベントでの強化
欧州	• Threat Response Web コンソール：https://visibility.eu.amp.cisco.com • SecureX ポータル：https://securex.eu.security.cisco.com	• SecureX メニュー • SecureX リボン • Cisco SecureX Threat Response への Secure Network Analytics アラームの送信 • Secure Network Analytics セキュリティイベントでの強化
アジア（APJC）	• Threat Response Web コンソール：https://visibility.apjc.amp.cisco.com • SecureX ポータル：https://securex.apjc.security.cisco.com	• SecureX メニュー • SecureX リボン • Cisco SecureX Threat Response への Secure Network Analytics アラームの送信

地域クラウドの選択に関する注意事項と制約事項

- 可能な場合は、Secure Network Analytics の導入環境に最も近い地域クラウドを使用してください。
- 異なるクラウド内のデータを集約またはマージすることはできません。
- 複数の地域からデータを集約する必要がある場合は、すべての地域のデバイスが同じ地域のクラウドにデータを送信する必要があります。
- 各地域のクラウド上にアカウントを作成できます。各クラウドのデータは区分されます。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Cisco Secure Network Analytics のデータと SecureX

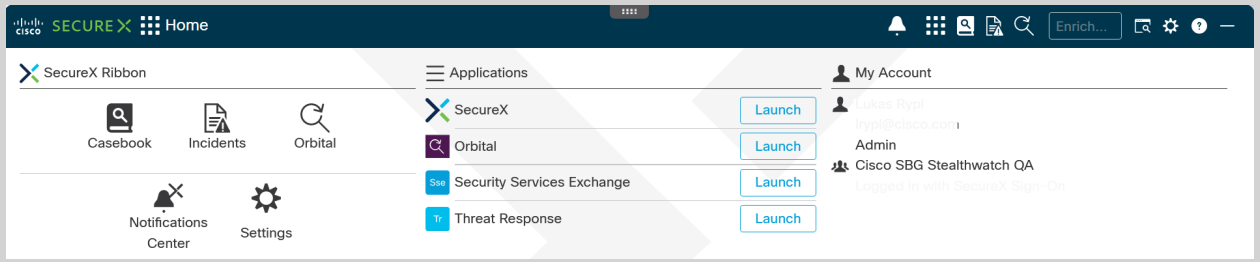
SecureX リボンとメニューについて

SecureX リボン

SecureX のリボンは、ページの下部にある Cisco Secure Network Analytics Manager（旧 Stealthwatch Management Console）の UI に表示されるウィジェットです。このリボンは、可視性の統合、自動化の実現、インシデント対応ワークフローの迅速化、脅威ハンティングの改善を行う一連の分散型機能を提供します。これらの機能は、リボン内にアプリケーション（アプリ）とツールの形式で表示されます。

リボンを設定すると、Manager の任意のページから、インシデントとケースブックの管理、Observable の検索、調査と脅威ハンティングの開始、SecureX と統合された他の製品へのアクセスなどを行うことができます。

リボンを設定するには、「SecureX のリボンとメニューの承認」の項を参照してください。



リボンの詳細については、『Cisco SecureX Getting Started Guide』の「Cisco SecureX Ribbon」の項を参照してください。

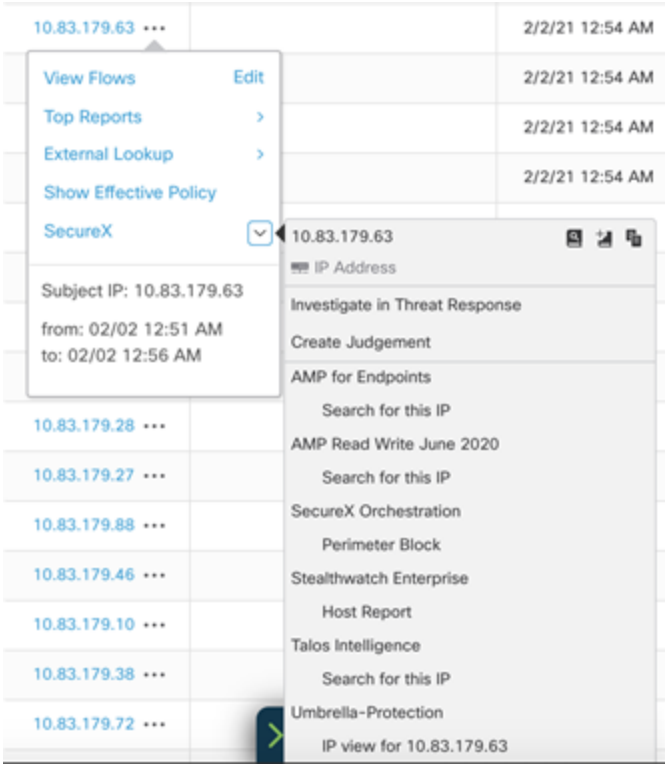
SecureX メニュー

SecureX によって、他のシスコ製品のデータとともにシスコの脅威インテリジェンスリソースを活用できる中心的なアクセスポイントが提供されます。

メニューは、SecureX と統合されている他の製品とグループにリンクしています。メニューで一部のアクションを直接実行することも、統合製品にピボットして追加のアクションを実行することもできます。

Secure Network Analytics では、SecureX 統合の設定後に、Manager の該当する IP アドレスの横にある ••• （[省略記号（Ellipsis）]）アイコンをクリックすることでメニューを使用できます。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



メニューから使用できる機能の詳細については、「SecureX menu」のヘルプトピックを参照してください。

メニューのヘルプを表示するには、SecureX にログインする必要があります。

SecureX ダッシュボードの Secure Network Analytics タイルについて

(Stealthwatch と表示されている)次の Secure Network Analytics タイルは、SecureX ダッシュボードで使用できます。

タイル名	説明	使用可能時間帯	ピボット先
上位のアラームホスト	最後のリセット時以降ネットワーク上でアクティブになっていて、アラーム重大度別にソートされた上位 7 位までの内部ホストを提供する。	直近の 24 時間	ホストレポート

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

タイル名	説明	使用可能時間帯	ピボット先
カテゴリ別のホストのアラーム	最後のリセット時以降ネットワーク上でアクティブになっていて、アラーム重大度別にソートされた上位 7 位までの内部ホスト。	直近の 24 時間	ネットワーク セキュリティ ダッシュボード
カウント別の上位のアラーム	カウント別の上位 10 位のアラームを表す。	直近の 24 時間 過去 7 日	ネットワーク セキュリティ ダッシュボード
可視性アセスメント	内部ネットワークスキャナ、Remote Access 侵害、感染の可能性があるマルウェア、脆弱なプロトコルサーバー、DNS リスクなど、可視性アセスメントカテゴリ内のホスト数。	直近の 24 時間 過去 7 日	可視性アセスメント ダッシュボード
ネットワークの可視性	ホスト数とトラフィック量の統計情報を提供する。	直近の 24 時間 過去 7 日	可視性アセスメント ダッシュボード
トラフィック別の上位の内部ホストグループ	相互に通信されたトラフィック別の上位 10 位の内部ホストグループ。	直近の 12 時間	内部ホストグループのホストグループレポート
トラフィック別の上位のホストグループ	内部ホストグループと通信したトラフィック別の上位 10 位の外部ホストグループ。	直近の 12 時間	内部ホストグループのホストグループレポート

（Stealthwatch と表示されている）Secure Network Analytics を使用して SecureX ダッシュボードを設定する方法については、「Secure Network Analytics タイルを使用した SecureX ダッシュボードの設定」の項を参照してください。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Cisco SecureX Threat Response への Secure Network Analytics アラームの送信について

SecureX 統合を設定すると、アラームメタデータから作成された、対応する Sighting、Observable、および Indicator オブジェクトを持つ Incident として、Secure Network Analytics アラームから Cisco SecureX Threat Response プライベート インテリジェンス ストアにシステムを昇格できるようになります。

この情報は、Incident から派生した対応する Sighting および Indicator として調査プロセス時に Incident Manager 内で、また、Threat Response の Web コンソール内で使用できます。

対応管理の Threat Response インシデントアクションでは、一般的なアクションパラメータの他に次のオプションを設定できます。

- [Incident信頼度レベル(Incident Confidence Level)]: Cisco SecureX Threat Response に送信される Incident に設定する信頼度レベルを選択できます。
- [新しいTargetエンティティの作成(Create a new Target entity)]: Secure Network Analytics が Cisco SecureX Threat Response の Target としてアラームからホストを指定できるようにします。詳細については、「Secure Network Analytics アラームの CTIM オブジェクトへの変換について」の項を参照してください。
    - Cisco SecureX Threat Response に送信する必要があるホスト情報を決定するときに内部 IP アドレスのみを含める場合は、[Threat ResponseにTargetを作成する(内部ホストのみ)(Create Targets in Threat Response for Internal hosts only)] オプションを選択します。
    - Cisco SecureX Threat Response に送信する必要があるホスト情報を決定するときに内部と外部両方の IP アドレスを含める場合は、[Threat ResponseにTargetを作成する(内部ホストと外部ホスト)(Create Targets in Threat Response for internal and external hosts)] オプションを選択します。
- [アラームデータからのホストの詳細を使用(Use host details from the alarm data)]: ターゲットオブジェクトを送信元ホストとターゲットホスト用に構築するか、送信元ホストのみまたはターゲットホストのみ用に構築するかを指定できます。

詳細については、「応答管理の設定(Configuring Response Management)」ヘルプトピックを参照してください([設定(Configure)] > [検出応答管理(DETECTION Response Management)] を選択します。 ([ヘルプ(Help)]) アイコンをクリックします)。

- 以前のバージョンの Secure Network Analytics(旧 Stealthwatch)で Cisco SecureX Threat Response に Secure Network Analytics アラームを送信するように設定した場合は、Threat Response Incident のアクションが自動的に作成されます。
- 関係ポリシーから派生したアラーム用に作成されたインシデントには、この情報はアラームで利用できないため、Observable としての IP アドレスは含まれません。
- Incident には、「Secure Network Analytics アラームの CTIM オブジェクトへの変換について」の項で指定した特定の条件の Target オブジェクトが含まれます。
- Secure Network Analytics アラームから作成された Incident は、地域クラウドとともに配置された CTR コンソールから表示できます。詳細については、「SecureX 地域クラウド」の項を参照してください。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

SecureX の Secure Network Analytics エンリッチメントデータについて

Manager が Cisco Security Services Exchange に登録され、Secure Network Analytics モジュールが SecureX で設定されると、Threat Response ワークフローで Secure Network Analytics からのエンリッチメントデータを確認できるようになります。

調査で要求されたすべての有効な IP アドレスについて、Secure Network Analytics は、この IP に関連付けられているセキュリティイベントを、対応する Sighting および Indicator オブジェクトの形式で返します。

[SecureXの設定(SecureX Configuration)] フォームで返されるセキュリティイベントに、次のパラメータを設定できます。

- SecureX からの調査リクエストを許可するかどうか。
- セキュリティイベントを返す Secure Network Analytics ドメイン。
- 送信される上位イベントの数。
- セキュリティイベントを返す期間。

Cisco Threat Intel モデルについて

SecureX に送信する前に、Secure Network Analytics アラームとセキュリティイベントが Cisco Threat Intel Model(CTIM)オブジェクトに変換されます。

CTIM の詳細については、Threat Intel Model のマニュアルを参照してください。

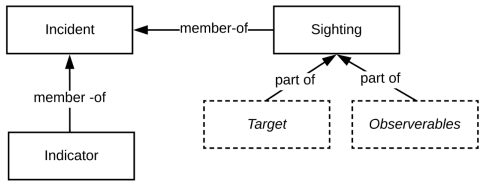
この変換で使用される主要なエンティティを次に示します。

- Incident:組織に影響する指標の個別のインスタンスと、インシデント対応に関連する情報。
- Sighting:特定の日時にサイバー上で観測されたデータにおける記録。
- Observable:一貫性のある ID を持ち、意図または特性(ドメイン名、IP アドレス、ファイルハッシュ、特定のデバイスまたはユーザー)ごとに分類されるのに十分な安定性がある、単純で原始的な値。Secure Network Analytics では、IP アドレスタイプの Observable についてのみ情報を共有します。
- Target:脅威の標的となったデバイス、ID、またはリソース。ターゲットは 1 つ以上の Observable によって識別されます。
- Indicator:悪意のある動作を示す動作パターンまたは一連の条件についての記述。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Secure Network Analytics アラームの CTIM オブジェクトへの変換について

Threat Response のインシデントアクションによって送信されたすべてのアラームは、インシデント、検出情報、インジケータとそれらの間の関係に変換されます。次の図は、CTIM モデルでの Secure Network Analytics アラームの表示を示しています（簡易版）。



Incident の Sighting オブジェクトを作成する場合、Secure Network Analytics には、次の制約がある Observable が含まれます。

- リレーションシップ ポリシー イベントから派生したアラームには、Sighting オブジェクトに Observable オブジェクトがありません。
- 送信元が「複数の送信元」またはターゲットが「複数の送信先」であるアラームには、該当する Observable は、Sighting のオブジェクトに含まれません。

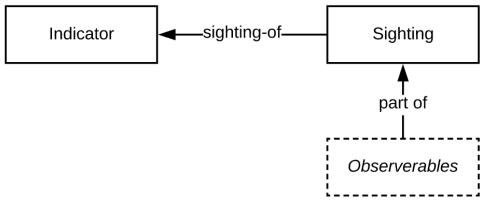
検出情報のターゲットオブジェクトを構築するためのルールは、次の追加の成約を使用してアラームを処理する Threat Response のインシデントアクションから取得されます。

- アラームの送信元または送信先が「複数の送信先」の場合、ターゲットオブジェクトは含まれません。

Secure Network Analytics セキュリティイベントの CTIM オブジェクトへの変換について

SecureX からの調査リクエストに応じて、Secure Network Analytics は IP アドレスに関連付けられたセキュリティイベントを返します。

すべてのセキュリティイベントは、次の図に示すように、リレーションシップを使用して CTIM モデルの Sighting および Indicator オブジェクトに変換されます。



Secure Network Analytics セキュリティイベントを CTIM オブジェクトに変換する場合、次の制約事項とルールが適用されます。

- ターゲットオブジェクトは、セキュリティイベントの Sighting オブジェクトに含まれていません。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Cisco Cloud アカウント

SecureX へのアクセスに必要なアカウント

SecureX および関連ツールを使用するには、使用予定の地域クラウドで次のいずれかのアカウントを持っている必要があります。

- シスコ セキュリティアカウント
- AMP for Endpoints アカウント
- Cisco Threat Grid アカウント

詳細については、『SecureX Sign-On Guide』を参照してください。

> お客様またはお客様の組織ですでに、使用予定の地域クラウドで上記のいずれかのアカウントをお持ちの場合は、既存のアカウントを使用してください。新しいアカウントを作成しないでください。

SecureX にアクセスするためのアカウントの作成

アカウントの作成の詳細については、『SecureX Sign-On Guide』を参照してください。

組織のシスコ セキュリティアカウントへのアクセスの管理

お客様がシスコ セキュリティアカウントの所有者または管理者の場合は、別のユーザーに組織のシスコ セキュリティアカウントへのアクセス権を付与でき、既存のユーザーを管理できます（アカウントのアクティベーションの電子メールを再送信するなど）。

ユーザーを管理するには、次の手順を実行します。

1. ブラウザウィンドウで、自身の地域のシスコセキュリティアカウントに移動します。
   - 北米：https://castle.amp.cisco.com
   - ヨーロッパ：https://castle.eu.amp.cisco.com
   - アジア（APJC）：https://castle.apjc.amp.cisco.com
2. [ユーザー（Users）] をクリックします。
3. ユーザーアクセス権を追加または編集します。
   [アカウント管理者（Account Administrator）] を選択した場合は、ユーザーにはユーザーアクセス権を付与して管理する権限が与えられます。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Cisco Secure Network Analytics と SecureX の設定

SecureX 統合の設定

Secure Network Analytics で SecureX 統合を設定すると、次のことが可能になります。

- Secure Network Analytics の UI で SecureX のメニューを使用する。
- Secure Network Analytics の UI で SecureX のリボンを使用する。
- Cisco SecureX Threat Response プライベート インテリジェンス ストアに Secure Network Analytics アラームを送信する。

前提条件

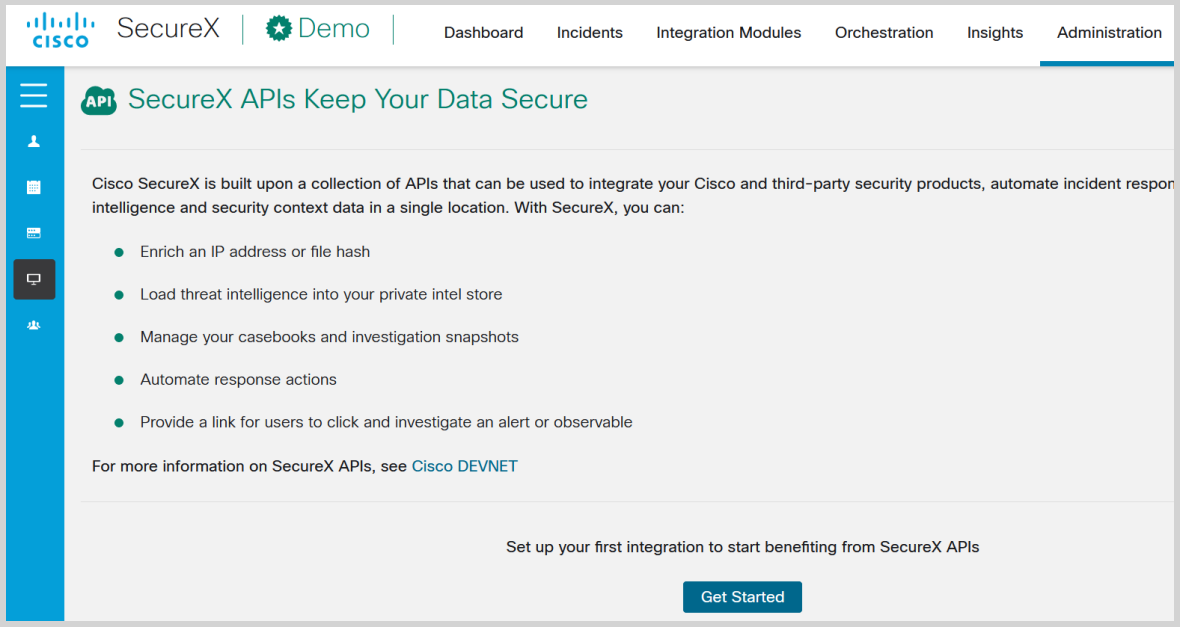
- Manager v7.2.1 以降
- SecureX にアクセスするためのアカウントがある（「SecureX へのアクセスに必要なアカウント」を参照）。
- Manager から Cisco Cloud、SecureX プライベート インテリジェンス API、および地域の SecureX ポータルにアウトバウンド接続できる。
    - 北米クラウド：
        - api-sse.cisco.com、ポート 443
        - visibility.amp.cisco.com、ポート 443
        - private.intel.amp.cisco.com、ポート 443
        - securex.us.security.cisco.com、ポート 443
    - EU クラウド：
        - api.eu.sse.itd.cisco.com、ポート 443
        - visibility.eu.amp.cisco.com、ポート 443
        - private.intel.eu.amp.cisco.com、ポート 443
        - securex.eu.security.cisco.com、ポート 443
    - アジア（APJC）クラウド：
        - api.apjc.sse.itd.cisco.com、ポート 443
        - visibility.apjc.amp.cisco.com、ポート 443
        - private.intel.apjc.amp.cisco.com、ポート 443
        - securex.apjc.security.cisco.com、ポート 443
    - Orbital ユーザーのみ：次の追加ホストにアウトバンド接続を許可する。
        - 北米：orbital.amp.cisco.com、ポート 443
        - ヨーロッパ：orbital.eu.amp.cisco.com、ポート 443
        - アジア：orbital.apjc.amp.cisco.com、ポート 443
- Secure Network Analytics の導入環境でセキュリティイベントとアラームが期待どおりに生成されている。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

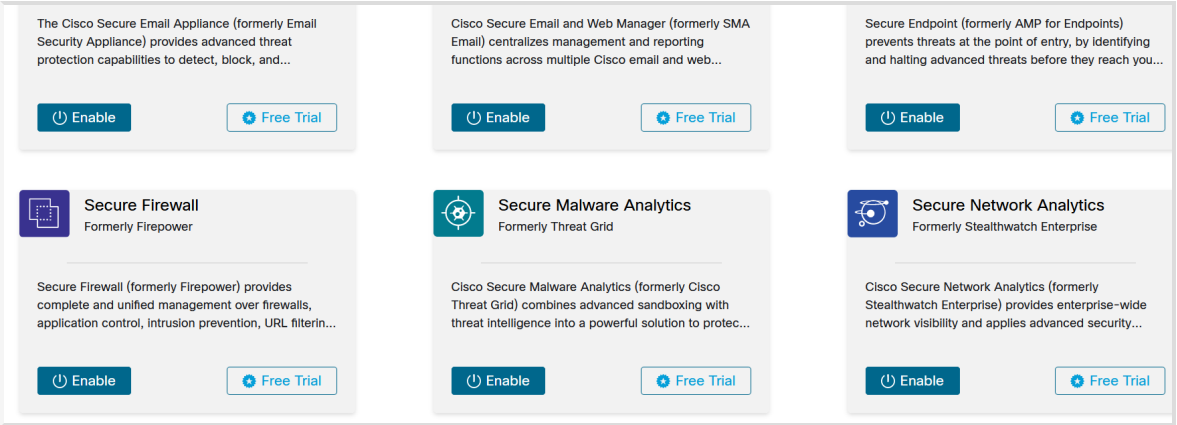
手順

SecureX 統合を設定するには、次の手順を実行します。

1. SecureX の地域クラウドに移動します。
   - 北米クラウド：https://securex.us.security.cisco.com
   - ヨーロッパクラウド：https://securex.eu.security.cisco.com
   - アジア（APJC）クラウド：https://securex.apjc.security.cisco.com
2. エンドポイント向け SecureX、Cisco Threat Grid、またはシスコのセキュリティ アカウントのクレデンシャルを使用してサインインします。
3. [管理（Administration）] > [API クライアント（API Clients）] を選択します。
4. 初めて設定する場合は、[開始（Get Started）] ボタンをクリックします。

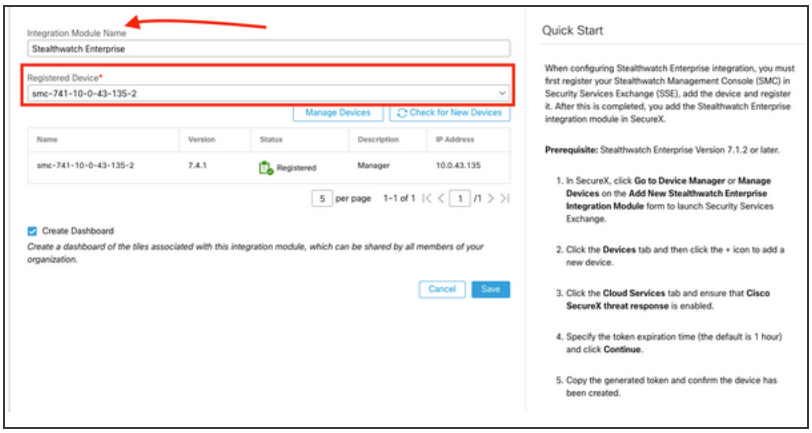


5. SecureX リボンを選択し、[モジュールの設定（Configure a Module）] ボタンを選択します。
6. [Secure Network Analytics] タイルを選択し、[有効（Enable）] ボタンをクリックします。

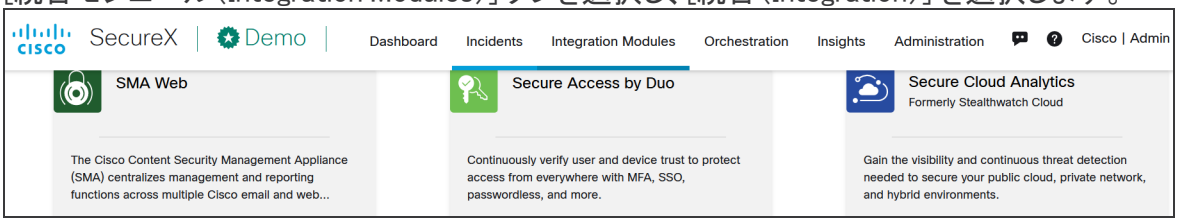


© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

7. 新しい [Secure Network Analysis] 統合モジュール を追加し、ドロップダウンリストからデバイスを選択します。[ダッシュボードの作成（Create Dashboard）] チェックボックスをオンにして [保存（Save）] をクリックします。



8. [統合モジュール（Integration Modules）] タブを選択し、[統合（Integration）] を選択します。



9. 開いているダイアログで、API クライアントの名前と説明を入力し、次の範囲を選択します。

- Admin
- Feedback
- Integration
- Orbital
- Registry
- Users
- Casebook
- Global Intel:read
- Notification
- Private Intel
- Response
- Webhook
- Enrich:read
- Inspect:read
- Oauth
- Profile
- Telemetry:write

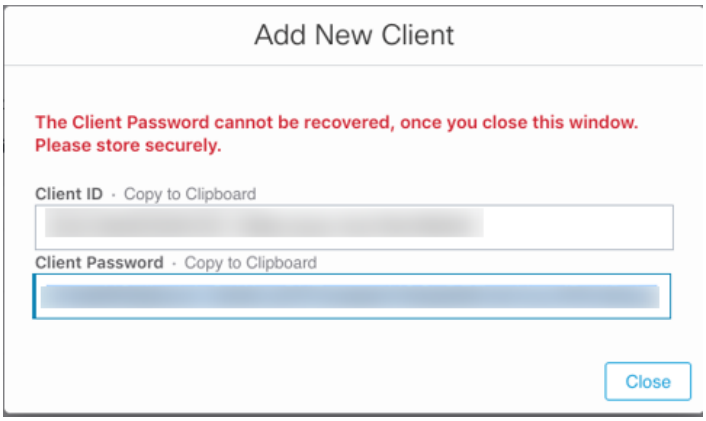
> API クライアントが生成された後は範囲を変更できません。

10. [新しいクライアントの追加（Add New Client）] をクリックします。

> 新しいクライアント ID を作成するには、[管理（Administration）] > [API クライアント（API Clients）] を選択し、[API クライアントの生成（Generate API Client）] をクリックします。

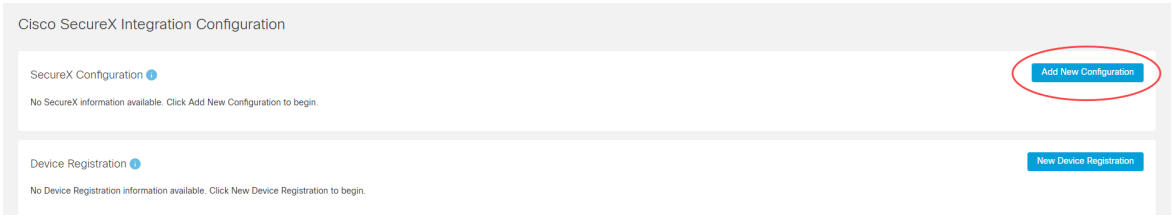
11. システムは、クライアント ID とクライアントパスワードを作成します。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



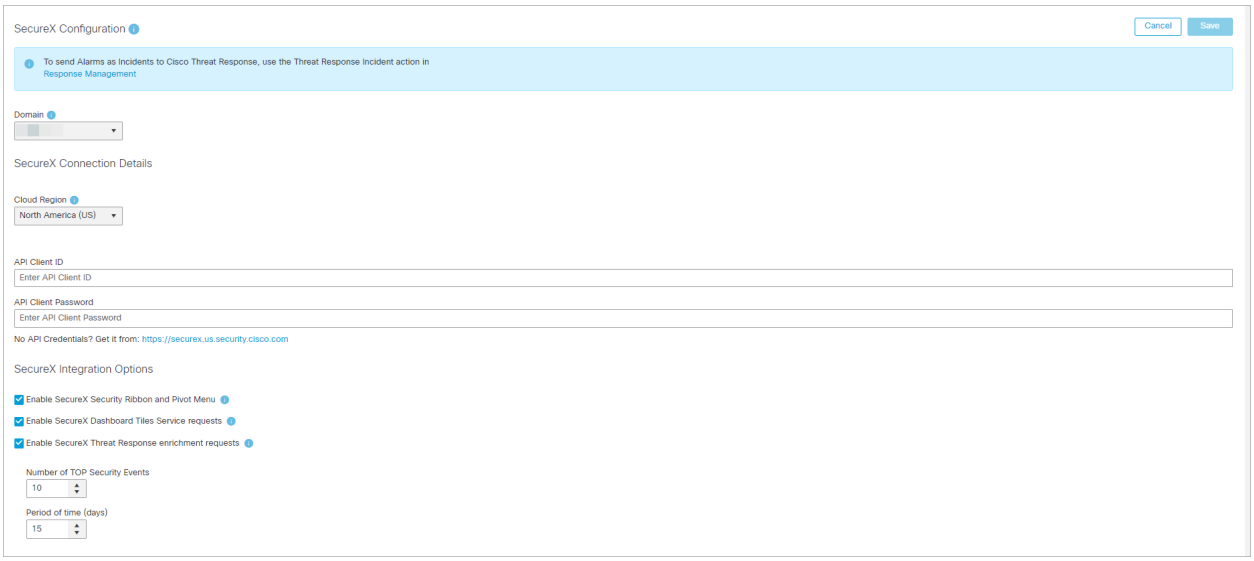
このウィンドウを閉じると、クライアントパスワードを回復できません。

12. プライマリ管理者または設定管理者として Manager にログインします。
13. ナビゲーションメニューで、[設定(Configuration)] > [SecureX 統合(INTEGRATIONS SecureX)] をクリックします。
14. [SecureX の設定(SecureX Configuration)] セクションで、[新しい設定を追加(Add New Configuration)] をクリックします。



15. 開いているフォームで、API クライアントの作成に使用した地域クラウドを選択し、ステップ 11 のクライアント ID とクライアントパスワードを貼り付けます。
16. 有効にする統合オプションを選択し、[保存(Save)] をクリックします。システムは API クレデンシャルを検証して保存します。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



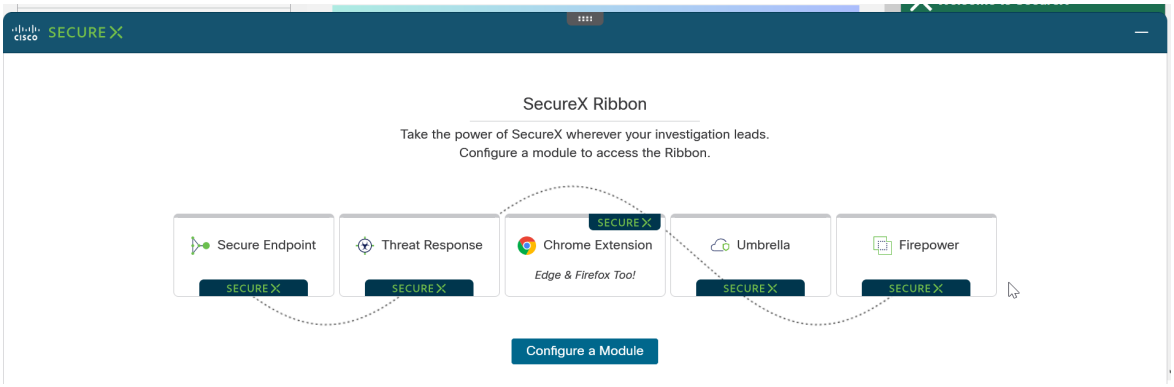
SecureX のリボンとメニューの承認

SecureX の設定が完了したら、Manager の任意のページにあるリボン、または [SecureX の設定（SecureX Configuration）] ページから、SecureX のリボンとメニューを承認できます。

[SecureXの設定（SecureX Configuration）] ページにある SecureX のリボンの認証ウィジェットには、リボンの現在の承認ステータスが表示され、リボンを承認したり、承認を解除したりできます。

SecureX のリボンからの承認

1. Manager のページの下部にある SecureX のリボンを展開します。

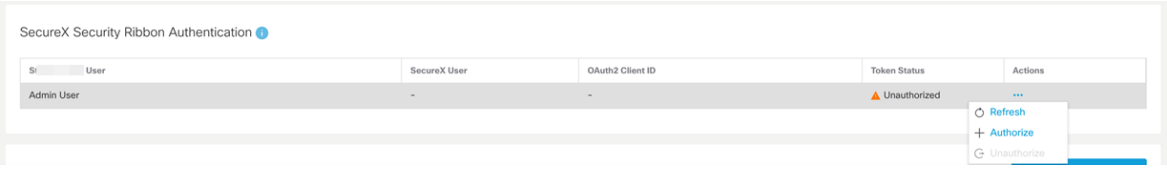


2. [SecureX を取得（Get SecureX）] をクリックします。SecureX のログインページにリダイレクトされます。
3. クレデンシャルを使用して SecureX にログインします。
4. 指定した範囲で SecureX にアクセスするために、Manager SecureX のリボンクライアントを承認するように求められます。
5. アクセス権を付与します。リボンが開いた状態で Manager ページにリダイレクトされ、Manager でリボンを使用できるようになります。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

[SecureXの設定（SecureX Configuration）] ページからの承認

1. Manager にログインします。
2. [設定（Configure）] > [SecureX 統合（INTEGRATIONS SecureX）] を選択します。
3. [SecureX セキュリティリボンの認証（SecureX Security Ribbon Authentication）] ウィジェットの [アクション（Actions）] メニューを開き、[...]> [承認する（Authorize）] を選択します。SecureX のログインページにリダイレクトされます。



4. クレデンシャルを使用して SecureX にログインします。
5. 指定した範囲で SecureX にアクセスするために、Manager SecureX のリボンクライアントを承認するように求められます。
6. アクセス権を付与します。リボンが開いた状態で Manager ページにリダイレクトされ、Manager でリボンを使用できるようになります。

別の SecureX アカウントで SecureX のリボンを使用する必要がある場合は、現在のユーザーの承認を解除してから新しいユーザーで再度承認する必要があります。

現在の SecureX リボンの承認解除

1. [SecureX の設定（SecureX Configuration）] ページで、[SecureX セキュリティリボンの認証（SecureX Security Ribbon Authentication）] ウィジェットにある [アクション（Actions）] メニューを開き、[...] を選択> [承認解除（Unauthorize）] をクリックします。
2. 上記の手順に従って、別のユーザーで認証します。

Threat Response インシデントアクションの設定

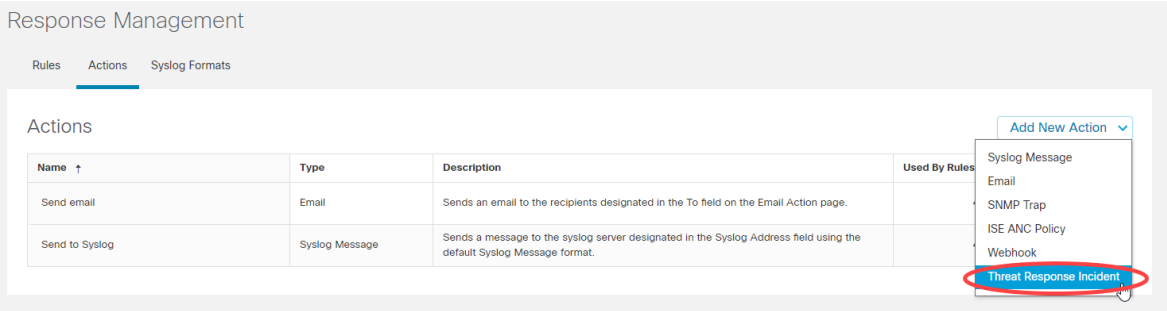
> 以前のバージョンの Secure Network Analytics（旧 Stealthwatch）で Cisco SecureX Threat Response に Secure Network Analytics アラームを送信するように設定した場合は、Threat Response Incident のアクションが自動的に作成されます。

対応管理で Threat Response のインシデントアクションを設定するには、次の手順を実行します。

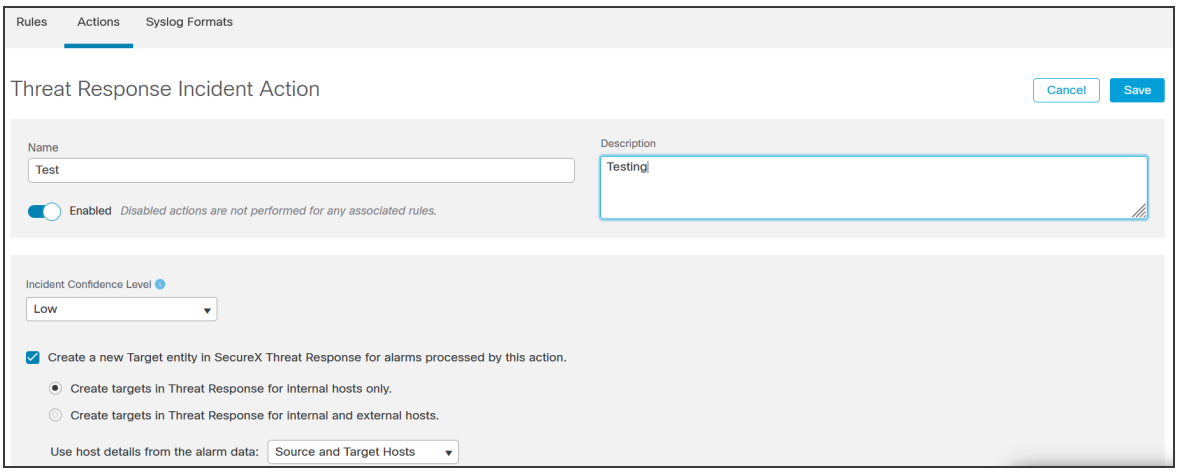
1. Manager にログインします。
2. [設定（Configure）] > [検出対応管理（DETECTION Response Management）] の順に選択します。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3. [アクション（Actions）] タブをクリックしてから、[新しいアクションの追加（Add New Action）] > [Threat Response Incident] の順にクリックします。



4. フォームに入力し、[保存（Save）] をクリックします。

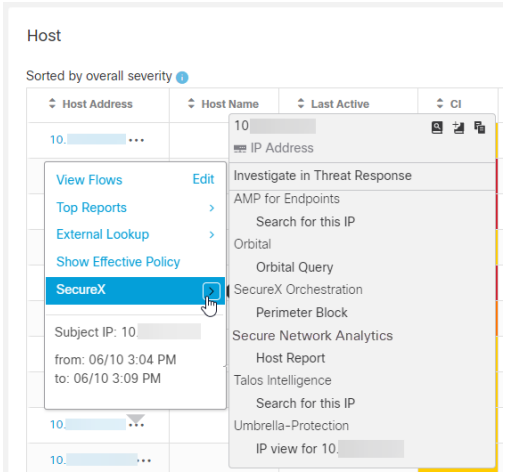


アクションのオプションの詳細については、「Cisco SecureX Threat Response への Secure Network Analytics アラームの送信について」と「対応管理の設定」のヘルプトピックを参照してください。

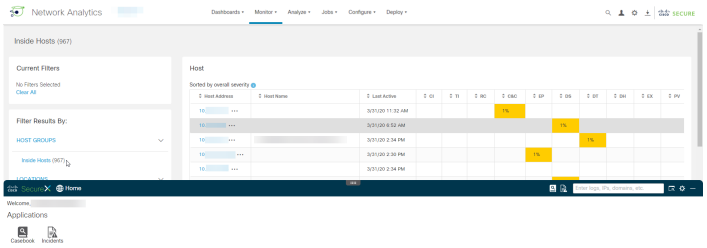
検証

1. Manager で SecureX のメニューとリボンが使用可能であることを確認します。
    - SecureX のメニューの場合：
        - 該当する IP アドレスを含む Manager の任意のページを開きます。
        - 該当する IP アドレスの横にある ••• （[省略記号（Ellipsis）]）アイコンをクリックします。
        - 表示されるポップアップメニューで、[SecureX] の横にある矢印をクリックします。第 2 のポップアップメニューがメニューコンテンツと共に表示されます。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



- SecureX のリボンの場合：
  - Manager の任意のページに移動します。ページの下部にある  （SecureX のリボン）アイコンをクリックしてウィジェットを展開します。



2. SecureX で Secure Network Analytics アラームを確認します。
   a. Secure Network Analytics がクリティカルまたは重大なセキュリティアラームを検出するか、テストセキュリティアラームが生成されるまで待ちます。
   b. SecureX の地域クラウドにログインします。
   c. SecureX のリボンの Incidents アプリ、または Cisco SecureX Threat Response の Incident Manager に移動します。
   d. リストにアラームが表示されています。

Cisco Cloud での Manager の登録

Cisco Security Services Exchange（SSE）クラウドは、一元管理の Manager で使用できます。SSE クラウドで Manager を登録すると、SecureX で Manager からセキュリティイベントなどのエンリッチメントデータを取得して調査ワークフローに含めたり、SecureX ダッシュボードの（Stealthwatch と表示されている）Secure Network Analytics タイルを取得したりできます。

詳細については、「SecureX の Secure Network Analytics エンリッチメントデータについて」、および「SecureX ダッシュボードの Secure Network Analytics タイルについて」の項を参照してください。

- SSE はデフォルトで有効になっています。
- 自動登録を使用する場合は、SSE アカウントとスマート ライセンス アカウントをリンクする必要があります。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

> ⚠ デフォルトの Manager アイデンティティ証明書で提供されるものとは異なるカスタム Manager アイデンティティ証明書を使用している場合は、Manager で追加の設定手順が必要になることがあるため、テクニカルサポートにお問い合わせください。

自動登録手順

次の条件が満たされると、Manager は SSE クラウドに自動的に登録されます。

- SSE オプションは、外部サービスで Manager に対して有効になります。
- Manager はまだ SSE に登録されていません。
- お使いの製品はスマート ソフトウェア ライセンスに登録されています。手順については、『Smart Software Licensing』ガイドを参照してください。

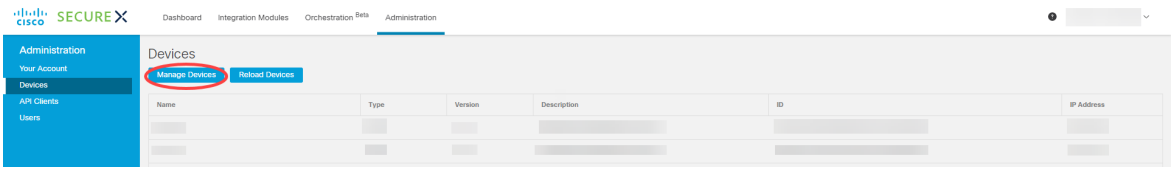
SSE を有効または無効にするには、次の手順を実行します。

1. Manager にログインします。
2. [設定(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
3. Manager の [アクション(Actions)] 列の下にある ••• ([省略記号(Ellipsis)]) アイコンをクリックし、[アプライアンス設定の編集(Edit Appliance Configuration)] をクリックします。
4. [全般(General)] をクリックします。
5. [外部サービス(External Services)] で、[Cisco Security Services Exchange] チェックボックスをオンまたはオフにして、自動登録を有効または無効にします。
6. [設定の適用(Apply Settings)] をクリックします。SSE を有効にした場合は、手順 7 に進み、デバイスを登録します。
7. [セキュリティ分析(Security Insight)] ダッシュボードに戻ります。
8. [設定(Configure)] > [SecureX 統合(INTEGRATIONS SecureX)] を選択します。
9. [デバイス登録(Device Registration)] セクションで、[新しいデバイスの登録(New Device Registration)] をクリックします。
10. [自動登録(Register Automatically)] を選択します。

アカウントのリンク

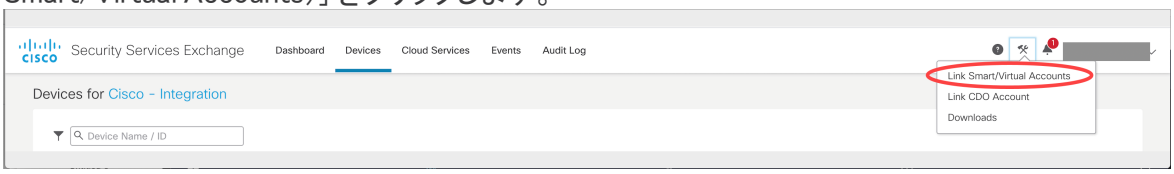
スマート ライセンス アカウントを Cisco Security Services Exchange アカウントにリンクするには、次の手順を実行します。

1. SecureX の地域クラウドに移動し、Cisco Advanced Malware Protection for Endpoints、Cisco Threat Grid、またはシスコ セキュリティ アカウントのログイン情報を使用してログインします。
2. [管理(Administration)] タブをクリックします。[デバイス(Devices)] > [デバイスの管理(Manage Devices)] を選択して Security Services Exchange に移動できるようにします。



© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3. 🛠 ([ツール(Tools)] アイコンをクリックし、[スマート/仮想アカウントのリンク(Link Smart/Virtual Accounts)] をクリックします。

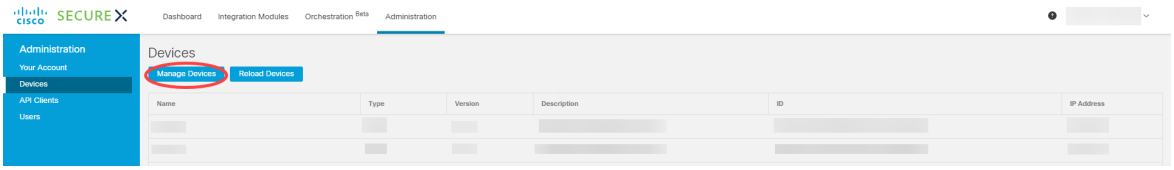


4. アカウントのリストを含むポップアップからスマートアカウントを選択します。

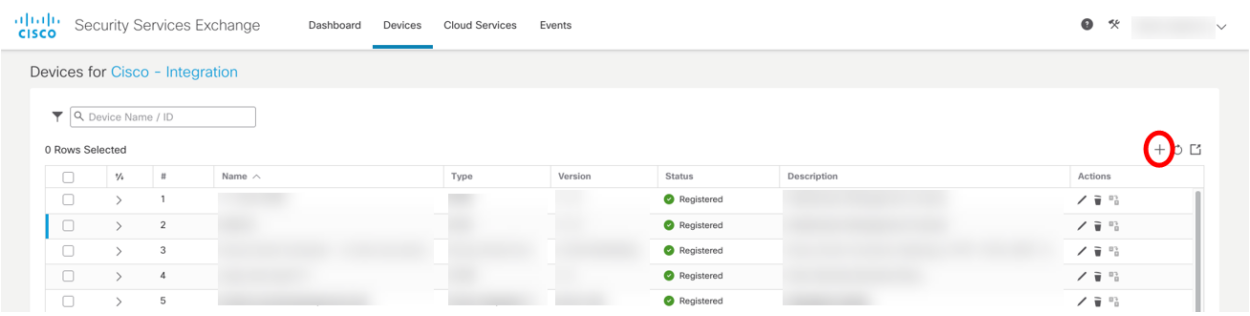
手動登録手順

Security Services Exchange に Manager を手動で登録するには、次の手順を実行します。

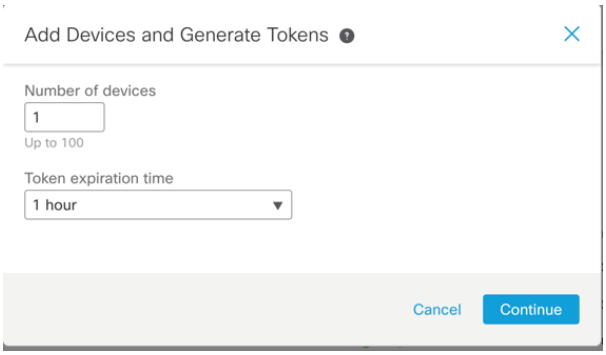
1. SecureX 地域クラウドに移動し、エンドポイント向け SecureX、Cisco Threat Grid、またはシスコ セキュリティアカウントのログイン情報を使用してログインします。
2. [管理(Administration)] タブをクリックします。[デバイス(Devices)] > [デバイスの管理(Manage Devices)] を選択して Security Services Exchange に移動できるようにします。



3. [デバイス(Devices)] タブをクリックし、ページの右側にある ＋ ([デバイスの追加とトークンの生成(Add Devices and Generate Tokens)]) をクリックします。

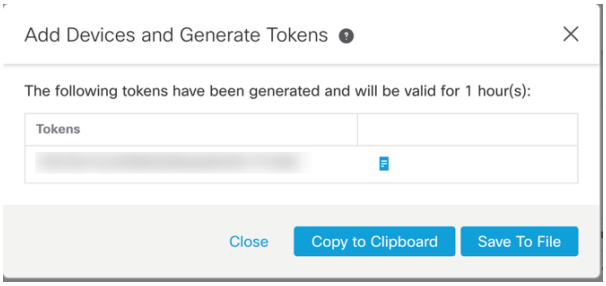


4. 開いているダイアログで、[続行(Continue)] をクリックし、デバイスのトークンをシステムに生成させます。

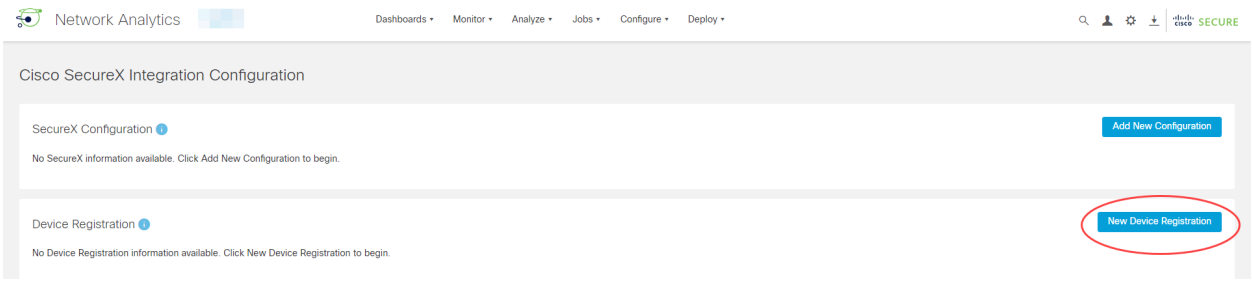


© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

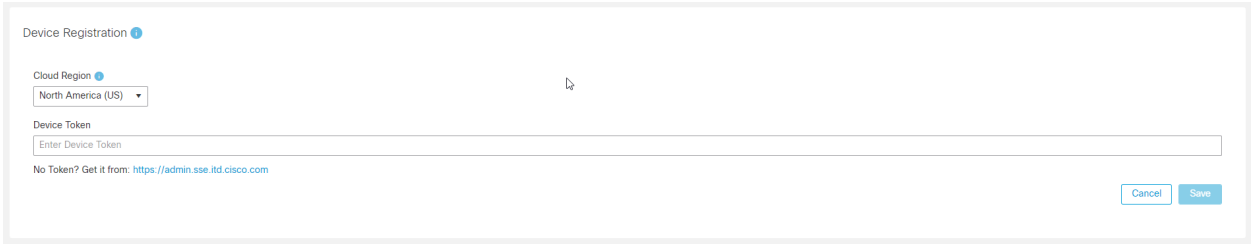
5. 生成されたトークンをクリップボードにコピーするか、生成されたトークンをファイルに保存します。



6. プライマリ管理者または設定管理者として Manager にログインします。
7. [設定（Configure）] > [SecureX 統合（INTEGRATIONS SecureX）] を選択します。
8. [デバイス登録（Device Registration）] セクションで、[新しいデバイスの登録（New Device Registration）] をクリックします。



9. 開いているダイアログで、SecureX の地域クラウドと一致するクラウド地域を選択し、手順 5 で生成して保存した Security Services Exchange トークンを挿入し、[保存（Save）] をクリックします。



10. デバイスは Cisco Security Services Exchange に登録され、ステータスは [登録済み（Enrolled）] として表示されます。
11. Cisco Security Services Exchange ポータルでデバイスのステータスを確認します。デバイスのステータスは、[登録済み（Enrolled）] として表示される必要があります。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

SecureX での Cisco Secure Network Analytics 統合モジュールの設定

SecureX で Secure Network Analytics からエンリッチメントデータとダッシュボードタイルを取得するには、統合モジュールを設定する必要があります。

前提条件

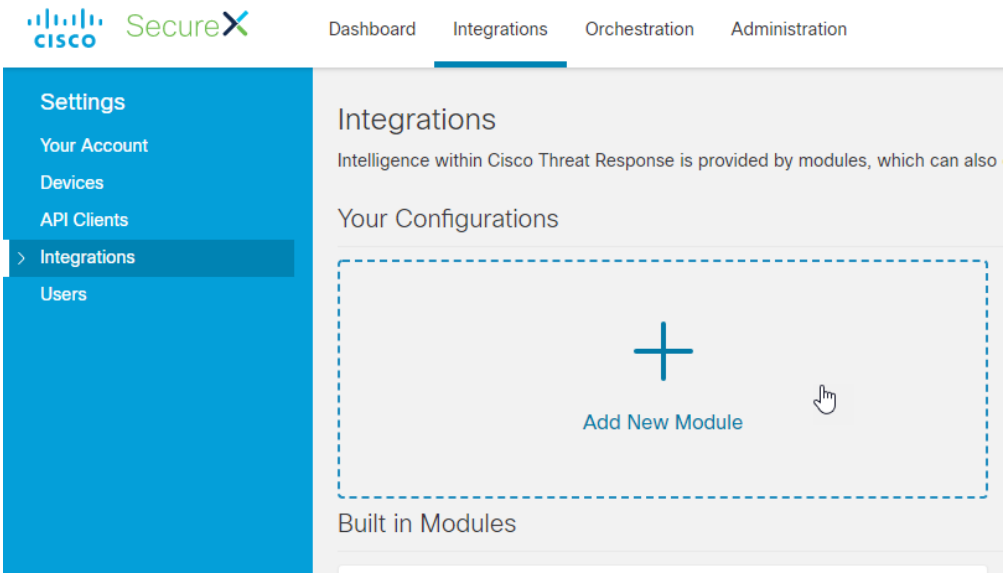
- Manager が Cisco Security Services Exchange クラウドに登録されている。
- Cisco SecureX Threat Response が、Cisco Security Services Exchange ポータルのクラウドサービスで有効になっている。

  詳細については、「Cisco Cloud での Manager の登録」の項を参照してください。

手順

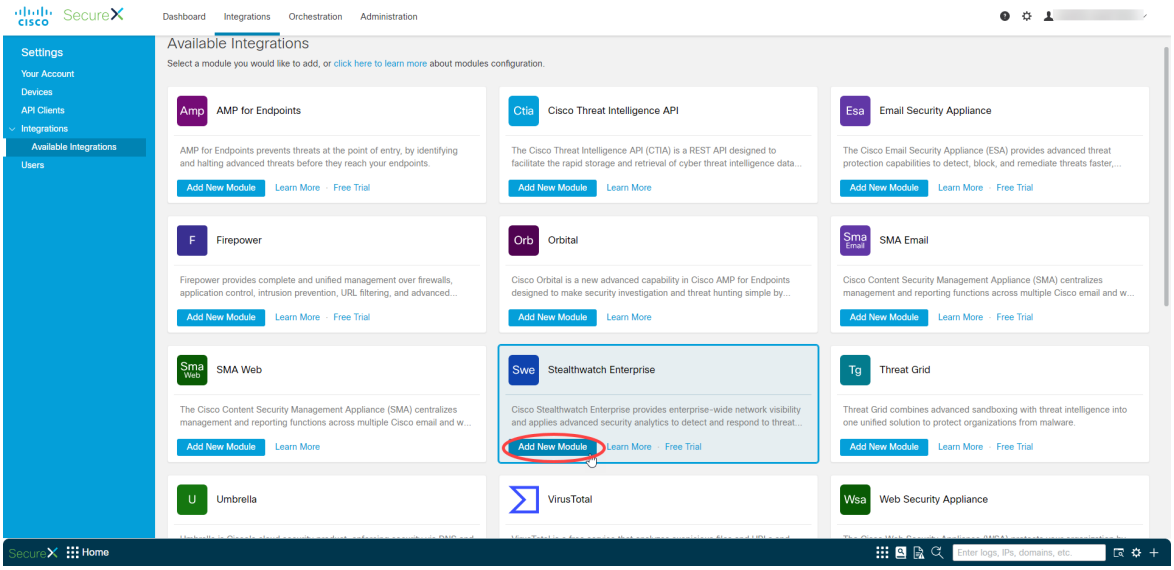
SecureX で Secure Network Analytics モジュールを設定するには、次の手順を実行します。

1. SecureX の地域クラウドに移動し、Cisco Advanced Malware Protection for Endpoints、Cisco Threat Grid、またはシスコ セキュリティ アカウントのログイン情報を使用してログインします。
2. [統合モジュール(Integration Modules)] > [統合(Integrations)] を選択します。
3. [新しいモジュールを追加(Add New Module)] をクリックします。[使用可能な統合(Available Integrations)] ページが開きます。

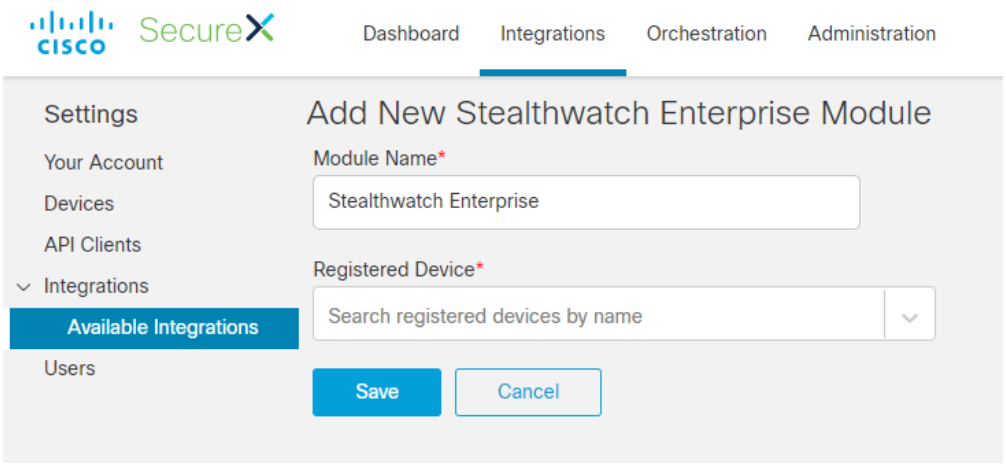


© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

4. Stealthwatch Enterprise モジュールを見つけて、[新しいモジュールを追加（Add New Module）] をクリックします。



5. 開いているダイアログで、次のようにします。
   a. モジュールに名前を付けます。
   b. [登録済みデバイス（Registered Device）] ドロップダウンから、Manager を見つけます。
   c. [保存（Save）] をクリックします。



6. Cisco SecureX Threat Response が Manager からエンリッチメントデータを取得できることを確認します。手順は次のとおりです。
   a. Manager のセキュリティダッシュボードを確認し、セキュリティイベントを生成する IP を見つけます。
   b. Cisco SecureX Threat Response の調査検索パネルにこの IP を入力します。
   c. グラフには、要求されたホストとのセキュリティイベントに関連する他のホストが表示されます。
   d. Sightings は要求されたホストに関連付けられているセキュリティイベントを表します。

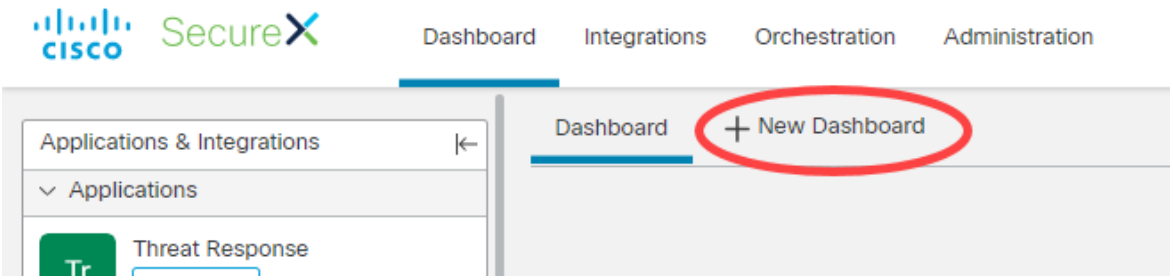
© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Secure Network Analytics タイルを使用した SecureX ダッシュボードの設定

> （Stealthwatch と表示されている）Secure Network Analytics タイルを SecureX ダッシュボードに追加する前に、Secure Network Analytics 統合モジュールを設定する必要があります。

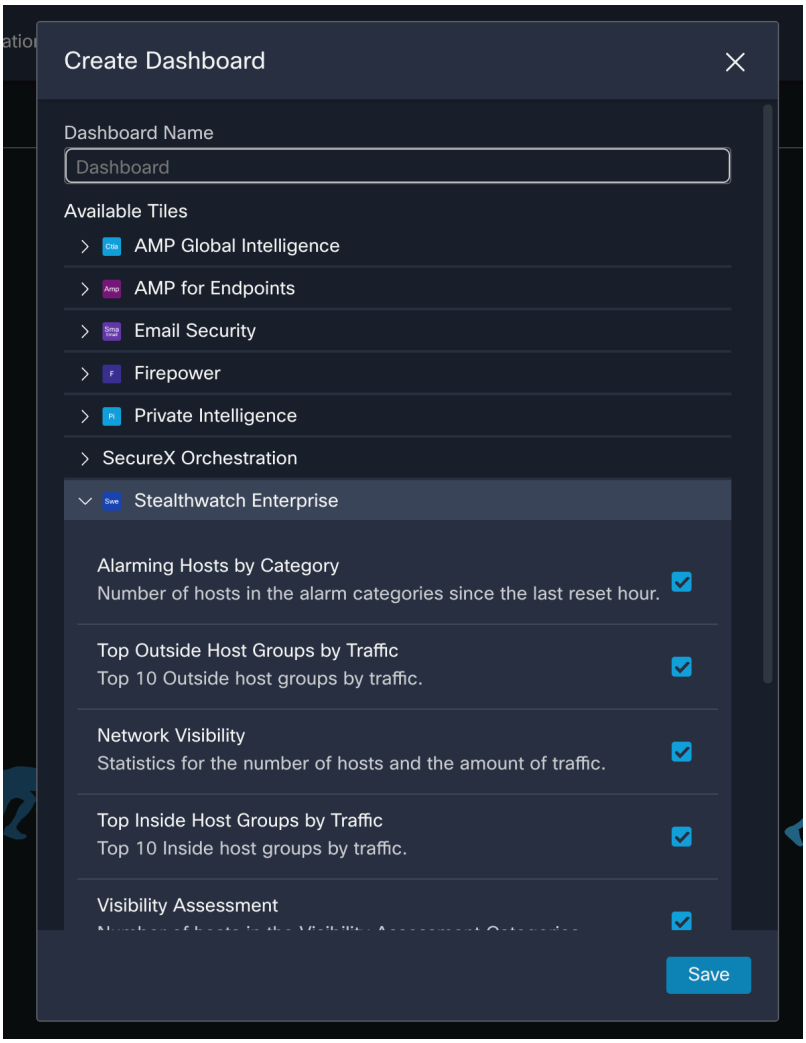
（Stealthwatch と表示されている）Secure Network Analytics タイルをダッシュボードに追加するには、次の手順を実行します。

1. ブラウザウィンドウで、自身の地域の SecureX ポータルに移動します。
   - 北米：https://securex.us.security.cisco.com
   - ヨーロッパ：https://securex.eu.security.cisco.com
   - アジア（APJC）：https://securex.apjc.security.cisco.com
2. シスコ セキュリティまたは Cisco Threat Grid アカウントを使用してログインします。
3. ダッシュボードのメニューバーで、[新規ダッシュボード（New Dashboard）] をクリックして、[ダッシュボードの作成（Create Dashboard）] フォームを開きます。



4. 開いたダイアログで、[ダッシュボード名（Dashboard Name）] を入力し、使用可能なタイルの下にある Stealthwatch Enterprise モジュールを見つけます。
5. Stealthwatch Enterprise を展開し、ダッシュボードに追加するタイルを選択します。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



6. [保存(Save)]をクリックします。

   選択したタイルが、関連するデータとともにダッシュボードレイアウトに表示されます。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

既知の問題と制限事項

- フェールオーバーは、v7.4 の SecureX 統合ではサポートされていません。SNA フェールオーバーペアの両方の Manager から統合を機能させるには、セカンダリ Manager で設定を繰り返す必要があります。
- Backup and Restore は、Cisco Security Services Exchange Cloud ポータルのデバイス登録ではサポートされていません。Manager の [SecureX の設定（SecureX Configuration）] にある [デバイス登録（Device Registration）] パネルには、クラウドにおけるデバイス登録の実際のステータスが表示されます。したがって、デバイス登録のバックアップから設定を復元することはできません。バックアップ後に削除した場合は、復元後に登録を再実行する必要があります。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 3 月 3 日	初版
2_0	2023 年 7 月 18 日	最新の UI の手順を更新。

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL：https://www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。（1721R）

© 2023 Cisco Systems, Inc. and/or its affiliates.
All rights reserved.