

Cisco Secure Firewall Management Center と Security Analytics and Logging (SaaS) の統合ガイド

初版 : 2020 年 7 月 21 日

最終更新 : 2022 年 11 月 8 日

Secure Firewall Management Center と Cisco Security Analytics and Logging (SaaS) の統合

Secure Firewall Threat Defense イベントを保存するのに追加のスペースが必要な場合は、Cisco Security Analytics and Logging (SaaS) を使用して Threat Defense イベントを Stealthwatch クラウドに送信して保存したり、必要に応じて Threat Defense イベントデータを Stealthwatch クラウドを使用したセキュリティ分析に利用できるようにすることができます。ライセンスに応じて、Cisco Defense Orchestrator (CDO) または Stealthwatch にイベントを表示できます。

この統合は、Management Center が管理する Threat Defense デバイス専用です。このドキュメントは、Threat Defense ソフトウェアを実行していないデバイス、Secure Firewall デバイスマネージャが管理するデバイス、または Management Center が管理する Threat Defense 以外のデバイスには適用されません。

Cisco Security Analytics and Logging (SaaS) の詳細については、<https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html> を参照してください。

シスコのセキュリティ分析とロギングリモートイベントストレージオプションの比較

イベントデータを Management Center の外部に保存するための類似しているが異なるオプション:

オンプレミス	SaaS
ファイアウォールの背後に設置するストレージシステムを購入し、ライセンスを取得してセットアップします。	ライセンスとデータストレージプランを購入し、データをシスコのクラウドに送信します。

オンプレミス	SaaS
サポートされるイベントタイプ： <ul style="list-style-type: none"> • 接続 • セキュリティ関連の接続 • 侵入 • ファイルおよびマルウェア • LINA 	サポートされるイベントタイプ： <ul style="list-style-type: none"> • 接続 • セキュリティ関連の接続 • 侵入 • ファイルおよびマルウェア
syslog と直接統合の両方をサポートします。	syslog と直接統合の両方をサポートします。 クラウドへのイベント送信方法の比較 (3 ページ) を参照してください。
<ul style="list-style-type: none"> • Secure Network Analytics Manager ですべてのイベントを表示します。 • Management Center イベントビューアから相互起動して、Secure Network Analytics Manager でイベントを表示します。 • Management Center でリモートに保存された接続とセキュリティ関連の接続のイベントを表示します。 	ライセンスに応じて CDO または Secure Network Analytics で、イベントを表示します。Management Center イベントビューアから相互起動します。
詳細については、『 <i>Secure Firewall Management Center Administration Guide</i> 』またはオンラインヘルプの「Data Storage」の章にあるリンクを参照してください。	

クラウドへのイベント送信方法の比較

Syslog 経由での送信	直接送信
<ul style="list-style-type: none"> Secure Event Connector (SEC) が必要です 各 SEC が 1 秒あたり最大 100,000 イベントをサポートできるため、ファイアウォールからの高いログ出力率に有効です SEC は、CDO または CDO 以外の管理対象デバイスに設定できます。 ファイアウォールでのイベント処理の負担が軽減されるため、ファイアウォール機能のためにリソースが解放されます。 集中化は、特に地理的分散環境では、常に可能または適切とは限りません。 別途インストールが必要です 	<ul style="list-style-type: none"> 地理的分散環境をサポートしているため、分散拠点に最適です。 スマートライセンスが必要です。 <p>Cisco Smart Software Manager オンプレミスサーバー (旧 Smart Software Satellite Server) またはエアギャップ展開を使用している場合はサポートされません。</p> <ul style="list-style-type: none"> 個別のインストールやサービスは必要ありません。 ファイアウォールリソースの負担は比較的大きくなります。

SAL (SaaS) 統合の要件と前提条件

次の要件は、SAL (SaaS) にイベントを送信する両方の方法に適用されます。

要件または前提条件のタイプ	要件
デバイスおよびマネージャ	<p>Threat Defense を管理する Management Center デバイス</p> <p>syslog 経由で送信する場合：バージョン 6.4 以降</p> <p>直接送信する場合：バージョン 7.0</p> <p>必要なバージョンは、Management Center およびすべての管理対象 Threat Defense デバイスに適用されます。</p> <p>システムの展開が完了し、イベントが正しく生成されている必要があります。</p>

要件または前提条件のタイプ	要件
地域のクラウド	<p>イベントの宛先となる地域クラウドを決定します。</p> <p>イベントは、異なる地域のクラウドから表示したり、異なる地域のクラウド間で移動することはできません。</p> <p>直接接続を使用して、SecureX または Cisco SecureX Threat Response と統合するためにクラウドにイベントを送信する場合は、この統合に対して同じ地域 CDO クラウドを使用する必要があります。</p> <p>イベントを直接送信する場合、Management Center で指定する地域クラウドは CDO テナントの地域と一致する必要があります。</p>
データプラン	<p>システムに必要なクラウドストレージの容量を決定します。</p> <p>ストレージ要件の計算とデータプランの購入 (6 ページ) を参照してください。</p>
ライセンス	<ul style="list-style-type: none"> • Cisco Security Analytics and Logging ライセンス：任意 ライセンスのオプションと説明については、SAL (SaaS) ライセンス (5 ページ) を参照してください。 • CDO ライセンス：追加の CDO ライセンスは必要ありません。 • Stealthwatch Cloud ライセンス：追加のライセンスは必要ありません。 • Management Center ライセンス：追加のライセンスは必要ありません。
アカウント	この統合のライセンスを購入すると、この機能をサポートする CDO テナントアカウントが提供されます。
サポートされるイベントタイプ	侵入、接続、セキュリティ関連の接続、ファイル、およびマルウェアイベント
ユーザー ロール	<p>Management Center で、次の手順を実行します。</p> <ul style="list-style-type: none"> • 管理者 • アクセス管理者 • ネットワーク管理者 • セキュリティ承認者
イベントを直接送信する場合の追加要件	「 直接統合の前提条件 (15 ページ) 」を参照してください。

要件または前提条件のタイプ	要件
追加の前提条件	各手順の「はじめる前に」または「前提条件」を参照してください。

SAL (SaaS) ライセンス

ライセンス	詳細
無料トライアル	30 日間の無料トライアルライセンスを取得するには、 https://info.securexanalytics.com/sal-trial.html にアクセスしてください。
Logging and Troubleshooting	イベントを Cisco Cloud に保存し、CDO の Web インターフェイスを使用して、保存されたイベントを表示およびフィルタ処理します。
(オプション) Logging Analytics and Detection	<p>システムは、Threat Defense イベントに Stealthwatch Cloud の動的エンティティモデリングを適用し、行動モデリング分析を使用して Stealthwatch Cloud の観測値とアラートを生成することができます。Cisco Single Sign-On を使用して、CDO から、プロビジョニングされた Stealthwatch Cloud ポータルを相互起動できます。</p> <p>SAL のライセンスを購入すると、ログを表示するための CDO テナントへのアクセスと、脅威を検出するための SWC インスタンスが提供されます。SAL のユーザーは、これらの 2 つのポータルにアクセスして SAL が提供する結果を確認するために個別の CDO ライセンスまたは SWC ライセンスを必要としません。</p>
(オプション) Total Network Analytics and Detection	<p>システムは、Threat Defense イベントとネットワークトラフィックの両方に動的エンティティモデリングを適用し、観測値とアラートを生成します。Cisco Single Sign-On を使用して、CDO から、プロビジョニングされた Stealthwatch Cloud ポータルを相互起動できます。</p> <p>SAL のライセンスを購入すると、ログを表示するための CDO テナントへのアクセスと、脅威を検出するための SWC インスタンスが提供されます。SAL のユーザーは、これらの 2 つのポータルにアクセスして SAL が提供する結果を確認するために個別の CDO ライセンスまたは SWC ライセンスを必要としません。</p>

SAL (SaaS) ライセンスオプションの詳細については、『Cisco Security Analytics and Logging Ordering Guide』 (<https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html>) を参照してください。

SAL (SaaS) ライセンスは、Cisco Defense Orchestrator テナントを使用してファイアウォールログを表示する権利と、分析用の Stealthwatch Cloud (SWC) インスタンスを提供します。これらの製品のいずれかを使用するために個別のライセンスを保持する必要はありません。

SAL (SaaS) ライセンスを購入するには、シスコの認定セールス担当者にお問い合わせるか、発注ガイド（前述のリンク）にアクセスして SAL-SUB で始まる PID を検索してください。

この製品に関する追加情報は次のとおりです。 <https://apps.cisco.com/Commerce/guest>

ストレージ要件の計算とデータプランの購入

Cisco Cloud が Threat Defense から毎日受け取るイベント数を反映したデータプランを購入する必要があります。これは「日次取り込み率」と呼ばれます。

データストレージ要件を見積もるには、次の手順を実行します。

- （推奨）購入前に Cisco Security Analytics and Logging (SaaS) の無料トライアルに参加します。 [SAL \(SaaS\) ライセンス \(5 ページ\)](#) を参照してください。
- <https://ngfwpe.cisco.com/ftd-logging-estimator> でロギングボリューム見積ツールを使用します。

データプランは、さまざまな日単位およびさまざまな年単位で利用できます。データプランの詳細については、『Cisco Security Analytics and Logging Ordering Guide』（<https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html>）を参照してください。



-
- (注) SAL (SaaS) ライセンスとデータプランがある場合、その後は別のライセンスを取得するだけで、別のデータプランを取得する必要はありません。ネットワークトラフィックのスループットが変化した場合は、別のデータプランを取得するだけで、別の SAL (SaaS) ライセンスを取得する必要はありません。
-

SAL SaaS から Management Center へのイベント送信方法

この統合を正常に展開するには、次のいずれかのトピックのすべての手順に従います。

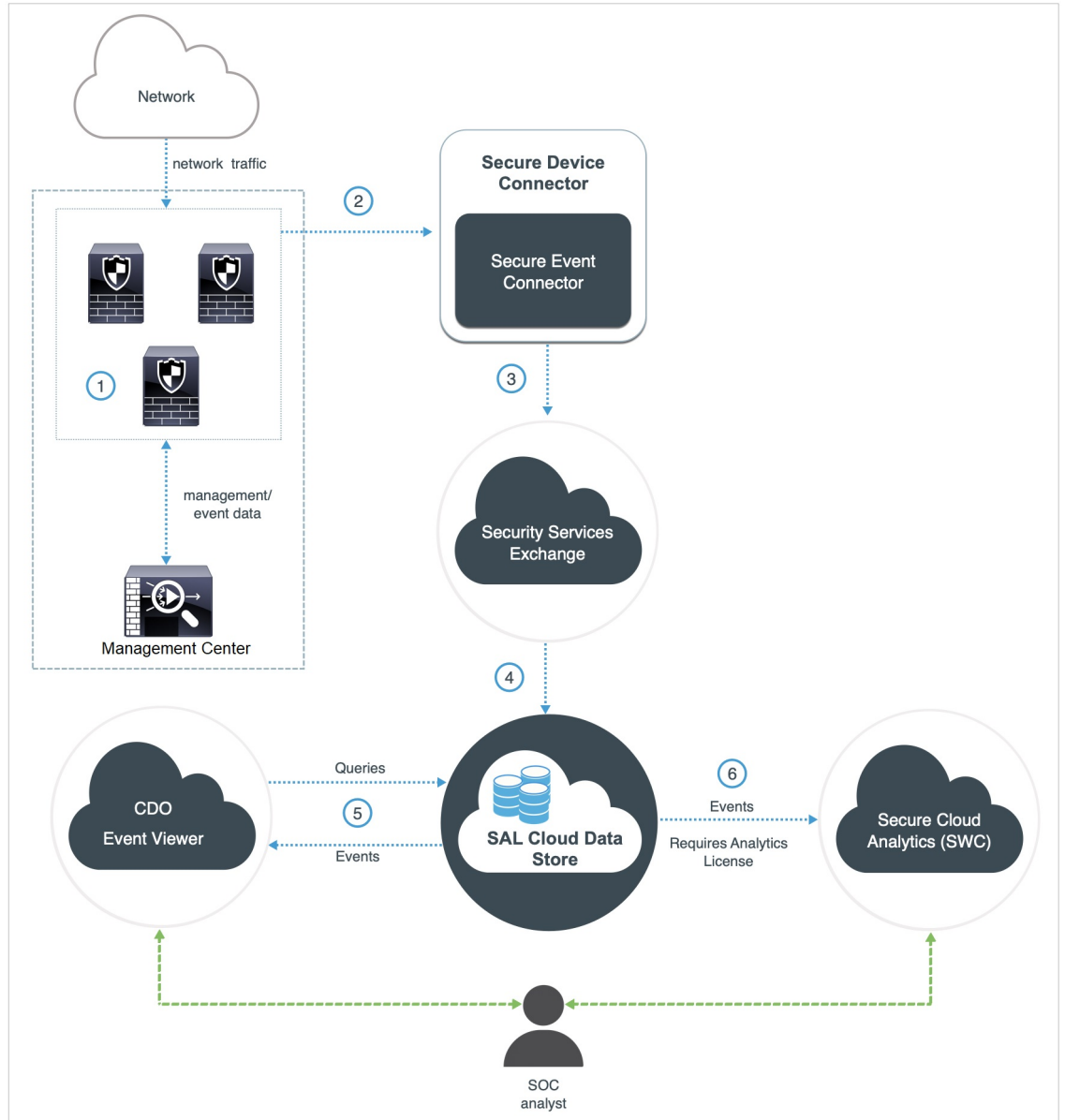
- [直接接続を使用した SAL \(SaaS\) でのイベントデータストレージの設定方法 \(13 ページ\)](#)
- [Syslog を使用した SAL \(SaaS\) でのイベントデータストレージの設定方法 \(7 ページ\)](#)

Syslog を使用した SAL (SaaS) でのイベントデータストレージの設定方法

	操作手順	詳細情報
ステップ	要件と前提条件を確認する	SAL (SaaS) 統合の要件と前提条件 (3 ページ) を参照してください。
ステップ	必要なライセンス、アカウント、およびデータストレージプランを取得する	シスコの認定営業担当者にお問い合わせください。
ステップ	多要素認証を使用して CDO アクセスをセットアップする	CDO へのサインインについては、CDO のオンラインヘルプに記載されている手順を参照してください。 https://docs.defenseorchestrator.com/Welcome_to_Cisco_Defense_Orchestrator/0015_Signing_on_to_CDO
ステップ	VMWare仮想マシンでオンプレミスの Secure Device Connector (SDC) をセットアップする	このコンポーネントは、デバイスがイベントを送信するコンポーネントである SEC のインストールを可能にするためののみ必要です。 CDO のオンラインヘルプの説明に従って、次のいずれかを使用します。 <ul style="list-style-type: none"> • (推奨) CDO 提供の VM イメージを使用します。 • CDO 提供のイメージを使用せずに SDC を作成します。 <p>重要手順の前提条件を省略しないでください。ただし、この統合には適用されないオンボーディングに関する情報は無視してください。</p>
ステップ	作成した SDC 仮想マシンに Secure Event Connector (SEC) をインストールします。	これは、デバイスがイベントを送信するコンポーネントです。 Secure Event Connector をインストールするには、CDO のオンラインヘルプを参照してください。 重要手順の前提条件を省略しないでください。ただし、この統合には適用されないオンボーディングに関する情報は無視してください。

	操作手順	詳細情報
ステップ	管理対象デバイスに syslog イベントを SEC に送信させるように Management Center を設定します。	Threat Defense デバイスからのセキュリティ イベント syslog メッセージの送信 (10 ページ)
ステップ	イベントが正常に送信されていることを確認する	イベントの表示および操作 (28 ページ) を参照してください。
ステップ	(オプション) 接続イベントをクラウドに送信していて、それらを Management Center に保存しない場合は、Management Center のストレージを無効にします。	Management Center のオンラインヘルプで、データベースイベント制限に関するトピックにある接続イベントについての情報を参照してください。
ステップ	(オプション) Management Center から CDO への相互起動を設定して、Management Center に表示されるイベントからクラウド内の関連イベントに簡単にピボットできるようにします。	Management Center のオンラインヘルプを参照してください。
ステップ	(任意) CDO の一般設定を指定する	たとえば、シスコのサポートスタッフがデータを使用できないようにすることができます。 CDO のオンラインヘルプで、「 一般設定 」を参照してください。
ステップ	(任意) 同僚がイベントを表示および操作するための CDO ユーザーアカウントを作成する	CDO のオンラインヘルプで、「 新規 CDO ユーザーの作成 」を参照してください。

Syslog を使用した SAL (SaaS) へのイベント送信の概要



①	Management Center 管理対象デバイスがイベントを生成します。
②	Threat Defense デバイスは、サポートされているイベントを syslog メッセージとして、ネットワーク上の仮想マシンにインストールされている Secure Event Connector (SEC) に送信します。
③	SEC はイベントを Cisco クラウドセキュリティ製品に使用される Security Services Exchange (SSE)、クラウド間およびオンプレミス間での識別と認証、およびデータストレージを処理するセキュアな中間クラウドサービスに送信します。

④	SSE は、イベントを Cisco Security Analytics and Logging (SAL) クラウドデータストアに転送します。
⑤	CDO イベントビューアは、イベントについて SAL クラウドデータストアにクエリを実行し、SOC アナリストに追加のコンテキストを提供します。
⑥	(Analytics ライセンスがある場合のみ) Cisco Secure Cloud Analytics (旧 SWC) は、SAL クラウドデータストアからイベントを受信し、SOC アナリストに製品の分析機能へのアクセスを提供します。



(注) CDO ポータルのほとんどの機能は、この統合には適用されません。たとえば、CDO はデバイスを管理しないため、デバイスは CDO にオンボーディングされません。

Threat Defense デバイスからのセキュリティイベント syslog メッセージの送信

この手順では、Management Center によって管理される Threat Defense デバイスからセキュリティイベント（接続、セキュリティ関連接続、侵入、ファイル、およびマルウェアのイベント）の syslog メッセージを送信するためのベストプラクティス設定について説明します。



(注) 多くの Threat Defense syslog 設定は、セキュリティイベントには適していません。この手順で説明するオプションのみを設定してください。

始める前に

- Management Center で、セキュリティイベントを生成するようにポリシーを設定するとともに、予期されるイベントが [分析 (Analysis)] メニューの該当するテーブルに表示されることを確認します。
- syslog サーバーの IP アドレス、ポート、およびプロトコル (UDP または TCP) を収集します。

CDO にサインインします。その後、CDO ブラウザウィンドウの右上にあるユーザーメニューから [セキュアコネクタ (Secure Connectors)] を選択します。[Secure Event Connector] をクリックすると、右側に必要な情報が表示されます。
- デバイスが syslog サーバーに到達できることを確認します。
- 詳細については、Management Center のオンラインヘルプで「接続ロギング」の章を参照してください。

手順

ステップ 1 Management Center の Web インターフェイスにサインインします。

ステップ 2 Threat Defense デバイスの syslog 設定を指定します。

- a) [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] をクリックします。
- b) Threat Defense デバイスに関連付けられているプラットフォーム設定ポリシーを編集します。
- c) 左側のナビゲーションペインで、[Syslog] をクリック。
- d) [syslog サーバー (Syslog Servers)] をクリックし、[追加 (Add)] をクリックして、サーバー、プロトコル、インターフェイス、および関連情報を入力します。

上記の CDO から収集した IP アドレス、ポート、およびプロトコルを使用してください。

EMBLEM 形式とセキュア syslog は、この統合ではサポートされていません。

このページのオプションについて疑問がある場合は、Management Center のオンラインヘルプで「syslog サーバーの設定」のトピックを参照してください。

- e) [syslog 設定 (Syslog Settings)] をクリックし、次の設定を行います。


- **syslog メッセージのタイムスタンプを有効化**
- **タイムスタンプ形式**
- **Enable Syslog Device ID**

- f) [ロギングのセットアップ (Logging Setup)] をクリックします。
- g) [EMBLEM 形式で syslogs を送信 (Send syslogs in EMBLEM format)] がオフになっていることを確認します。
- h) 設定を保存します。

ステップ 3 アクセス コントロール ポリシーの一般的なログ設定 (ファイルおよびマルウェアロギングを含む) を指定します。

- a) [ポリシー (Policies)] > [アクセスコントロール (Access Control)] をクリックします。
- b) 該当するアクセス コントロール ポリシーを編集します。
- c) [ロギング (Logging)] をクリックします。
- d) [FTD 6.3 以降 : デバイスに展開した FTD プラットフォーム設定の syslog 設定を使用する (FTD 6.3 and later: Use the syslog settings configured in the FTD Platform Settings policy deployed on the device)] をオンにします。
- e) (任意) **syslog の重大度** を選択します。
- f) ファイルおよびマルウェアイベントを送信する場合は、[ファイル/マルウェアイベントの syslog メッセージを送信する (Send Syslog messages for File and Malware events)] をオンにします。
- g) [保存 (Save)] をクリックします。

ステップ 4 アクセス コントロール ポリシーのセキュリティ関連接続のイベントのロギングを有効にします。

- a) 同じアクセス コントロール ポリシーで、[セキュリティ インテリジェンス (Security Intelligence)] タブをクリックします。
- b) 次の各場所で、**ロギング** () をクリックし、接続の開始および終了と [syslog サーバー (Syslog Server)] を有効にします。
 - [DNS ポリシー (DNS Policy)] の横。
 - [ブロックリスト (Block List)] ボックスの、[ネットワーク (Networks)] と [URL (URLs)] 。
- c) [保存 (Save)] をクリックします。

ステップ 5 アクセス コントロール ポリシーの各ルールの syslog ロギングを有効にします。

- a) 同じアクセス コントロール ポリシーで、[ルール (Rules)] タブをクリックします。
- b) 編集するルールをクリックします。
- c) ルールの [ロギング (Logging)] タブをクリックします。
- d) 接続の開始時と終了時の両方を有効にします。
- e) ファイルイベントをログに記録する場合は、[ファイルのロギング (Log Files)] を選択します。
- f) [syslog サーバー (Syslog Server)] を有効にします。
- g) ルールが [アクセスコントロールログでデフォルトの syslog 設定を使用する (Using default syslog configuration in Access Control Logging)] であることを確認します。
オーバーライドを設定しないでください。
- h) [追加 (Add)] をクリックします。
- i) ポリシーの各ルールに対して手順を繰り返します。

ステップ 6 侵入イベントを送信する場合は、次の手順を実行します。

- a) アクセス コントロール ポリシーに関連付けられている侵入ポリシーに移動します。
- b) 侵入ポリシーで、[詳細設定 (Advanced Settings)] > [Syslog アラート (Syslog Alerting)] > [有効 (Enabled)] をクリックします。
ポリシーがアクセス コントロール ロギング用に設定されたデフォルト設定を使用していることを確認します。
- c) [戻る (Back)] をクリックします。
- d) 左側にあるナビゲーションウィンドウの [ポリシー情報 (Policy Information)] をクリックします。
- e) [変更を確定 (Commit Changes)] をクリックします。

次のタスク

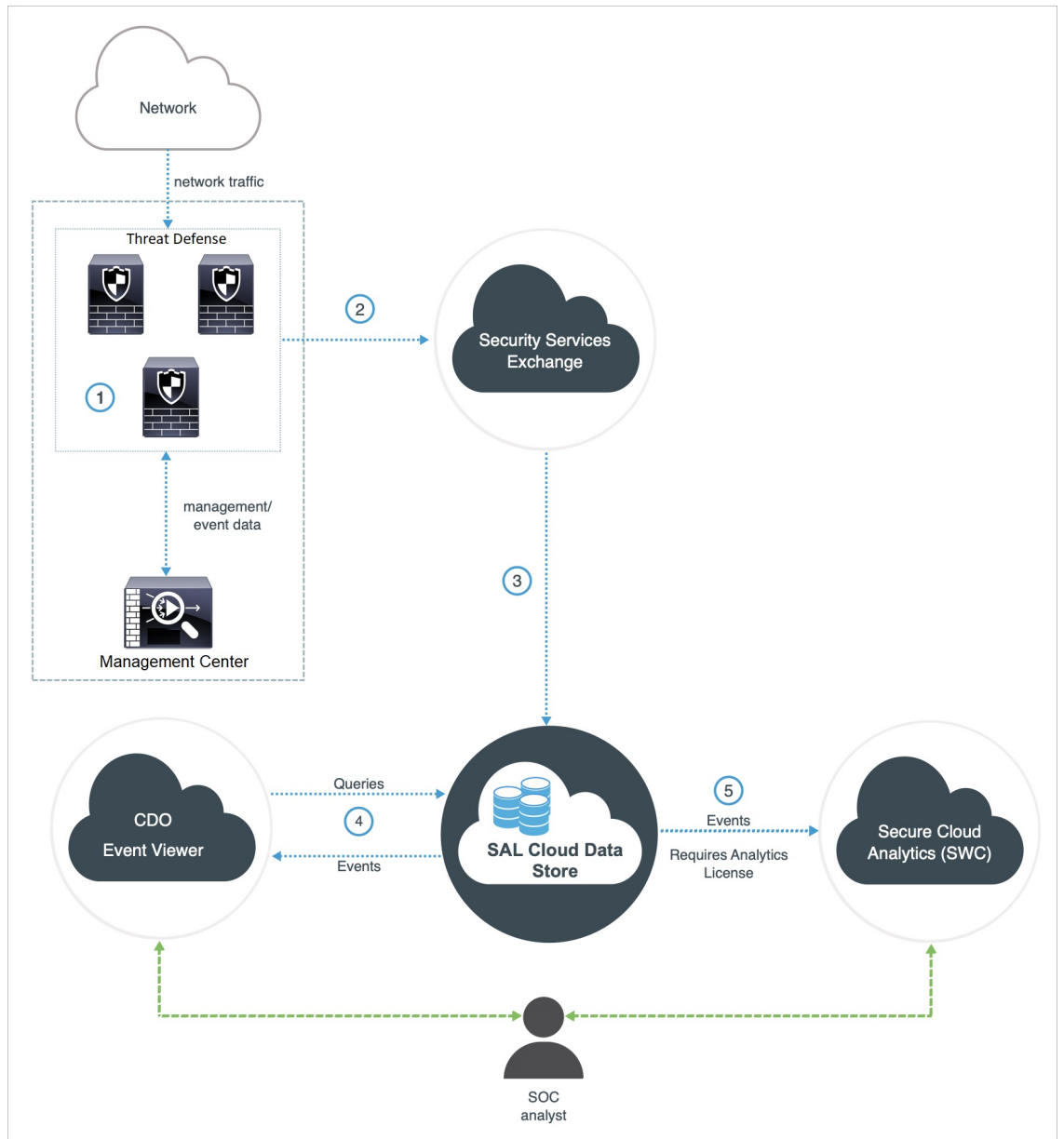
- 変更が完了したら、変更を管理対象デバイスに展開します。

直接接続を使用した SAL (SaaS) でのイベントデータストレージの設定方法

ここでは、直接接続を使用して SAL (SaaS) でイベントデータストレージを設定する方法について説明します。

動作の仕組み

次の図は、直接統合の動作の仕組みを示しています。



①	Management Center 管理対象デバイスがイベントを生成します。
②	Threat Defense デバイスはサポート対象のイベントを Cisco クラウドセキュリティ製品に使用される Security Services Exchange (SSE)、クラウド間およびオンプレミス間での識別と認証、およびデータストレージを処理するセキュアな中間クラウドサービスに送信します。
③	SSE は、イベントを Cisco Security Analytics and Logging (SAL) クラウドデータストアに転送します。
④	CDO イベントビューアは、イベントについて SAL クラウドデータストアにクエリを実行し、SOC アナリストに追加のコンテキストを提供します。
⑤	(Analytics ライセンスがある場合のみ) Cisco Secure Cloud Analytics (旧 SWC) は、SAL クラウドデータストアからイベントを受信し、SOC アナリストに製品の分析機能へのアクセスを提供します。

この統合の主要コンポーネント

コンポーネント	説明
Threat Defense	マルウェアやアプリケーション層攻撃からの保護、統合された侵入防御、クラウド提供型脅威インテリジェンスなど機能を備えた次世代ファイアウォール。
Management Center	複数のプラットフォームで動作する特定のシスコセキュリティ製品の管理における中枢。ポートおよびプロトコル制御、アプリケーション制御、IPS、URL フィルタリング、およびマルウェア防御の機能のために、Threat Defense ソフトウェアを統合して管理します。
Security Services Exchange	シスコのクラウドセキュリティ製品で使用される、クラウド間およびオンプレミスとクラウドの間での識別、認証、およびデータストレージを処理するセキュアな中間クラウドサービス。
CDO	さまざまなセキュリティ製品にわたるセキュリティポリシーの変更を管理するために使用できるクラウドベースのマルチデバイスマネージャー。このプラットフォームにより、分散拠点やその他の高度に分散された環境でポリシーを効率的に管理して、一貫したセキュリティ実装を実現できます。
Cisco Secure Cloud Analytics (旧 Secure Network Analytics Cloud)	動的エンティティモデリングを Threat Defense イベントに適用し、この情報に基づいて検出を生成するクラウドプラットフォーム。これにより、ネットワークから収集されたテレメトリの詳細な分析が可能になり、ネットワークトラフィックの傾向を特定し、異常な動作を調べることができます。

コンポーネント	説明
SecureX	シスコの統合セキュリティレポートフォリオを既存のインフラストラクチャに接続する、シンプルなプラットフォーム エクスペリエンス。可視性の統合、自動化の実現、ネットワーク、エンドポイント、クラウド、アプリケーションのセキュリティ強化に役立ちます。
Cisco SecureX Threat Response	複数の製品やソースから集約されたデータを使用して、脅威を検出、調査、分析、対応するために役立つクラウドプラットフォーム。

直接統合の前提条件

前提条件タイプ	要件
SAL (SaaS) にイベントを送信するための一般的な要件	この表の要件に加えて、 SAL (SaaS) 統合の要件と前提条件 (3 ページ) およびサブトピックの項目を満たす必要があります。
ライセンスング	<p>Cisco Smart Software Manager に Management Center を登録します。</p> <p>Management Center Web インターフェイスで、[System] (⚙) > [Smart Licenses] をクリックして、次のことを確認します。</p> <ul style="list-style-type: none"> • [Usage Authorization] ステータスが [Authorized] になっている。 • [Product Registration] ステータスが [Registered] になっている。 <p>次の点を考慮してください。</p> <ul style="list-style-type: none"> • この統合は評価ライセンスではサポートされていません。 • お使いの環境では Cisco Smart Software Manager オンプレミス サーバー (旧 Smart Software Satellite Server) を使用できないか、またはエアギャップ環境に導入できません。

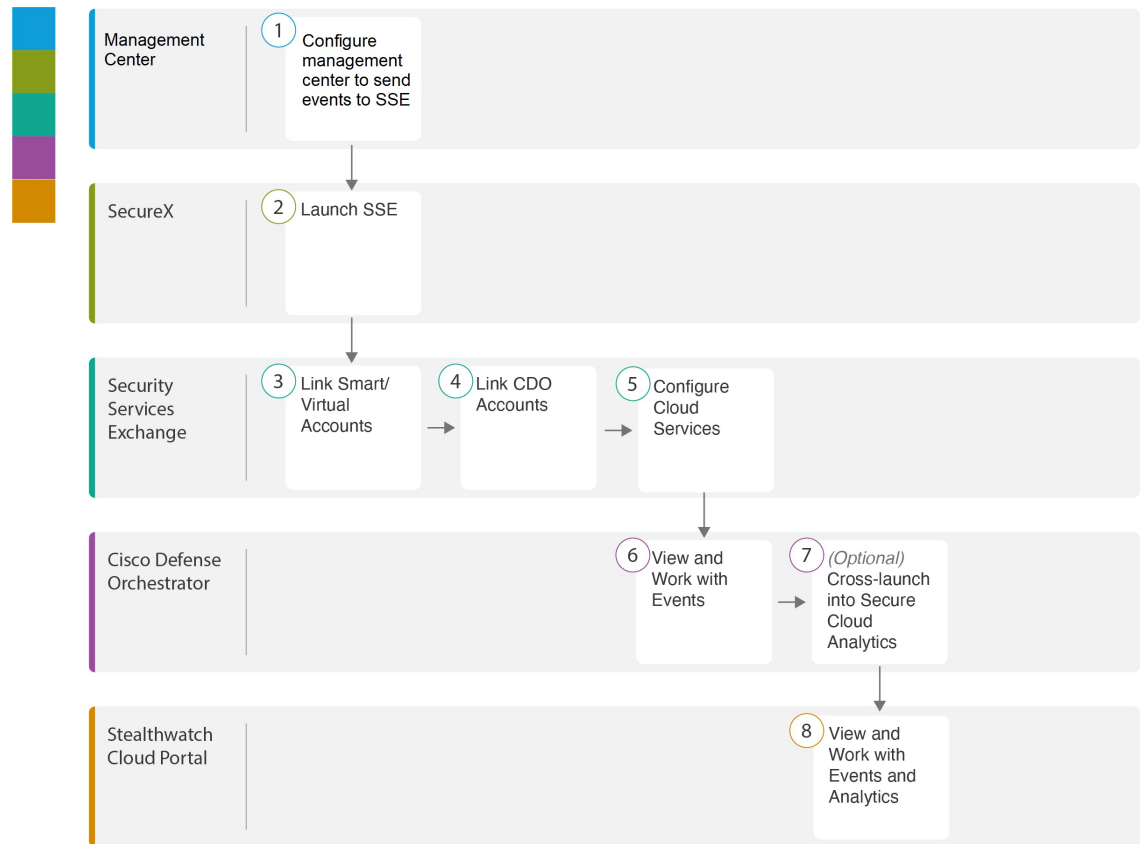
前提条件タイプ	要件
アカウント	<ul style="list-style-type: none"> • 製品のライセンスを取得する Cisco スマート アカウントには管理者権限が必要です。 スマートアカウントのユーザーロールを決定するには、次の手順を実行します。 <ol style="list-style-type: none"> 1. https://software.cisco.com にアクセスします。 2. [Manage Smart Account] をクリックします。 3. ページの右上の領域 ([Help] リンクの上) でスマートアカウントを選択します。 4. [ユーザー (Users)] タブをクリックします。 5. 自分のユーザー ID を検索します。 • Management Center アカウントには次のユーザーロールのいずれかが必要です。 <ul style="list-style-type: none"> • 管理者 • アクセス管理者 • ネットワーク管理者 • セキュリティ承認者 <p>ユーザーロールを決定するには、Management Center Web インターフェイスで [System] (⚙) > [Users] をクリックします。</p> • CDO アカウントには次のユーザーロールのいずれかが必要です。 <ul style="list-style-type: none"> • 管理者 • スーパー管理者 • SecureX アカウントには次のユーザーロールのいずれかが必要です。 <ul style="list-style-type: none"> • 管理者

前提条件タイプ	要件
接続性	<p>Management Center および管理対象デバイスは、ポート 443 で次のアドレスの Cisco Cloud に対してアウトバウンド方向に接続できる必要があります。</p> <ul style="list-style-type: none">• 北米クラウド：<ul style="list-style-type: none">• api.sse.cisco.com• https://eventing-ingest.sse.itd.cisco.com• https://mx01.sse.itd.cisco.com• EU クラウド：<ul style="list-style-type: none">• api.eu.sse.itd.cisco.com• https://eventing-ingest.eu.sse.itd.cisco.com• https://mx01.eu.sse.itd.cisco.com• アジア (APJC) クラウド：<ul style="list-style-type: none">• api.apj.sse.itd.cisco.com• mx01.apj.sse.itd.cisco.com• eventing-ingest.apj.sse.itd.cisco.com

SAL (SaaS) での直接接続を使用したイベントデータストレージの設定

直接統合を使用して、イベントデータストレージを SAL (SaaS) で設定するには、次の手順を実行します。

SAL (SaaS) での直接接続を使用したイベントデータストレージの設定



		ワークスペース
①	Management Center	<ul style="list-style-type: none"> イベントを Security Services Exchange へ送信するように Management Center (バージョン7.1以前) を設定します。(19 ページ)。 Security Services Exchange にイベントを送信するように Management Center (バージョン7.2以降) を設定します。(21 ページ)。
②	SecureX	Security Services Exchange の起動 (22 ページ)
③	Security Services Exchange	Security Services Exchange でのスマートアカウントまたはバーチャルアカウントのリンク (23 ページ)
④	Security Services Exchange	Security Services Exchange での CDO アカウントのリンク (25 ページ)
⑤	Security Services Exchange	Security Services Exchange でのクラウドサービスの設定 (27 ページ)
⑥	CDO	イベントの表示および操作 (28 ページ)

		ワークスペース
⑦	CDO	Cisco Secure Cloud Analytics でのイベントの表示と操作 (28 ページ) : Secure Cloud Analytics を相互起動する
⑧	Cisco Secure Cloud Analytics	Cisco Secure Cloud Analytics でのイベントの表示と操作 (28 ページ)

イベントを **Security Services Exchange** へ送信するように **Management Center** (バージョン 7.1 以前) を設定します。

Management Center のバージョンが 7.1 以前 (バージョン 7.0.2 を除く) の場合は、次の手順に従って、管理対象の Threat Defense デバイスがイベントを SSE へ直接送信するように Management Center を設定します。Management Center のバージョンが 7.0.2 の場合は、[Security Services Exchange](#) にイベントを送信するように Management Center (バージョン 7.2 以降) を設定します。

始める前に

Management Center Web インターフェイスで、次の手順を実行します。

- [System] > [Configuration] ページに移動し、クラウドの [Devices] リストで明確に識別される一意の名前を Management Center に付けます。
- Threat Defense デバイスを Management Center に追加し、それらにライセンスを割り当て、システムが正常に動作することを確認します。必要なポリシーを作成し、生成されたイベントが Management Center Web インターフェイスの [分析 (Analysis)] タブに想定どおりに表示されていることを確認します。

手順

ステップ 1 Management Center Web インターフェイスで、[システム (System)] > [統合 (Integration)] をクリックします。

ステップ 2 [Cisco Cloud リージョン (Cisco Cloud Region)] ウィジェットで、[地域 (Region)] ドロップダウンリストから地域クラウドを選択し、[保存 (Save)] をクリックします。

(注) すでに Management Center が選択した地域クラウドに登録されている場合は、[保存 (Save)] ボタンが非アクティブになります。

この手順で選択した地域は、Cisco Support Diagnostics およびシスコ サポート ネットワーク機能にも使用されます (該当し有効にしている場合)。

地域クラウドを選択する場合は、次の点を考慮してください。

- 可能な場合は、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。

イベントを Security Services Exchange へ送信するように Management Center (バージョン 7.1 以前) を設定します。

- 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。
- 地域クラウドごとにアカウントを作成でき、各クラウドのデータは個別に維持されます。

ステップ 3 [Cisco Cloud イベントの設定 (Cisco Cloud Event Configuration)] ウィジェットで、イベントを SSE に送信するように Management Center を設定します。

1. [Cisco Cloud イベントの設定 (Cisco Cloud Event Configuration)] スライダをクリックして、設定を有効にします。
2. SSE に送信するイベントのタイプを有効または無効にします。

(注) クラウドに送信するイベントを複数の統合で使用できます。次の表を参照してください。

統合	サポートされるイベントのオプション	注意
セキュリティ分析とロギング	すべて (All)	高プライオリティ接続イベントには次のものがあります。 <ul style="list-style-type: none"> • セキュリティ関連の接続イベント。 • ファイルおよびマルウェアイベントに関連する接続イベント。 • 侵入イベントに関連する接続イベント。
シスコ SecureX と Cisco SecureX Threat Response	お使いのバージョンに応じて、以下が含まれます。 <ul style="list-style-type: none"> • 一部の接続イベント • Intrusion • ファイルおよびマルウェアのイベント 	すべての接続イベントを送信する場合、Cisco SecureX と Cisco SecureX Threat Response ではセキュリティイベントのみサポートされます。

3. [保存 (Save)] をクリックします。

ステップ 4 [保存 (Save)] をクリックします。

次のタスク

[Security Services Exchange の起動 \(22 ページ\)](#)

Security Services Exchange にイベントを送信するように Management Center (バージョン 7.2 以降) を設定します。

Management Center のバージョンが 7.0.2 または 7.2 以降の場合は、次の手順に従って、管理対象のデバイスがイベントを SSE へ直接送信するように Management Center を設定します。

始める前に

Management Center Web インターフェイスで、次の手順を実行します。

- [System] > [Configuration] ページに移動し、クラウドの [Devices] リストで明確に識別される一意の名前を Management Center に付けます。
- Threat Defense デバイスを Management Center に追加し、それらにライセンスを割り当て、システムが正常に動作することを確認します。必要なポリシーを作成し、生成されたイベントが Management Center Web インターフェイスの [分析 (Analysis)] タブに想定どおりに表示されていることを確認します。

手順

ステップ 1 Management Center で [Integration] > [SecureX] の順に選択します。

ステップ 2 [Current Region] ドロップダウンから地域クラウドを選択します。

(注) SecureX が有効になっていて、Management Center が選択した地域クラウドに登録されている場合、地域クラウドを変更すると SecureX が無効になります。地域クラウドを変更した後、SecureX を再度有効にすることができます。

地域クラウドを選択する場合は、次の点を考慮してください。

- 可能な場合は、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。
- 地域クラウドごとにアカウントを作成でき、各クラウドのデータは個別に維持されます。

ステップ 3 Cisco Cloud のイベント設定を有効にして、クラウドに送信するイベントのタイプを選択します。

1. [Send events to the cloud] チェックボックスをオンにして、設定を有効にします。
2. クラウドに送信するイベントのタイプを選択します。

(注) クラウドに送信するイベントを複数の統合で使用できます。次の表を参照してください。

統合	サポートされるイベントのオプション	注意
セキュリティ分析とロギング	すべて (All)	高プライオリティ接続イベントには次のものがあります。 <ul style="list-style-type: none"> • セキュリティ関連の接続イベント。 • ファイルおよびマルウェアイベントに関連する接続イベント。 • 侵入イベントに関連する接続イベント。
シスコ SecureX と Cisco SecureX Threat Response	お使いのバージョンに応じて、以下が含まれます。 <ul style="list-style-type: none"> • 一部の接続イベント • Intrusion • ファイルおよびマルウェアのイベント 	すべての接続イベントを送信する場合、Cisco SecureX と Cisco SecureX Threat Response ではセキュリティイベントのみサポートされます。

- (注)
- [侵入イベント (Intrusion Events)] を有効にすると、Management Center デバイスは影響フラグとともにイベントデータを送信します。
 - [File and Malware Events] を有効にすると、Threat Defense デバイスから送信されるイベントに加えて、レトロスペクティブイベントが Management Center デバイスから送信されます。

ステップ 4 [保存 (Save)] をクリックします。

次のタスク

[Security Services Exchange の起動 \(22 ページ\)](#)

Security Services Exchange の起動

手順

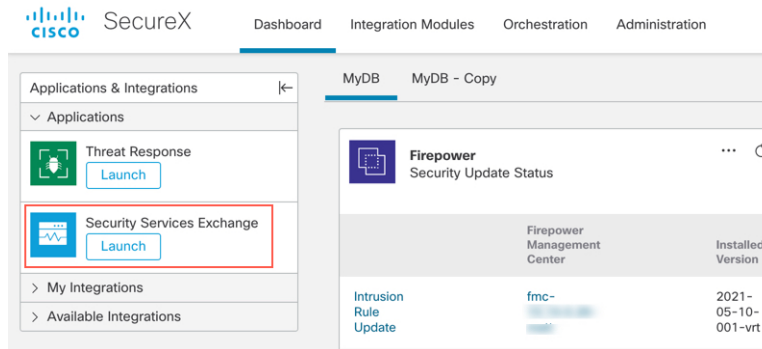
ステップ 1 <https://sign-on.security.cisco.com> にアクセスします。

ステップ 2 SecureX サインオンアカウントを使用してサインインします。

ステップ 3 プロンプトが表示されたら、Duo Security を使用して認証します。

ステップ 4 SecureX を起動する地域を選択します。

ステップ 5 [アプリケーションと統合 (Applications & Integrations)] ペインで、[アプリケーション (Applications)] > [Security Services Exchange] の下にある [起動 (Launch)] をクリックします。



新しいタブに Security Services Exchange ポータルが開きます。

次のタスク

[Security Services Exchange でのスマートアカウントまたはバーチャルアカウントのリンク \(23 ページ\)](#)

Security Services Exchange でのスマートアカウントまたはバーチャルアカウントのリンク

異なるライセンス管理スマートアカウント（またはバーチャルアカウント）に登録されている製品をクラウド内の単一のビューに統合するには、それらのライセンス管理アカウントを SSE へのアクセスに使用するアカウントにリンクする必要があります。

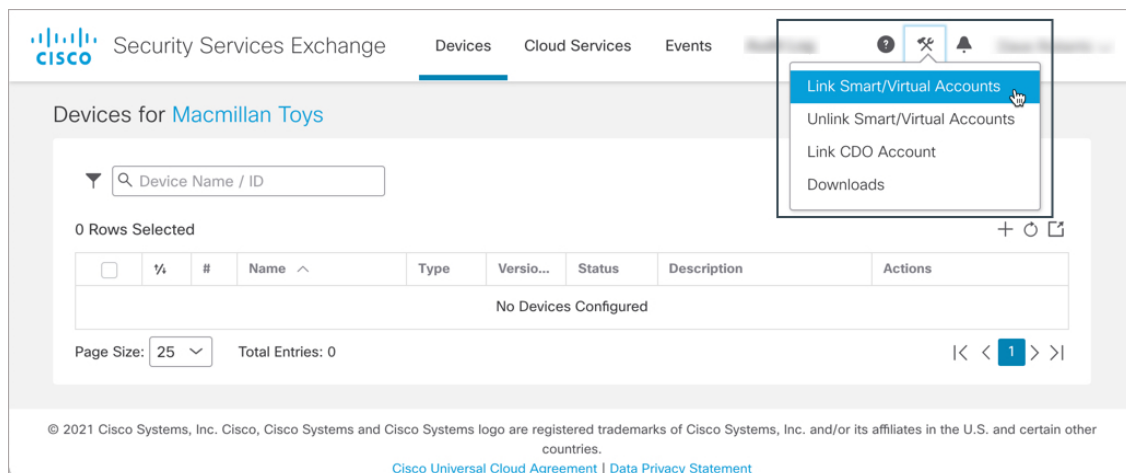
始める前に

- ライセンス管理アカウントをリンクするには、（製品のライセンスを取得する）すべてのライセンス管理アカウントと SecureX/SSE へのアクセスに使用するアカウントに、管理者レベルのスマートアカウントまたはバーチャルアカウントの権限が必要です。
- Cisco SecureX Threat Response で使用するためにすでにリンクされたアカウントがある場合は、SAL (SaaS) のためにそれらのアカウントを再度リンクする必要はなく、その逆も同様です。
- この手順を実行するには、Cisco.com のログイン情報が必要になります。

手順

ステップ 1 [Security Services Exchange の起動 \(22 ページ\)](#)。

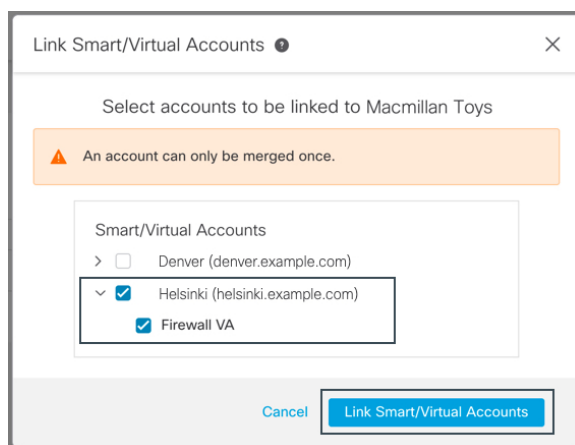
ステップ 2 右上隅にある [ツール (Tools)] ボタン (☒) をクリックし、[スマート/バーチャルアカウントのリンク (Link Smart/Virtual Accounts)] を選択します。



ステップ 3 [Link More Accounts] をクリックします。

ステップ 4 サインインを要求されたら、Cisco.com のログイン情報を使用してサインインします。

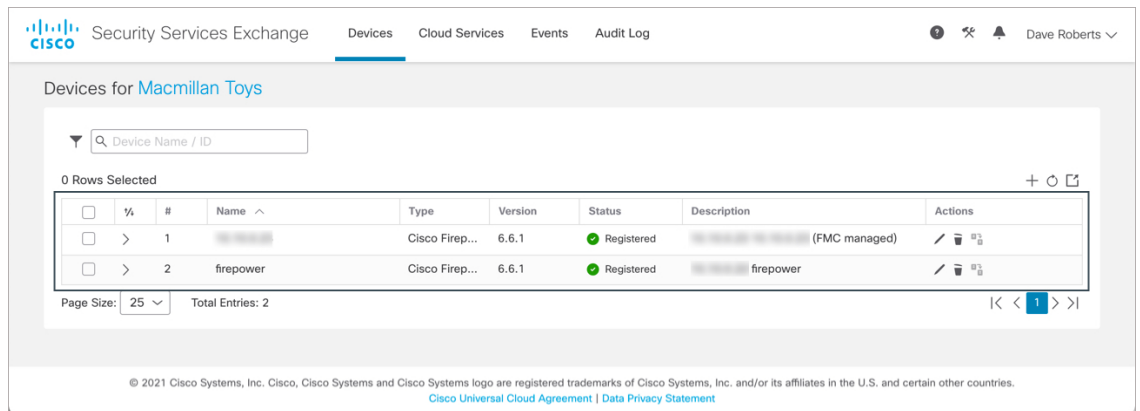
ステップ 5 このクラウドアカウントと統合するアカウントを選択します。



ステップ 6 [スマート/バーチャルアカウントのリンク (Link Smart/Virtual Accounts)] をクリックします。

ステップ 7 [OK] をクリックして、先へ進みます。

ステップ 8 Management Center とその管理対象デバイスが [デバイス (Devices)] タブに表示されていることを確認します。



次のタスク

[Security Services Exchange での CDO アカウントのリンク \(25 ページ\)](#)

Security Services Exchange での CDO アカウントのリンク

CDO アカウントを、SSE のデバイスに関連付けられているアカウントとマージする必要があります。

次の点を考慮してください。

- 1 つの SecureX/Cisco SecureX 脅威応答アカウントにマージできる CDO テナントは 1 つだけです。
- 複数の地域クラウドに異なるアカウントがある場合は、地域クラウドごとに個別にアカウントをマージする必要があります。
- SecureX クラウドのアカウントをマージする場合は、同じクラウドで Cisco SecureX Threat Response に対して再度マージする必要はありません。逆も同様です。

始める前に

- CDO ユーザーアカウントには管理者またはネットワーク管理者の権限が必要です。
- SSE へのアクセスに使用する SecureX または Cisco SecureX Threat Response のアカウントに管理者権限が必要であることを確認してください。
- CDO で、アカウントの新しい API トークンを生成します。
 1. マージするアカウントのログイン情報を使用して、適切な地域 CDO ポータルにサインインします。たとえば、米国のクラウドは <https://defenseorchestrator.com> で、EU のクラウドは <https://defenseorchestrator.eu> です。
 2. マージするテナントアカウントを選択します。
 3. ウィンドウの右上隅にあるユーザーメニューから、[設定 (Settings)] を選択します。

4. [My Tokens] セクションで、[Generate API Token] または [Refresh] をクリックします。
5. トークンをコピーします。

API トークンの詳細については、CDO のオンラインヘルプ

(https://docs.defenseorchestrator.com/Configuration_Guides/Devices_and_Services/API_Tokens)
を参照してください。

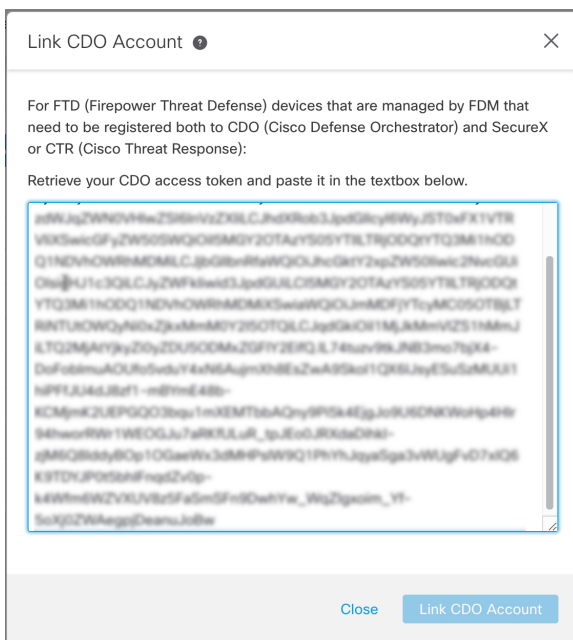
手順

ステップ 1 Security Services Exchange の起動 (22 ページ)。

ステップ 2 右上隅にある [ツール (Tools)] ボタン (🔧) をクリックし、[CDO アカウントのリンク (Link CDO Account)] を選択します。

The screenshot shows the Cisco Security Services Exchange interface. The top navigation bar includes 'Security Services Exchange', 'Devices', 'Cloud Services', 'Events', and 'Audit Log'. The user 'Dave Roberts' is logged in. A dropdown menu is open, showing options: 'Link Smart/Virtual Accounts', 'Unlink Smart/Virtual Accounts', 'Link CDO Account' (highlighted), and 'Downloads'. Below the menu, a table titled 'Devices for Macmillan Toys' is visible, showing 4 rows of device information. The table columns are: % (checkbox), #, Name, Type, Version, Status, Description, and Actions. The first row shows a Cisco Firepower device with version 6.6.1 and status 'Registered'. The other three rows show Cisco Firepower devices with version 7.0.0 and status 'Registered'. The page size is set to 25, and there are 6 total entries.

ステップ 3 CDO からコピーしたトークンを貼り付けます。



ステップ 4 リンクする目的のアカウントをリンクしていることを確認し、[CDOアカウントのリンク (Link CDO Account)] をクリックします。

次のタスク

[Security Services Exchange でのクラウドサービスの設定 \(27 ページ\)](#)

Security Services Exchange でのクラウドサービスの設定

手順

ステップ 1 [Security Services Exchange の起動 \(22 ページ\)](#)。

ステップ 2 [クラウドサービス (Cloud Services)] タブをクリックします。

ステップ 3 イベントサービスオプションが有効になっていることを確認します。

ステップ 4 [イベント (Events)] タブにイベントが予想どおりに表示されていることを確認します。

次のタスク

- [イベントの表示および操作 \(28 ページ\)](#)
- [Cisco Secure Cloud Analytics でのイベントの表示と操作 \(28 ページ\)](#)

イベントの表示および操作

クラウドでイベントを表示および検索するには、次の手順を実行します。

手順

ステップ 1 ブラウザを使用して、イベントの送信先の地域 CDO クラウドに移動します。

- 北米 :
<http://www.defenseorchestrator.com>
- 欧州 :
<http://www.defenseorchestrator.eu>

ステップ 2 CDO にサインインします。

ステップ 3 ナビゲーションバーから、[モニタリング (Monitoring)] > [イベントロギング (Event Logging)] を選択します。

ステップ 4 [履歴 (Historical)] タブを使用して履歴イベントデータを表示します。デフォルトでは、このタブがビューアに表示されます。

ステップ 5 ライブイベントを表示するには、[ライブ (Live)] タブをクリックします。

このページで実行できることの詳細については、CDO のオンラインヘルプで [イベント表示](#) の手順を参照してください。

次のタスク

Logging Analytics and Detection ライセンスまたは **Total Network Analytics and Detection** ライセンスがある場合は、[CDO のオンラインヘルプ](#) で手順を参照して Stealthwatch Cloud ポータルを相互起動してください。

Cisco Secure Cloud Analytics でのイベントの表示と操作

Cisco Secure Cloud Analytics でイベントを表示および検索するには、次の手順を実行します。

手順

ステップ 1 マージするアカウントのログイン情報を使用して、適切な地域 CDO サイトにサインインします。たとえば、米国のクラウドは <https://defenseorchestrator.com> で、EU のクラウドは <https://defenseorchestrator.eu> です。

ステップ 2 ナビゲーションバーから [モニタリング (Monitoring)] > [セキュリティ分析 (Security Analytics)] を選択します。

新しいブラウザタブに Stealthwatch Cloud ポータルが開きます。

ステップ 3 (1回限りのアクティビティ) イベントのシームレスなフローを確保するには、イベントビューアを使用する前に、Stealthwatch Cloud ポータルで次の手順を実行します。

1. Secure Cloud Analytics が正しい CDO テナントと統合されているかどうかを確認します。CDO テナントを表示するには、[設定 (Settings)] > [センサー (Settings)] をクリックします。
2. 監視するサブネットを Secure Cloud Analytics に追加します。サブネットを追加するには、[設定 (Settings)] > [サブネット (Subnets)] をクリックします。

詳細については、Secure Cloud Analytics のオンラインヘルプを参照してください。

ステップ 4 イベントを表示するには、[調査 (Investigate)] > [イベントビューア (Event Viewer)] をクリックします。

詳細については、Secure Cloud Analytics のオンラインヘルプを参照してください。

よくある質問

SAL に関する詳細情報はどこで入手できますか。

SAL の「[使用する前に](#)」と「[よくある質問](#)」も参照してください。

デバイスを **CDO** にオンボードする必要はありますか。

いいえ。デバイスを CDO にオンボードしないでください。

SecureX または **Cisco Threat Response** を使用する場合、**CDO** アカウントをマージする必要はありますか。

[直接接続を使用した SAL \(SaaS\) でのイベントデータストレージの設定方法 \(13 ページ\)](#) で説明されているプロセスを使用して、イベントをクラウドに直接送信する場合のみ。

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。