クラウドへのイベントの直接送信

- 直接統合について （1 ページ）
- 直接統合の要件 （1 ページ）
- Cisco Cloud にイベントを直接送信する方法 （4 ページ）
- 直接統合のトラブルシューティング （13 ページ）

直接統合について

Firepower リリース 6.4 以降では、サポートされているイベントを Firepower Threat Defense（FTD）デバイスから Cisco Cloud へ直接送信するように Firepower システムを設定できます。

具体的には、Firepower デバイスが Security Services Exchange（SSE）にイベントを送信し、そこから、それらのイベントを Cisco SecureX Threat Response に表示されるインシデントに自動的に、または手動で昇格させることができます。

直接統合の要件

要件のタイプ	要件
Firepower デバイス	Firepower Threat Defense デバイス • によって管理 Firepower Management Center • Firepower Device Manager によって管理

要件のタイプ	要件
Firepower のバージョン	US クラウド：6.4 以降 EU クラウド：6.5以降 APJC クラウド：6.5以降 バージョン要件は、デバイスと FMC の両方に適用されます（該当する場合）。
ライセンシング	この統合には特別なライセンスは必要ありません。ただし、これらのオプションの内容に注意してください。 • Cisco SecureX Threat Response に表示するイベントを生成するには、Firepower システムにライセンスが必要です。 詳細については、「https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-licensing-information-listing.html」を参照してください。 • この機能は Firepower 評価ライセンスではサポートされていません。 • この環境は Cisco Smart Software Satellite サーバを使用できないか、またはエアギャップ環境に導入できません。
アカウント	直接統合のアカウントの要件 （3 ページ）を参照してください。

要件のタイプ	要件
接続	FMC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。 • 北米クラウド： • api sse.cisco.com • https://eventing-ingest.sse.itd.cisco.com • https://mx01.sse.itd.cisco.com • EU クラウド（Firepower 6.5以降）： • api sse.cisco.com • 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（Firepower 6.5以降）： • api.apj.sse.itd.cisco.com • mx01.apj.sse.itd.cisco.com • eventing-ingest.apj.sse.itd.cisco.com
全般	Firepower システムが予期したとおりにイベントを生成しています。

直接統合のアカウントの要件

- Firepower イベントデータを送信する地域クラウドのアカウントが必要です。

  サポートされているアカウントタイプについては、Cisco SecureX Threat Response のアクセスに必要なアカウント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のアカウントをお持ちの場合は、別のアカウントを作成しないでください。異なるアカウントのデータを集約またはマージすることはできません。

  アカウントを取得するには、にアクセスするためのアカウントの取得 Cisco SecureX Threat Responseを参照してください。

  クラウドアカウントには管理者レベルの権限が必要です。

- 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 ロールを特定するには、https://software.cisco.com に移動して [スマート アカウントの管理（Manage Smart Account）] をクリックし、ページの右上の領

域にあるスマート アカウントを選択し、[ユーザ（Users）] をクリックしてユーザ ID を検索します。

- 使用権ライセンスのスマート アカウントと、クラウドへのアクセスに使用するアカウントの両方が同じ Cisco CCO アカウントに関連付けられている必要があります。
- Firepower アカウントには次のユーザ ロールのいずれかが必要です。
  - 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

Cisco Cloud にイベントを直接送信する方法

（注） デバイスがすでにクラウドにイベントを送信している場合は、イベントの再送信を設定する必要はありません。SecureX および Cisco SecureX Threat Response は、同じイベントデータのセットを使用します。

	操作手順	詳細情報
ステップ	送信するイベント、それらのイベントの送信方法、使用する地域クラウドなどを決定します。	次のトピックを参照してください。 Firepower との統合に関する重要な情報： Cisco SecureX Threat Response
ステップ	要件を満たす。	直接統合の要件 （1 ページ） およびそれらのサブトピック。
ステップ	ブラウザで、デバイスを管理し、イベントをフィルタ処理するために使用する Cisco SecureX Threat Response のクラウドポータルである Security Services Exchange にアクセスする。	アクセス Security Services Exchange （6 ページ） を参照してください。
ステップ	（FDMのみ）CDO を使用して FTD デバイスの設定を管理する場合は、CDO アカウントを、このドキュメントで説明するサービスに使用するアカウントとマージする必要があります。	（FDM が管理する FTD のみ）CDO アカウントとセキュリティアカウントのマージ （7 ページ） を参照してください。

	操作手順	詳細情報
ステップ	Security Services Exchange で、組織内のさまざまなアカウントに登録されたデバイスからデータを表示して操作できるようにライセンスアカウントをリンクする。	スマートライセンスアカウントのリンク （8 ページ）を参照してください。
ステップ	Security Services Exchange でイベント サービスを有効にする。	[クラウドサービス（Cloud Services）] をクリックして次のオプションを有効にします。 • **Cisco SecureX Threat Response** • **イベント**
ステップ	Firepower 製品で、Cisco Cloud との統合を有効にする。	**ヒント**：これらのトピックの前提条件をスキップしないでください。 • Firepower Device Manager（FDM）によって管理されているデバイスの場合は次を参照してください。 Cisco Cloud にイベントを送信するための FDM の設定 （9 ページ） • Firepower Management Center（FMC）によって管理されているデバイスの場合は次を参照してください。 Cisco Cloud にイベントを送信するための FMC So デバイスの設定 （11 ページ）
ステップ	Firepower システムがイベントを生成する時間を確保します。	--
ステップ	統合が正しくセットアップされていることを確認する。 必要に応じて問題をトラブルシューティングする。	参照先： • イベントが Security Services Exchange に到達しているか（直接接続）の確認 （12 ページ） • 直接統合のトラブルシューティング （13 ページ）
ステップ	重要でない特定のイベントを自動的に削除し、特定のイベントを自動的にインシデントに昇格させてに表示されるようにCisco SecureX Threat Response Security Services Exchange を設定する。	イベントのフィルタ処理とイベントの昇格については、Security Services Exchange のオンライン ヘルプの情報を参照してください。 SSE にアクセスするには、アクセス Security Services Exchange （6 ページ）を参照

	操作手順	詳細情報
ステップ	SecureX で、Firepower モジュールを追加します。 このモジュールが設定されている場合、CTR は、侵入イベントがまだ昇格されていない場合でも、SSE 内の侵入イベントからの検知物を返します。	SecureX で、[Integration Modules] > [Available Integration Modules] に移動して、Firepower モジュールを追加します。 このモジュールの詳細については、SecureX でオンラインヘルプを参照してください。
ステップ	Cisco SecureX Threat Response で、昇格したイベントが予期したとおりに Incident Manager に表示されることを確認します。	Cisco SecureX Threat Response で [インシデント（Incidents）] をクリックします。

アクセス Security Services Exchange

始める前に

ブラウザで、ポップアップのブロッキングを無効にします。

手順

ステップ 1 ブラウザウィンドウで、お客様のCisco SecureX Threat Response クラウドに移動します。

- 北米クラウド： https://visibility.amp.cisco.com
- ヨーロッパのクラウド： https://visibility.eu.amp.cisco.com
- アジア クラウド： https://visibility.apjc.amp.cisco.com

ステップ 2 SecureX、エンドポイント向け AMP、Cisco Threat Grid、またはシスコのセキュリティアカウントのログイン情報を使用してサインインします。

お客様のアカウントログイン情報は、地域クラウドに固有のものです。

ステップ 3 Security Services Exchange に移動します。

[モジュール（Modules）] > [デバイス（Devices）] > [管理デバイス（Managing Devices）] を選択します。

Security Services Exchange が新しいブラウザ ウィンドウに開きます。

（FDM が管理する FTD のみ）CDO アカウントとセキュリティアカウントのマージ

FDM 管理対象 Firepower Threat Defense（FTD）デバイスを Cisco Defense Orchestrator（CDO）、および SecureX または Cisco SecureX Threat Responseで使用する場合は、CDO アカウントを SecureX または Cisco SecureX Threat Response 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。

1つの SecureX/Cisco SecureX Threat Response 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。

この操作は元に戻せません。

始める前に

マージする必要があるアカウントのログイン情報を使用して、CDO および該当する地域の SecureX または Cisco SecureX Threat Response クラウドにサインインできる必要があります。

CDO ユーザアカウントには管理者またはネットワーク管理者権限が必要です。

SecureX または Cisco SecureX Threat Response アカウントには管理者権限が必要です。

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、US クラウドは https://defenseorchestrator.com、EU クラウドは https://defenseorchestrator.eu です。

ステップ 2 マージするテナントアカウントを選択します。

ステップ 3 CDO で、アカウントの新しい API トークンを生成します。

a) ウィンドウの右上隅にあるユーザメニューから、[Settings] を選択します。

b) [My Tokens] セクションで、[Generate API Token] または [Refresh] をクリックします。

c) トークンをコピーします。

API トークンの詳細については、次の CDO のオンラインヘルプを参照してください。
https://docs.defenseorchestrator.com/Configuration_Guides/Devices_and_Services/API_Tokens

ステップ 4 まだ Security Services Exchange（SSE）を確認していない場合：

a) マージするアカウントを使用して、該当する SecureX 地域クラウドにサインインします。

b) Security Services Exchange に移動します。

SecureX で、[Administration] > [Devices] > [Manage Devices] を選択します。

Security Services Exchange が新しいブラウザ ウィンドウに開きます。

ステップ 5 SSE で、任意のページの右上から > [Link CDO Account] をクリックします。

ステップ 6 CDO からコピーしたトークンを貼り付けます。

ステップ 7 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ます。

ステップ 8 [Link CDO Account] をクリックします。

次のタスク

- この手順の結果、アカウントのクレデンシャルは変更されません。マージ後も、アカウントのマージ前に使用していた各製品（CDO、SecureX、CTRなど）に同じログイン情報を使用してアクセスします。
- デバイスを SSE に登録する前にこの手順を完了した場合：

  Cisco Cloud にイベントを直接送信する方法 （4 ページ）の手順に進みます。
- CDO と SecureX または Cisco SecureX Threat Response の統合用にデバイスを登録した後にこの手順を実行した場合は、SSE の [Devices] ページでデバイスインスタンスが重複している可能性があります。

  この場合、以前に CDO 登録に関連付けたデバイスのインスタンスは、SecureX または Cisco SecureX Threat Response の統合に使用されるアカウントにも関連付けられています。

  マージ前にデバイスによって生成されたイベントは、マージ後に同じデバイスによって生成されたイベントとは異なるデバイス ID を持ちます。

  イベントを生成したデバイスにイベントをマッピングする必要がない場合は、マージされたアカウントに関連付けられたデバイスの [Unregistered] デバイスエントリを削除できます。

スマートライセンス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 SecureX および Cisco SecureX Threat Response 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、すべてのライセンス管理アカウントと SecureX または Cisco SecureX Threat Response 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権限が必要です。
- リンクされたアカウントを表示するにはユーザ レベルのアカウントで十分です。

- Cisco SecureX Threat Response で使用するアカウントがリンク済みの場合は、SecureX 用に再度リンクする必要はありません。その逆も同様です。
- この手順を実行するには、Cisco.com（CCO）のクレデンシャルが必要になります。

手順

ステップ 1 Security Services Exchange の任意のページの右上隅にあるツールボタン（🛠）をクリックし、[Link Accounts] を選択します。

ステップ 2 [Link More Accounts] をクリックします。

ステップ 3 サインインを要求されたら、Cisco.com（CCO）のログイン情報を使用してサインインします。

ステップ 4 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 5 [アカウントのリンク（Link Accounts）] をクリックします。

スマートライセンスアカウントのリンク解除

現在リンクされているスマートライセンスアカウントのリンクを解除する必要がある場合は、Security Services Exchange（SSE）のオンラインヘルプの手順を参照してください。

Cisco Cloud にイベントを送信するための FDM の設定

（注） 使用可能なオプションは、FDM のバージョンによって異なります。ご使用のバージョンに該当しない手順はスキップしてください。たとえば、地域およびイベントタイプを選択する機能はバージョンによって異なります。

始める前に

- Cisco Cloud にイベントを直接送信する方法 （4 ページ） でここまでのステップを実行します。
- FDM で、デバイスの名前が一意であることを確認します。一意でない場合は、この時点で [デバイス（Device）] > [システム設定（System Settings）] > [ホスト名（Hostname）] で割り当てます。
- FDM で、少なくとも 1 つのアクセス制御ルールに侵入ポリシーおよびその他の適用されるポリシーを適用し、デバイスが正常にイベントを生成していることを確認します。
- クラウドログイン情報があり、アカウントが作成された Cisco SecureX Threat Response 地域クラウドにサインインできることを確認します。

  URL については、Cisco SecureX Threat Response 地域クラウドを参照してください。

- ブラウザで次の手順を実行します。
  - ポップアップ ブロッキングの無効化
  - サードパーティの Cookie の許可

手順

ステップ 1 Firepower Device Manager で、[デバイス（Device）] をクリックし、**[システム設定（System Settings）]** > **[クラウド サービス（Cloud Services）]** をクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [クラウド サービス（Cloud Services）] をクリックします。

ステップ 2 地域クラウドをまだ選択していない場合は、アカウントを作成した地域を選択します。

ステップ 3 クラウドに送信するイベントのタイプを選択します。

ステップ 4 [Cisco Threat Response] 機能の [有効にする（Enable）] コントロールをクリックします。

プロンプトが表示されたら、開示情報を読み、[承認（Accept）] をクリックします。

ステップ 5 Security Services Exchange にデバイスが正常に登録されたことを確認します。

a) ブラウザ ウィンドウに Security Services Exchange をまだ表示していない場合は、アクセス Security Services Exchange （6 ページ）を参照してください。

b) Security Services Exchange で、[デバイス（Devices）] をクリックします。

c) Firepower Threat Defense デバイスがリストに表示されていることを確認します。

注：[デバイス（Devices）] リストの FTD デバイスに表示される説明はシリアル番号であり、デバイスのコマンド ライン インターフェイスで **show running-config** コマンドを実行した場合に表示されるシリアル番号と一致します。

次のタスク

- 展開がハイアベイラビリティ構成の場合は、追加の手順について FDM のオンラインヘルプを参照してください。
- Cisco Cloud にイベントを直接送信する方法 （4 ページ）の残りのステップを続行します。

重要 これを設定した後に Cisco Defense Orchestrator との統合を有効にすると、デバイスが SSE から登録解除される場合があります。SSE の [Devices] タブでこの問題が確認された場合は、（FDM が管理する FTD のみ）CDO アカウントとセキュリティアカウントのマージ （7 ページ）を参照してください。

Cisco Cloud にイベントを送信するための FMC So デバイスの設定

管理対象の Firepower Threat Defense デバイスにイベントを直接クラウドに送信させるように Firepower Management Center を設定します。

（注） 使用可能なオプションは、FMC のバージョンによって異なります。ご使用のバージョンに該当しない手順はスキップしてください。

始める前に

- Firepower Management Center で次の手順を実行します。
  - [システム（System）] > [設定（Configuration）] ページに移動し、クラウドの [デバイス（Devices）] リストで明確に識別される一意の名前を FMC に付けます。
  - FTD デバイスを FMC 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していることを確認します（つまり、必要なポリシーが作成されており、イベントが生成されて [分析（Analysis）] タブの Firepower Management Center の Web インターフェイスに予期していたとおりに表示されています）。
- Cisco Cloud にイベントを直接送信する方法 （4 ページ） でここまでのステップを実行します。
- クラウドログイン情報があり、アカウントが作成された Cisco SecureX Threat Response 地域クラウドにサインインできることを確認します。

  URL については、Cisco SecureX Threat Response 地域クラウドを参照してください。

手順

ステップ 1 Firepower Management Center で [システム（System）] > [統合（Integration）] を選択します。

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

ステップ 3 [Cisco Cloud] または [Cisco Cloud Event Configuration]（FMC のバージョンによって異なります）のスライダを有効にします。

ステップ 4 （まだ選択していない場合）アカウントを作成した [Cisco Cloud Region] を選択します。

ステップ 5 クラウドに送信するイベントのタイプを有効にします。

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。

- セキュリティ インテリジェンスの接続イベント
- 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

ステップ 6 [保存（Save）] をクリックします。

[保存（Save）] ボタンが使用できない場合は、すでに FMC が選択した地域クラウドに登録されていることを意味します。

ステップ 7 機能が正常に有効化されていることを確認します。

a) システムが同期されるまで数分間待ちます。
b) 機能を有効にしたのと同じページで Cisco Cloud の設定を表示するためのリンクをクリックします（リンクは同じ [Cisco Cloud] ボックス内にあります）。

Security Services Exchange が新しいブラウザ ウィンドウで開きます。

c) Cisco SecureX Threat Response アカウントへのアクセスに使用するクレデンシャルを使用してサインインします。
d) [デバイス（Devices）] をクリックします。
e) Firepower Management Center とその管理対象デバイスがリストに表示されていることを確認します。

次のタスク

Cisco Cloud にイベントを直接送信する方法 （4 ページ）の残りのステップを続行します。

イベントが Security Services Exchange に到達しているか（直接接続）の確認

始める前に

イベントが予期していたとおりに Firepower に表示されることを確認します。

手順

ステップ 1 まだ Security Services Exchange で作業していない場合はアクセス Security Services Exchange （6 ページ）を実行します。

ステップ 2 [イベント（Events）] をクリックします。

ステップ 3 デバイスからイベントを検索します。

予期していたイベントが表示されない場合は、直接統合のトラブルシューティング （13 ページ）のヒントを参照し、Cisco Cloud にイベントを直接送信する方法 （4 ページ）でもう一度確認してください。

直接統合のトラブルシューティング

クラウドへのアクセスに関する問題

- この統合の設定を試みる直前にクラウドアカウントをアクティブ化し、この統合の実装中に問題が発生した場合は、1 ～ 2 時間待ってから、クラウドアカウントへのログインを試します。
- アカウントに関連付けられている地域のクラウドの正しい URL にアクセスしていることを確認してください。

[デバイス（Device）] インターフェイスに統合が [有効（Enabled）] として表示されているが、[デバイス（Devices）] ページにデバイスが表示されない

- クラウドアカウントにリンクされていないスマートアカウントか、または仮想アカウントを使用してデバイスのライセンスが取得されている可能性があります。次のいずれかを実行します。
  - SSE で、デバイスのライセンスを取得したアカウントにリンクします。

    スマートライセンスアカウントのリンク （8 ページ）を参照してください。
  - リンクされているアカウントからデバイスのライセンスを取得するには、次を実行します。

    FMC または FDM での統合を無効にし、デバイスから現在のライセンスの登録を解除し、リンクされているアカウントからデバイスのライセンスを再取得してから、FDM または FMC で統合を再度有効にします。
- Firepower の設定で選択したのと同じ地域のクラウドを参照していることを確認します。クラウドへのイベントの送信開始時に地域を選択しなかった場合は、まず北米のクラウドを試してください。

FMC によって管理されるデバイスが [SSE Devices] ページに正しく表示されない

（6.4.0.4 より前のリリース）デバイスに手動で一意の名前を付けます。[Devices] リストの各行の鉛筆アイコンをクリックします。推奨：[説明（Description）] から IP アドレスをコピーします。

この変更はこの [デバイス（Devices）] リストに対してのみ有効であり、Firepower 導入環境内のどの場所にも表示されません。

（リリース6.4.0.4ー6.6）デバイス名は、SSE への初期登録時にのみ FMC から SSE に送信され、デバイス名が FMC で変更されても SSE で更新されません。

SSE の [Devices] ページで、以前に登録されたデバイスが予期せず未登録として表示される

これらのデバイスがFDMによって管理されているFTDデバイスであり、またはCisco SecureX Threat Response との統合のためにデバイスを SSE に登録した後に CDO との統合を有効にし、まだアカウントをマージしていない場合は、（FDM が管理する FTD のみ）CDO アカウントとセキュリティアカウントのマージ （7 ページ）の手順を実行してください。

予期していたイベントが [イベント（Events）] リストにない

- 正しい地域クラウドとアカウントを使用していることを確認します。
- デバイスがクラウドに到達できること、および必要なすべてのアドレスへのファイアウォールを介したトラフィックが許可されていることを確認します。
- [イベント（Events）] ページの [更新（Refresh）] ボタンをクリックしてリストを更新します。
- 予期していたイベントが Firepower に表示されることを確認します。
- FDM を使用している場合は、アクセスルールのロギング設定を確認します。
- SSE の [Cloud Services] ページの [Eventing] の設定で、自動削除（イベントのフィルタアウト処理）の設定を確認します。
- その他のトラブルシューティングのヒントについては、SSE のオンラインヘルプを参照してください。