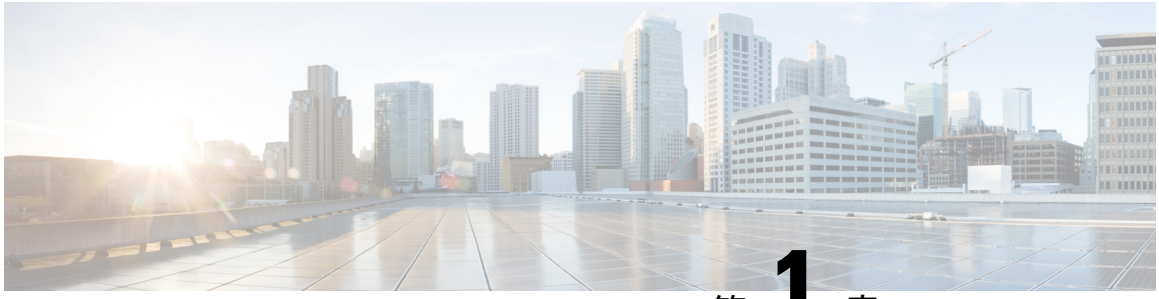
Cisco Firepower および SecureX 統合ガイド

初版：2020 年 6 月 24 日

最終更新：2021 年 3 月 3 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

Firepower との統合に関する重要な情報：SecureX

- Firepower と SecureX について （1 ページ）
- SecureX 地域クラウド （2 ページ）
- サポートされるイベント タイプ （3 ページ）
- クラウドへのイベント送信方法の比較 （3 ページ）
- ベスト プラクティス （4 ページ）

Firepower と SecureX について

シスコセキュリティ製品の購入に含まれる統合ポータルである SecureX を使用して、すべてのシスコセキュリティ製品のデータを表示します。

SecureX は簡素化されたプラットフォーム エクスペリエンスです。シスコの統合型セキュリティポートフォリオをお客様の既存のインフラストラクチャとつなぎ、可視性の統合、自動化の有効化、そしてネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティの強化を実現します。

SecureX の詳細については、https://www.cisco.com/c/en/us/products/security/securex/index.htmlを参照してください。

SecureX ポータルで Firepower データを表示して操作するには、このドキュメントの手順に従います。

SecureX 地域クラウド

地域	クラウドへのリンク	サポートされている Firepower 統合方式
北米	https://securex.us.security.cisco.com	• 直接統合： Firepower リリース 6.4 以降 • syslog 経由での統合： Firepower リリース 6.3 以降
欧州	https://securex.eu.security.cisco.com	• 直接統合： Firepower リリース 6.5 以降 • syslog 経由での統合： Firepower リリース 6.3 以降
アジア（APJC）	https://securex.apjc.security.cisco.com	• 直接統合： Firepower リリース 6.5 以降 • syslog 経由での統合： Firepower リリース 6.3 以降

地域クラウドの選択に関する注意事項と制約事項

地域クラウドを選択する前に、次の重要な点を考慮してください。

- Firepower のバージョンと統合方法（syslog または直接）が選択内容に影響を及ぼします。

  詳細については、SecureX 地域クラウド （2 ページ）を参照してください。
- 可能な場合は、Firepower 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。
- Firepower 製品で選択した地域は、シスコ サポート診断およびシスコ 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）。これらの詳細については、ご使用の Firepower 製品のオンラインヘルプを参照してください。

サポートされるイベント タイプ

Firepower と SecureX 統合では、次のイベントタイプがサポートされています。

表 *1 : Cisco Cloud* にイベントを送信するための *Firepower* バージョンのサポート

機能	FMC バージョンによって管理されているデバイス （直接統合）	FDM バージョンによって管理されている FTD デバイス （直接統合）	Syslog
侵入（IPS）イベント	6.3 以降（syslog 経由） 6.4 以降（直接接続経由）	6.3 以降（syslog 経由） 6.4 以降（直接接続経由）	サポートあり
セキュリティインテリジェンスの接続イベント	6.5 以降	6.5 以降	未サポート
ファイルおよびマルウェアのイベント	6.5 以降	6.5 以降	サポート対象外

クラウドへのイベント送信方法の比較

Firepower デバイスは、syslog を使用して、または直接的に Security Services Exchange ポータルを経由することで SecureX でイベントを利用可能にします。

直接送信	プロキシを使用した syslog 経由での送信
サポートされているバージョンの Firepower ソフトウェアを実行している Firepower Threat Defense（NGFW）デバイスのみをサポート	サポートされているバージョンの Firepower ソフトウェアを実行しているすべてのデバイスをサポート
Firepower 6.4 以降をサポート	Firepower 6.3 以降をサポート
サポートされるイベント タイプ （3 ページ）に示されているすべてのイベントタイプをサポートします。	侵入イベントのみをサポートします。

直接送信	プロキシを使用した syslog 経由での送信
アプライアンスおよびデバイスで最適なソフトウェアバージョンが実行されているかどうかなど、システムステータス情報を表示する SecureX タイルをサポートします。	システムステータス機能は、syslog ベースの統合ではサポートされていません。
Firepower Threat Defense デバイスのインターネットへの接続が必要	Firepower デバイスのインターネットへの接続は不要
Firepower の展開では、Smart Software Manager オンプレミスサーバー（旧称 Smart Software Satellite Server）は使用できません。	導入では、Smart Software Manager オンプレミスサーバーを使用できます。
オンプレミスのプロキシサーバーのセットアップとメンテナンスは不要	オンプレミス仮想 Cisco Security Services Proxy（CSSP）サーバーが必要 このプロキシサーバーの詳細については、Security Services Exchange（SSE）のオンラインヘルプを参照 SSE にアクセスするには、Security Services Exchange へのアクセス （32 ページ）を参照

ベスト プラクティス

参照先の手順に関するトピックの「要件」に関するトピックや「始める前に」のセクションを含め、次のトピックのガイドラインとセットアップ手順に厳密に従います。

- すべての統合：

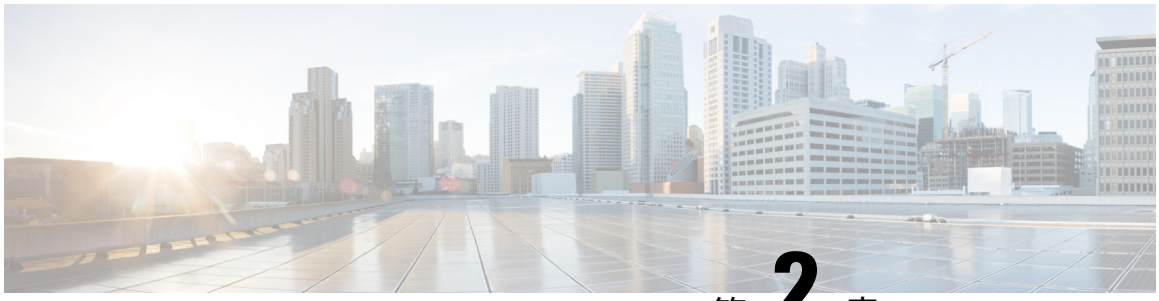
  地域クラウドの選択に関する注意事項と制約事項 （2 ページ）を参照してください。

- 直接統合の場合：

  Cisco Cloud にイベントを直接送信し、SecureX と統合する方法 （12 ページ）を参照してください。

- syslog を使用した統合の場合：

  「syslog を使用した Cisco Cloud へのイベントの送信方法 （30 ページ）」を参照してください。



第 2 章

シスコ クラウドアカウント

- SecureX のアクセスに必要なアカウント （5 ページ）
- SecureX にアクセスするためのアカウントの取得 （5 ページ）
- クラウドアカウントへのアクセスの管理 （6 ページ）

SecureX のアクセスに必要なアカウント

SecureX および関連ツール（SSE を含む）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
- SecureX アカウント

重要 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。アカウントに関連付けられたデータは、そのアカウントでのみ使用できます。

アカウントをお持ちでない場合は、SecureX にアクセスするためのアカウントの取得 （5 ページ）を参照してください。

SecureX にアクセスするためのアカウントの取得

重要 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。

手順

ステップ 1 使用する SecureX 地域クラウドを決定します。

「地域クラウドの選択に関する注意事項と制約事項 （2 ページ）」を参照してください。

ステップ 2 使用予定の地域クラウドでアカウントをまだお持ちでない場合は、そのクラウドでサポートされるアカウントを組織で所有しているかどうかを、お客様の管理部門でご確認ください。

サポートされているアカウントタイプについては、SecureX のアクセスに必要なアカウント （5 ページ）を参照してください。

ステップ 3 組織内の誰かがすでにその地域のシスコセキュリティアカウントをお持ちの場合は、次のように対応してください。

そのアカウントの管理者に、お客様用のアカウントの追加を依頼します。手順についてはクラウドアカウントへのアクセスの管理 （6 ページ）を参照してください。

ステップ 4 それ以外の場合は、組織用に新しいアカウントを作成します。（お客様が管理者になります）。

a) ブラウザで、選択した地域のクラウドに移動します。

リンクについては、SecureX 地域クラウド （2 ページ）を参照してください。

b) [Create an Account] をクリックします。

c) アカウントの作成について不明な点がある場合は、https://www.cisco.com/c/en/us/support/security/securex/series.html からリンクしている『*Cisco SecureX Sign-On Guide*』を参照してください。

クラウドアカウントへのアクセスの管理

ユーザーアカウントの管理は、所有しているクラウドアカウントのタイプによって異なります。

（注） Threat Grid または AMP for Endpoints アカウントを使用してクラウドにアクセスする場合は、これらの製品のマニュアルを参照してください。

SecureX アカウントへのユーザーアクセスの管理

組織が SecureX アカウントを使用してクラウドにアクセスしている場合は、この手順を使用してユーザーを管理します。

始める前に

SecureX アカウントには管理者レベルの権限が必要です。

手順

ステップ 1 SecureX の地域クラウドにサインインします。

ステップ 2 [Administration] をクリックします。

ステップ 3 不明な点がある場合は、SecureX のオンラインヘルプ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）。

手順

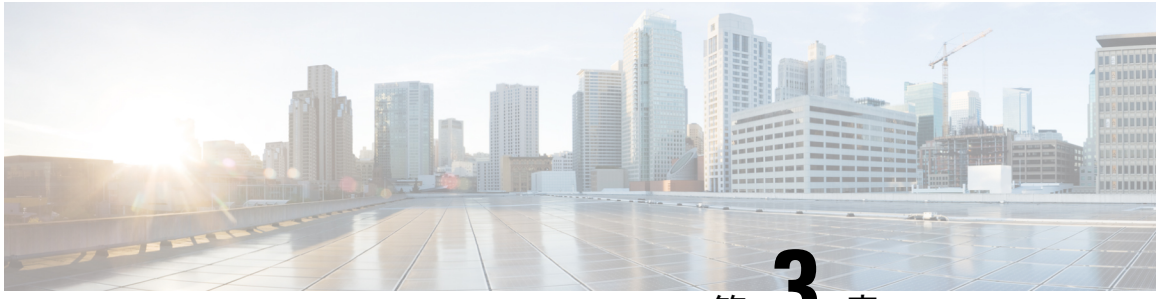
ステップ 1 適切な地域クラウドの URL に移動します。

- 北米： https://castle.amp.cisco.com
- 欧州： https://castle.eu.amp.cisco.com
- アジア（APJC）： https://castle.apjc.cisco.com

ステップ 2 [Users] をクリックします。

ステップ 3 ユーザーアクセス権を追加または編集します。

[Account Administrator] を選択した場合は、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。



第 3 章

クラウドへのイベントの直接送信

- 直接統合について （9 ページ）
- 直接統合の追加要件 （9 ページ）
- Cisco Cloud にイベントを直接送信し、SecureX と統合する方法 （12 ページ）
- 直接統合のトラブルシューティング （27 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 SecureX 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。

アプライアンスおよびデバイスが現在のソフトウェアバージョンを実行しているかどうかなど、システムステータスに関する情報も表示できます。

直接統合の追加要件

要件のタイプ	要件
Firepower デバイス	Firepower Threat Defense デバイス • Firepower Management Center によって管理 • 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。だだし、これらのオプションの内容に注意してください。 • SecureX 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。 • この統合はFirepower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。
アカウント	直接統合のアカウントの要件（12ページ）を参照してください。 FDM と CDO または Cisco Security Analytics and Logging (SaaS) を使用している場合は、（FDM が管理する FTD のみ）CDO アカウントと SecureX アカウントのマージ（16 ページ）も参照してください。

要件のタイプ	要件
Connectivity	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
アプライアンスおよびデバイスステータス機能の要件	アプライアンスおよびデバイスで最適なバージョンが実行されているかどうかなど、システム情報を表示するSecureXタイルを表示する場合は、次の手順を実行します。 • この機能はFMCの展開でのみサポートされ、FDMではサポートされていません。 • 直接接続を使用してクラウドにデータを送信する必要があります。 • Cisco Success Network（CSN）がFMCで有効になっている必要があります。 この設定を確認または有効にするには、FMCの[System] > [Smart Licenses]ページに移動します。不明な点がある場合は、FMCオンラインヘルプで「Cisco Success Network」を検索してください。 CSNを有効にした後、アプライアンスとデバイスのステータスタイルが更新されるまでに最大24時間かかります。
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、SecureX のアクセスに必要なアカウント （5 ページ）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、SecureX にアクセスするためのアカウントの取得 （5 ページ）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ーロールを特定するには、https://software.cisco.com に移動して [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、[Users] をクリックしてユーザー 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ー 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し、SecureX と統合する方法

（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 （以前の Cisco 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： SecureX （1 ページ）
ステップ	要件を満たす。	直接統合の追加要件 （9 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 SecureX のクラウドポータルである Security Services Exchange にアクセスする。	Security Services Exchange へのアクセス （15 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 SecureX アカウントのマージ （16 ページ）を参照してください。
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 （17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。	[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** • **Eventing**

	操作手順	詳細情報
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 （18 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 （20 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 （22 ページ） • 直接統合のトラブルシューティング （27 ページ）
ステップ	Security Services Exchange で、重要なイベントを自動的に昇格するようにシステムを設定します。	**重要** イベントの昇格を自動化しない場合は、SecureX で表示するために手動でイベントを確認して昇格させる必要があります。 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、Security Services Exchange へのアクセス （15 ページ）を参照
ステップ	（任意）Security Services Exchange で、一定の重要ではないイベントの自動削除を設定します。	イベントのフィルタリングについては、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、Security Services Exchange へのアクセス （15 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。	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	（FMC のみ）SecureX リボンを SecureX とすべてのシスコセキュリティ製品にピボットできるようにします。	「FMC での SecureX リボンの設定方法 （23 ページ）」を参照してください。

Security Services Exchange へのアクセス

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SecureX クラウドに移動します。

- 北米クラウド： https://securex.us.security.cisco.com
- ヨーロッパのクラウド： https://securex.eu.security.cisco.com
- アジア クラウド： https://securex.apjc.security.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。

[Integrations] > [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。

次のタスク

ヒント FMC で SecureX リボンを有効にすると、リボンを使用して FMC から SSE に直接アクセスできます。「FMC での SecureX リボンの有効化 （25 ページ）」を参照してください。

（FDM が管理する FTD のみ）CDO アカウントと SecureX アカウントのマージ

このタスクを実行するかどうかは、場合によって異なります。

FDM 管理対象 Firepower Threat Defense（FTD）デバイスを Cisco Defense Orchestrator（CDO）または Cisco Security Analytics and Logging (SaaS)、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。（Cisco SecureX Threat Response は、以前は Cisco Threat Response または CTR と呼ばれていました。）

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 ユーザー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ーメニューから、[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、Cisco Security Analytics and Logging (SaaS)、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し、SecureX と統合する方法 （12 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。（後者は以前 Cisco Threat Response または CTR と呼ばれていました。）
- リンクされたアカウントを表示するにはユーザー 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 [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し、SecureX と統合する方法 （12 ページ） でここまでのステップを実行します。
- CDO を使用している場合は、この手順を開始する前にアカウントを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 SecureX アカウントのマージ（16 ページ）」を参照してください。

- 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 [Device] > [System Settings] > [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 SecureX 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、SecureX 地域クラウド （2 ページ）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、[Device] をクリックし、**[System Settings]** > **[Cloud Services]** をクリックします。

[System Settings] ページがすでに表示されている場合は、目次で [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。

接続イベントの送信を選択した場合は、セキュリティインテリジェンス接続イベントのみがこの統合で使用されます。他の接続イベントはすべて、この統合では使用されません。

ステップ 4 [Cisco Threat Response] 機能の [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、[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、Security Services Exchange へのアクセス （15 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：[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し、SecureX と統合する方法 （12 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 SecureX アカウントのマージ （16 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。
  - [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 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 [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し、SecureX と統合する方法 （12 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 SecureX 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、SecureX 地域クラウド （2 ページ）を参照してください。
- 現在 syslog を使用してクラウドにイベントを送信している場合は、重複を避けるためにそれらの送信を無効にします。

手順

ステップ 1 Firepower Management Center で [System] > [Integration] を選択します。

ステップ 2 [Cloud Services] をクリックします。

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

ステップ 4 まだ有効にしておらず、FMC に [Cisco Cloud Region] オプションが表示されている場合は、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。

Firepower リリース 7.0 以降、クラウドに送信するイベントを複数の統合に使用できます。

統合	サポートされるイベントのオプション	注意
Cisco Security Analytics and Logging (SaaS) （Firepower バージョン 7.0 以降）	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。 • 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
シスコ SecureX と Cisco SecureX Threat Response	お使いの Firepower のバージョンに応じて、以下が含まれます。 • 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	* 接続イベントを送信する場合、シスコ SecureX と Cisco SecureX Threat Response ではセキュリティ インテリジェンス イベントのみサポートされます。

（注） Firepower リリース 7.1 以降

- [Send Intrusion Events to the cloud] を有効にすると、イベントは影響フラグとともに FMC デバイスから送信されます。
- [Send File and Malware Events to the cloud] を有効にすると、FTD 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 FMC デバイスから送信されます。

ステップ 6 [Save] をクリックします。

[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) SecureX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) [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し、SecureX と統合する方法 （12 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Security Services Exchange へのアクセス（15 ページ）を実行します。

ステップ 2 [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 （27 ページ）のヒントを参照し、Cisco Cloud にイベントを直接送信し、SecureX と統合する方法 （12 ページ）でもう一度確認してください。

FMC での SecureX リボンの設定方法

リボン機能は、Firepower リリース 7.0 で導入されました。

FMC からピボットして SecureX と統合し、その他のシスコセキュリティ製品に対して相互起動するには、このオプションを設定します。

手順	操作手順	詳細情報
1	SecureX リボンを設定するためのアカウント要件を確認します。	SecureX リボンを設定するためのアカウント要件 （23 ページ）を参照してください。
2	FMC Web インターフェイスから API クライアントのリダイレクト URL を取得します。	FMC Web インターフェイスで、[System]（⚙）> [SecureX] をクリックし、[SecureX Configuration] ウィジェットから 2 つのリダイレクト URL をコピーします。
3	SecureX で FMC の API クライアントを生成します。	SecureX で FMC の API クライアントを生成する （23 ページ）を参照してください。
4	FMC で SecureX リボンを有効にします。	「FMC での SecureX リボンの有効化 （25 ページ）」を参照してください。

SecureX リボンを設定するためのアカウント要件

FMC で SecureX リボンをオンに設定するには、次のことを確認します。

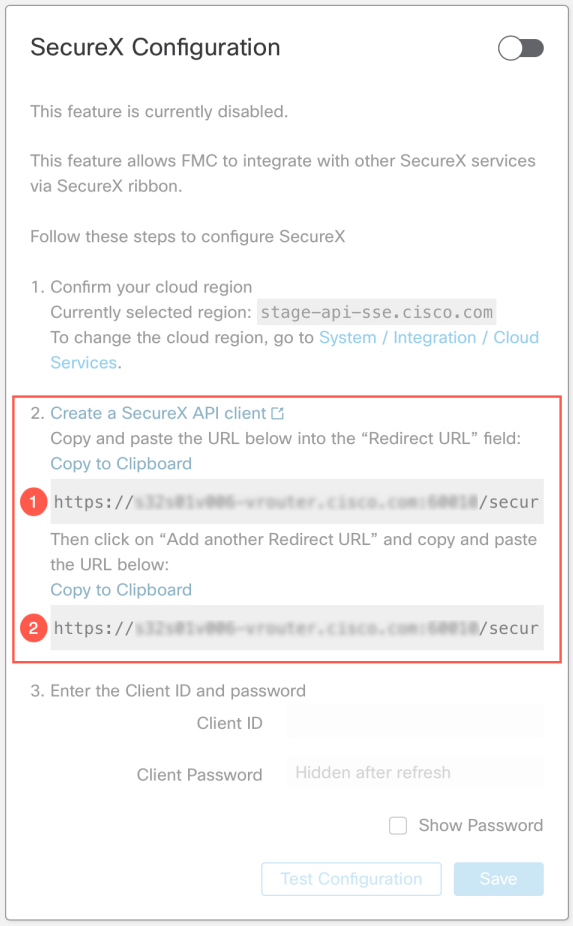
- 使用する地域クラウドに次のいずれかのアカウントがある。
  - シスコ セキュリティアカウント
  - AMP for Endpoints アカウント
  - Cisco Threat Grid アカウント
  - SecureX アカウント
- 組織、管理者、および認可された各ユーザーは、SecureX にアカウントを持っています。
- FMC、SecureX、および Cisco SecureX Threat Response の両方の管理者権限が必要です。

SecureX で FMC の API クライアントを生成する

FMC の SecureX リボンは、API クライアントを使用して SecureX API とプログラムで通信します。FMC の API クライアントを作成します。

始める前に

FMC Web インターフェイスから API クライアントのリダイレクト URL を取得します。FMC Web インターフェイスで、[System]（⚙）> [SecureX] をクリックし、[SecureX Configuration] ウィジェットから 2 つのリダイレクト URL をコピーします。



手順

ステップ 1 https://sign-on.security.cisco.com/に進みます。

ステップ 2 地域クラウド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 [Administration] > [API Clients] に移動します。

ステップ 6 [Generate API Client] をクリックします。

ステップ 7 API クライアントの名前を入力します。

ステップ 8 [OAuth Code Clients] タブをクリックします。

ステップ 9 [Client Preset] ドロップダウンリストから [Ribbon] を選択します。

[Ribbon] クライアントプリセットを選択すると、リボンに必要な範囲が自動的に選択されます。

ステップ 10 FMC Web インターフェイスからコピーした最初のリダイレクト URL を入力します。

ステップ 11 [Add another Redirect URL] をクリックし、FMC Web インターフェイスからコピーした 2 番目のリダイレクト URL を入力します。

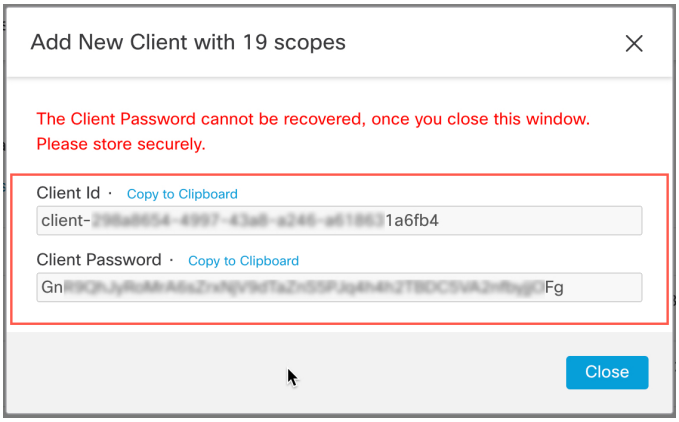
ステップ 12 ドロップダウンリストから、[Availability] を選択します。ユーザーまたは組織がクライアントを使用できるようにできます。

[Organization]（推奨）を選択した場合、組織のメンバーのみがクライアントを承認できます。

[Availability] オプションを選択しない場合、デフォルトで [Organization] に設定されます。

ステップ 13 [Add New Client] をクリックします。

クライアント ID とクライアントパスワードが生成され、[Add New Client] ウィンドウに表示されます。



（注） このウィンドウを閉じた後は、クライアントパスワードを回復できません。必要に応じて、後でアクセスできる場所に安全に保管してください。クライアントパスワードを紛失、または開示した場合、API クライアントを削除して新しいクライアントを作成する必要があります。

FMC での SecureX リボンの有効化

リボンを有効にすると、FMC のすべてのページの下部に表示され、すべての FMC ユーザーに表示されます。ただし、SecureX のアクセス権を持つ認可されたユーザーのみリボンを使用できます。

（注） 現在、一度有効にしたユーザーの認可を無効にすることはできません。

始める前に

- 組織、管理者、および認可された各ユーザーには、SecureX のアカウントが必要です。
- FMC と SecureX の両方の管理者権限が必要です。
- FMC で適切な地域クラウドを選択します。FMC Web インターフェイスで、[System]（⚙）> [Integration] をクリックし、[Cisco Cloud Region] ウィジェットで適切な地域を選択します。
- API クライアント ID とパスワードを手元に置いておきます。API クライアント ID とパスワードを取得する手順については、SecureX で FMC の API クライアントを生成する （23 ページ）を参照してください。

手順

ステップ 1 FMC でリボンを有効にします。

a) 管理者アカウントを使用して FMC にサインインします。
b) [System]（⚙）> [SecureX] の順に選択します。
c) スライダを有効にし、API クライアント ID とパスワードを入力します。
d) [Save] をクリックします。

これで、すべての FMC ユーザーにリボンが表示されます。

e) FMC ページを更新して、リボンを表示します。

リボンは、ウィンドウの下部に表示されます。

ステップ 2 リボンへのアクセスを承認します。

（各 FMC ユーザーは、リボンの初回クリック時にこの手順を実行する必要があります）。

a) リボンをクリックします。

SecureX リボンペインは、Firepower ウィンドウの下部に展開されます。

b) [Get SecureX] をクリックします。
c) プロンプトが表示されたら、SecureX にサインインします。
d) アクセスを許可するオプションをクリックします。

FMC ウィンドウに戻ります。

これで、リボンを使用する準備ができました。

次のタスク

- リボンを使用するすべての FMC ユーザーが SecureX クラウドのアカウントを持っていることを確認します。

- リボンを使用する、またはリボンの設定を行うには、SecureX のオンラインヘルプを参照してください。

  https://www.cisco.com/c/en/us/support/security/securex/series.html [英語] から入手可能な Cisco SecureX スタートアップガイドには、リボンに関する情報も含まれています。

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。

[Device] インターフェイスに統合が [Enabled] として表示されているが、[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 （17 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：[Description] から IP アドレスをコピーします。

この変更はこの [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

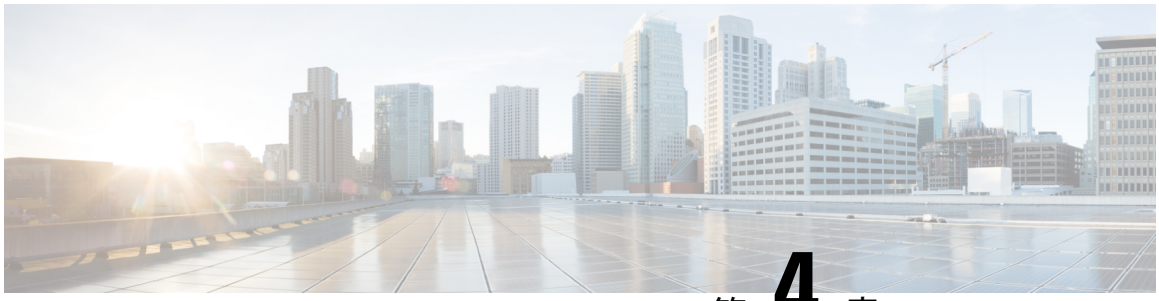
これらのデバイスが FDM によって管理されている FTD デバイスであり、SecureX または との統合のためにデバイスを SSE に登録した後に CDO との統合を有効にし、まだアカウントをマージしていない場合は、（FDM が管理する FTD のみ）CDO アカウントと SecureX アカウントのマージ （16 ページ）の手順を実行してください。

予期していたイベントが [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。
- [Events] ページの [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。

一部のイベントがありません

- 接続イベントを送信すると、セキュリティインテリジェンス接続イベントのみが使用されます。他の接続イベントはすべて無視されます。
- FMC で、グローバルブロックリストや許可リストおよび Threat Intelligence Director などのカスタム セキュリティ インテリジェンス オブジェクトを使用している場合は、それらのオブジェクトを使用して処理されるイベントを自動昇格するように SSE を設定する必要があります。イベントのインシデントへの昇格については、SSE オンラインヘルプの情報を参照してください。。



第 4 章

syslog を使用したクラウドへのイベントの送信

- syslog 経由での統合について （29 ページ）
- syslog を使用した統合の要件 （29 ページ）
- syslog を使用した Cisco Cloud へのイベントの送信方法 （30 ページ）
- syslog 統合のトラブルシューティング （33 ページ）

syslog 経由での統合について

Firepower リリース 6.3 以降では、サポートされているイベントを Firepower デバイスから Cisco Cloud に syslog を使用して送信できます。オンプレミス Cisco Security Services Proxy（CSSP）サーバーをセットアップし、このプロキシに syslog メッセージを送信するようにデバイスを設定する必要があります。

プロキシは収集したイベントを 10 分ごとに Security Services Exchange（SSE）へ転送します。そこから、SecureX に表示されるインシデントに自動または手動で昇格させることができます。

syslog を使用した統合の要件

要件のタイプ	要件
Firepower デバイス	サポートされているバージョンの Firepower ソフトウェアを実行しているデバイス
Firepower のバージョン	6.3 以降
使用予定の SecureX クラウドのアカウント	SecureX のアクセスに必要なアカウント （5 ページ） を参照してください。

要件のタイプ	要件
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。だだし、これらのオプションの内容に注意してください。 • SecureX に送信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。 • この統合は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、エアギャップ環境に導入できません。
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。

syslog を使用した Cisco Cloud へのイベントの送信方法

（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 （以前の Cisco 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： SecureX （1 ページ）
ステップ	要件を満たす。	syslog を使用した統合の要件 （29 ページ）を参照してください。
ステップ	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 SecureX のポータルである Security Services Exchange（SSE）にアクセスする。	Security Services Exchange へのアクセス （32 ページ）を参照してください。

	操作手順	詳細情報
ステップ	Cisco Security Services Proxy（CSSP）サーバーをインストールし、設定する。	無料のインストーラと手順を Security Services Exchange からダウンロードします。 SSE で、ブラウザ ウィンドウの右上の近くにある [Tools] ボタン（🛠）から [Downloads] を選択します。
ステップ	Security Services Exchange で、機能を有効にする。	[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** • **Eventing Service**
ステップ	サポートされているイベントの syslog メッセージをプロキシサーバーに送信するように Firepower デバイスを設定する。	• Firepower Device Manager（FDM）によって管理されているデバイスの場合は次の手順を実行します。 「侵入イベントの syslog の設定」の詳細については、FDM オンラインヘルプを参照してください。 • Firepower Management Center（FMC）によって管理されているデバイスの場合は次の手順を実行します。 「外部ツールを使用したイベント分析」の章に記載されている syslog の詳細については、FMC のオンラインヘルプを参照してください。
ステップ	Firepower 製品で、各イベントを生成したデバイスをメッセージが識別していることを確認する。	• Firepower Device Manager で次の手順を実行します。 [Device] > [Hostname] でホスト名を指定します。 • Firepower Management Center で、次の手順を実行します。 [Platform Settings] の [Syslog settings] タブで [Enable Syslog Device ID] を選択し、識別子を指定します。
ステップ	Firepower システムがサポート対象イベントを生成する時間を確保します。	--

	操作手順	詳細情報
ステップ	イベントが予期したとおりに Security Services Exchange に表示されていることを確認し、必要に応じてトラブルシューティングを行う。	参照先： • イベントが Security Services Exchange に到達（syslog 経由）しているかの確認 （33 ページ） • syslog 統合のトラブルシューティング （33 ページ）
ステップ	Security Services Exchange で、重要なイベントを自動的に昇格するようにシステムを設定します。	**重要** イベントの昇格を自動化しない場合は、SecureX で表示するために手動でイベントを確認して昇格させる必要があります。 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、Security Services Exchange へのアクセス （15 ページ）を参照
ステップ	（任意）Security Services Exchange で、一定の重要ではないイベントの自動削除を設定します。	イベントのフィルタリングについては、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、Security Services Exchange へのアクセス （15 ページ）を参照
ステップ	SecureX で、Firepower モジュールを追加します。	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。

Security Services Exchange へのアクセス

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SecureX クラウドに移動します。

- 北米クラウド： https://securex.us.security.cisco.com
- ヨーロッパのクラウド： https://securex.eu.security.cisco.com

- アジア クラウド： https://securex.apjc.security.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。

[Integrations] > [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。

イベントが Security Services Exchange に到達（syslog 経由）しているかの確認

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 メッセージがプロキシから Security Services Exchange に転送できるようになるには、Firepower デバイスがサポートされているイベントを検出してから 15 分待ちます。

ステップ 2 Security Services Exchange へのアクセス （32 ページ）。

ステップ 3 Security Services Exchange で [イベント（Events）] をクリックします。

ステップ 4 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、syslog 統合のトラブルシューティング （33 ページ）のヒントを参照し、syslog を使用した Cisco Cloud へのイベントの送信方法 （30 ページ）でもう一度確認してください。

syslog 統合のトラブルシューティング

イベントが CSSP に到達していない

デバイスからネットワーク上の CSSP に到達できることを確認します。

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。

予期していたイベントが [Events] リストにない

次の点をチェックします。

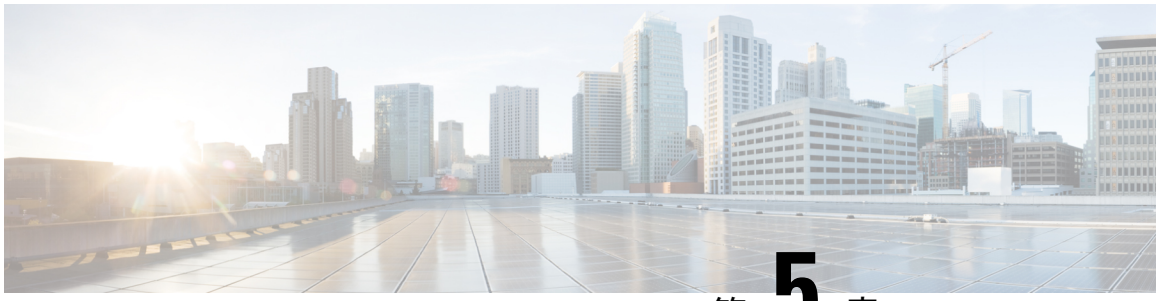
- [Events] ページの [Refresh] ボタンをクリックしてリストを更新します。
- 予期していたイベントが Firepower に表示されることを確認します。
- SSE の [Cloud Services] ページの [Eventing] の設定で、自動削除（イベントのフィルタアウト処理）の設定を確認します。
- イベントの送信先の地域クラウドを調べていることを確認します。

syslog のフィールドに関する質問

syslog のフィールドと説明については、https://www.cisco.com/c/en/us/support/security/defense-center/products-system-message-guides-list.html にある『Cisco Firepower Threat Defense Syslog Messages』ガイド を参照してください。

SecureX タイルから一部のイベントが欠落している

FMCで、グローバルブロックリストや許可リストなどのカスタム セキュリティ インテリジェンス オブジェクトを使用している場合は、それらのオブジェクトを使用して処理されるイベントを自動昇格するようにSSEを設定する必要があります。イベントのインシデントへの昇格については、SSE オンラインヘルプの情報を参照してください。。



第 5 章

次のステップ

- SecureX の使用に関する詳細情報 （35 ページ）
- Security Services Exchange 内の操作 （35 ページ）

SecureX の使用に関する詳細情報

SecureX の使用

SecureX の使用方法の詳細については、SecureX のオンラインヘルプを参照してください。

追加情報：http://cs.co/SecureX_faq

SecureX ダッシュボードの Firepower タイル

Firepower タイルを含む SecureX ダッシュボードのタイルの詳細については、https://www.cisco.com/c/en/us/td/docs/security/securex/tiles/securex-tiles-list.htmlを参照してください。

Security Services Exchange 内の操作

Security Services Exchange または Cisco Security Services Proxy の使用方法については、Security Services Exchange のオンライン ヘルプを参照してください。

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。