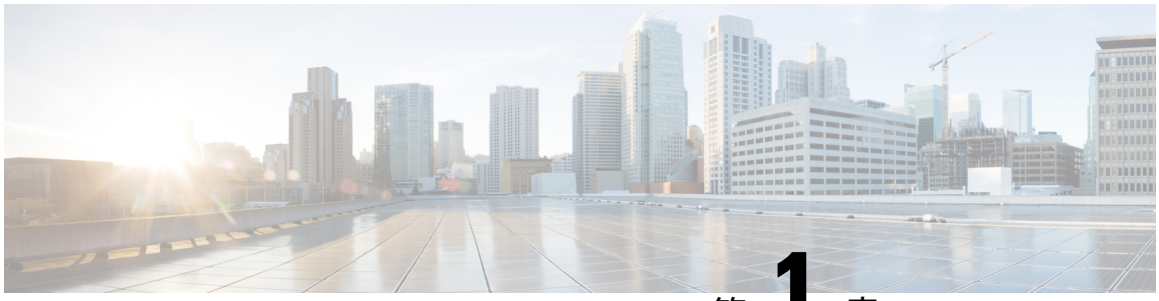
Cisco Secure Firewall Management Center（7.0.2 および 7.2）と SecureX の統合ガイド

初版：2022 年 5 月 31 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



第 1 章

Secure Firewall Management Center と SecureX の統合について

Secure Firewall Management Center と SecureX について

Cisco SecureX プラットフォームは、広範なシスコの統合型セキュリティポートフォリオとお客様のインフラストラクチャをつなぐことで、一貫した操作性を提供します。これにより可視性が統一され、自動化が実現し、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の全体でセキュリティが強化されます。

SecureX の詳細については、Cisco SecureX 製品のページを参照してください。

SecureX と Management Center の統合により、Management Center の全データの概要が提供されます。

このドキュメントの指示に従い、SecureX ポータルを使用して、Management Center バージョン 7.0.2 および 7.2 で管理されているデバイスのファイアウォール イベント データを表示および操作します。Management Center のバージョンが 7.1 以下の場合（7.0.2 を除く）、Management Center と SecureX の統合については『Cisco Secure Firewall Threat Defence and SecureX Integration Guide』[英語] の指示に従ってください。

SecureX 地域クラウド

地域	クラウドへのリンク	サポートされる統合方法と管理対象デバイスのバージョン	サポートされる Management Center バージョン
北米	https://securex.us.security.cisco.com	• 直接統合： バージョン 6.4 以降 • syslog を使用した統合： バージョン 6.3 以降	バージョン 7.0.2、バージョン 7.2 以降
欧州	https://securex.eu.security.cisco.com	• 直接統合： バージョン 6.5 以降 • syslog を使用した統合： バージョン 6.3 以降	バージョン 7.0.2、バージョン 7.2 以降
アジア（APJC）	https://securex.apjc.security.cisco.com	• 直接統合： バージョン 6.5 以降 • syslog を使用した統合： バージョン 6.3 以降	バージョン 7.0.2、バージョン 7.2 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。

- 地域クラウドの選択は、バージョンと統合方法（syslog または直接）によって異なります。

  詳細については「SecureX 地域クラウド」を参照してください。

- 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。
- 複数の地域クラウドのデータをマージまたは集約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。

- ご使用の製品で選択した地域は、 Cisco Support Diagnostics および Cisco Support Network 機能にも使用されます（該当し有効にしている場合）。これらの機能の詳細については、ご使用の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

Secure Firewall Management Center と SecureX の統合では、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バージョンのサポート

イベントタイプ	**Threat Defense** のデバイスバージョン（直接統合）	**Syslog**
侵入（IPS）イベント	6.4 以降	6.3 以降
セキュリティ接続イベント	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	サポート対象外

クラウドへのイベント送信方法の比較

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。

イベントの直接送信	**Syslog** を使用したプロキシサーバー経由のイベント送信
サポートされているバージョンのソフトウェアを実行している Threat Defense （NGFW）デバイスのみをサポートします。	サポートされているバージョンの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します。
バージョン 6.4 以降をサポートします。	バージョン 6.3 以降をサポートします。
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。

イベントの直接送信	Syslog を使用したプロキシサーバー経由のイベント送信
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。
Threat defense デバイスはインターネットに接続する必要があります。	デバイスをインターネットに接続する必要はありません。
展開時に Smart Software Manager オンプレミスサーバー（旧称 Smart Software Satellite Server）を使用できません。	展開時に、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です。	オンプレミス仮想 Cisco Security Service Proxy（CSSP）サーバーが必要です。 このプロキシ サーバーの詳細については、Security Services Exchange のオンライン ヘルプを参照 Security Services Exchange にアクセスするには、「Security Services Exchange へのアクセス」を参照してください。

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：

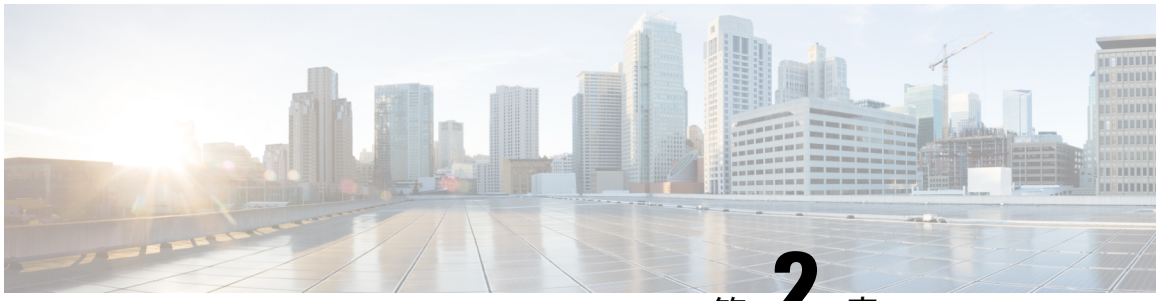
  地域クラウドの選択に関する注意事項と制約事項 （2 ページ）を参照してください。

- 直接統合の場合：

  Cisco Cloud にイベントを直接送信する方法 （14 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 （26 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 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、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
- Secure Endpoint アカウント
- Cisco Secure Malware Analytics 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 （6 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、使用する地域クラウドのアカウントをお持ちの場合は、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既存アカウントの使用

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」を参照してください。

ステップ 2 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 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。この説明については、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、組織の新しいアカウントを作成します（ユーザー自身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」を参照してください。

b) [Sign Up] 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、『Cisco SecureX Sign-On Guide』[英語] 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） Secure Malware Analytics または Secure Endpoint 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。

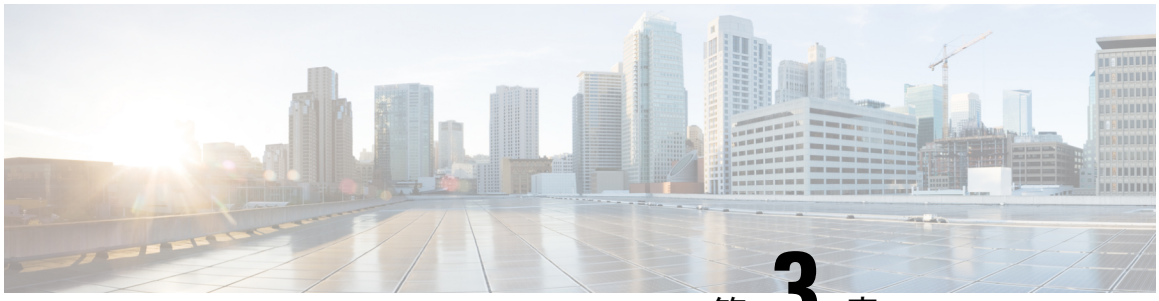
始める前に

SecureX アカウントには管理者レベルの権限が必要です。

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。



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

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

具体的には、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最新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。

直接統合の要件

要件のタイプ	要件
Cisco Secure Firewall デバイス	Management Center によって管理される Threat Defense デバイス。

要件のタイプ	要件
Cisco Secure Firewall のバージョン	管理対象デバイス • 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 Management Center バージョン 7.0.2、バージョン 7.2 以降。
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、システムにライセンスが必要です。 詳細については、Cisco Secure Firewall ライセンス情報を参照してください。 • 評価ライセンスを使用してこの統合を実行することはできません。 • 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。

要件のタイプ	要件
接続性	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。 • 北米クラウド： • api sse.cisco.com • https://eventing-ingest.sse.itd.cisco.com • https://mx*.sse.itd.cisco.com • https://securex.us.security.cisco.com • EU クラウド： • api.eu.sse.itd.cisco.com • https://eventing-ingest.eu.sse.itd.cisco.com • https://mx*.eu.sse.itd.cisco.com • https://securex.eu.security.cisco.com • アジア（APJC）クラウド： • api.apj.sse.itd.cisco.com • https://eventing-ingest.apj.sse.itd.cisco.com • https://mx*.apj.sse.itd.cisco.com • https://securex.apjc.security.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。 • 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。 • Management Center で Cisco Success Network を有効にする必要があります。 この設定を確認または有効にするには、**[Integration]** > **[SecureX]** に移動します。詳細については、「Cisco Success Network の登録設定」を参照してください。 Cisco Success Network 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。

要件のタイプ	要件
一般	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

- 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 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。複数のアカウント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決定するには、次の手順を実行します。

  1. https://software.cisco.com に進みます。
  2. [Manage Smart Account] をクリックし、ページの右上のエリアでスマートアカウントを選択します。
  3. [Users] タブをクリックして、お使いのユーザー 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。
- アカウントには、次のいずれかのユーザーロールが必要です。
  - 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

ハイアベイラビリティ展開と SecureX の統合

ハイアベイラビリティを設定するには、専用のフェールオーバーリンクで相互に接続されている 2 台の同じデバイスが必要です。2 台のデバイスがアクティブ/スタンバイペアを形成し、アクティブデバイスがトラフィックを通過させます。スタンバイデバイスはトラフィックを通過

させることはありませんが、アクティブデバイスの設定やその他の状態情報を同期しています。アクティブデバイスに障害が発生すると、スタンバイデバイスが引き継ぎ、ネットワークの運用を維持します。

次に、Threat Defense のハイアベイラビリティ展開と SecureX との統合に関するガイドラインについて説明します。

- Threat Defense のハイアベイラビリティまたはクラスタ展開を SSE と統合するには、すべてのピアを SSE と統合する必要があります。
- SSE との統合では、ハイアベイラビリティ展開におけるすべての Threat Defense デバイスでインターネット接続が必要です。
- Management Center のアクティブ/スタンバイ展開を SecureX と統合する場合は、アクティブピアを SecureX と統合する必要があります。
- Management Center のスタンバイピアをアクティブロールに昇格させると、アクティブピアとスタンバイピアの間で SecureX の設定が転送されます。SecureX リボンは、アクティブピアとスタンバイピアの両方に引き続き表示されます。
- Management Center のハイアベイラビリティ展開を中断すると、両方のピアが SecureX と統合されたままになります。

ハイアベイラビリティ展開の構成と管理の詳細については、Threat Defense および Management Center のオンラインヘルプを参照してください。

SecureX ワンクリック統合ソリューションについて

ワンクリック統合ソリューションを使用して、SecureX を有効にすると、次のことが実行されます。

- Management Center および管理対象デバイスは、SecureX 組織を使用して SSE に登録されます。
- システムのクラウド接続スイッチのデバイスライセンスと管理は、シスコスマートライセンスから SecureX 組織に切り替わります。
- Management Center および管理対象デバイスは、SecureX アカウントを使用してファイアウォールイベントをクラウドに送信します。
- SecureX ワンクリック統合ソリューションを使用すると、SecureX プラットフォーム内のすべてのファイアウォールイベントを表示できます。SecureX を使用してスマートライセンスを手動で紐づける必要はありません。

SecureX 統合機能を有効にすると、Management Center と管理対象デバイスが SecureX プラットフォームと直接統合されます。SecureX リボンは Management Center のすべてのページに表示され、Management Center から SecureX にすばやく切り替えて、他のシスコセキュリティ製品を相互起動できます。

SecureX オーケストレーションについて

SecureX オーケストレーションは、SecureX でローコードまたはゼロコード手法でワークフローとアトミックアクションを構築するためのプロセス自動化プラットフォームです。これらのワークフローは、シスコまたはサードパーティのさまざまなリソースやシステムと連携できます。

Management Center でこの機能を有効にすると、SecureX ユーザーが作成した自動ワークフローが Management Center リソースと連携できるようになります。

SecureX オーケストレーション機能の詳細については、SecureX のオンラインヘルプを参照してください。

Cisco Cloud にイベントを直接送信する方法

	操作手順	詳細情報
ステップ	送信するイベントのタイプ、イベントの送信方法、使用する地域クラウドを決定する。	「Secure Firewall Management Center と SecureX の統合について」を参照してください。
ステップ	直接統合の要件を満たす。	「直接統合の要件」を参照してください。
ステップ	イベントを送信する Cisco Cloud の地域を設定する。	「Cisco Cloud にイベントを送信するための Management Center デバイスの設定」を参照してください。
ステップ	Secure Firewall Management Center 管理対象デバイスを設定してイベントをクラウドに送信し、イベントのタイプを選択する。	「Cisco Cloud にイベントを送信するための Management Center デバイスの設定」を参照してください。
ステップ	SecureX と Management Center の統合を有効にする。	「Secure Firewall Management Center と SecureX の統合」を参照してください。
ステップ	SecureX ユーザーが作成した自動化ワークフローが Management Center と情報をやり取りできるようにする場合は、SecureX オーケストレーションを有効にする。	「Secure Firewall Management Center と SecureX の統合」を参照してください。

	操作手順	詳細情報
ステップ	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、Cisco Success Network を有効にする。	「Cisco Success Network の登録設定」を参照してください。
ステップ	（任意）システムヘルス関連の情報を Cisco Cloud にストリーミングし、シスコが問題を事前に通知できるようにする場合は、Cisco Support Diagnostics を有効にします。	「Cisco Support Diagnostics の登録設定」を参照してください。
ステップ	SecureX インターフェイスに Firepower モジュールを追する。	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。

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

管理対象の Threat Defense デバイスがイベントを直接クラウドに送信するように Management Center を設定します。

始める前に

- 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 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していることを確認します必要なポリシーが作成され、生成されたイベントが Management Center Web インターフェイスの [Analysis] タブに想定どおりに表示されているかを確認します。
- 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」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。

ステップ 1 ファイアウォールイベントの送信に使用するシスコ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

（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。

ステップ 2 Management Center で **[Integration]** > **[SecureX]** の順に選択します。

ステップ 3 [Current Region] ドロップダウンから地域クラウドを選択します。

ステップ 4 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に使用できます。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
Cisco Security Analytics and Logging (SaaS)	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	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）
- [Intrusion Events] を有効にすると、イベントは影響フラグとともに Management Center デバイスから送信されます。
- [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 5 [Save] をクリックします。

Secure Firewall Management Center と SecureX の統合

この手順では、Management Center と SecureX を統合して、SecureX プラットフォームでファイアウォールイベントを表示できるようにする方法について説明します。

始める前に

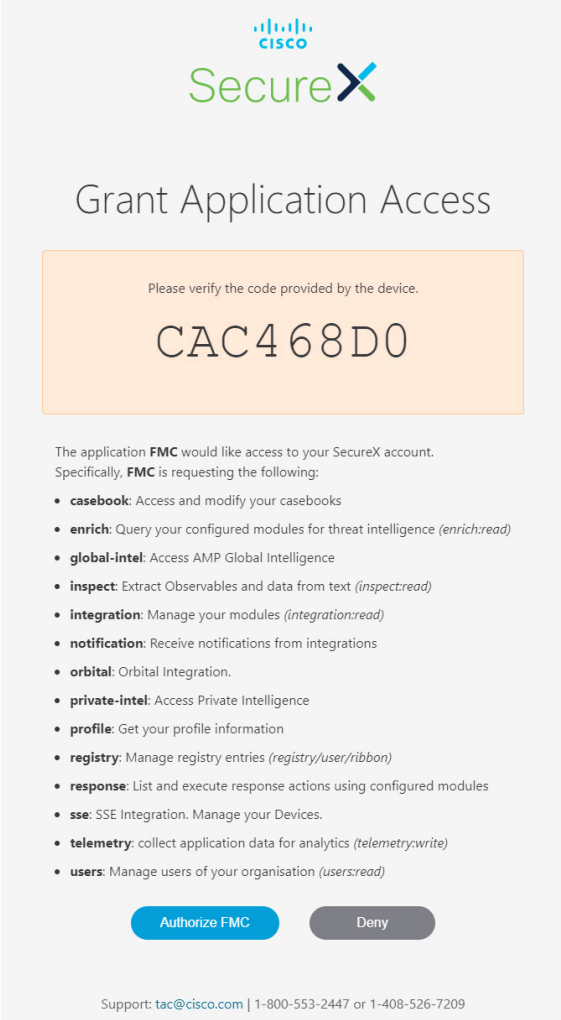
- SecureX サインオンアカウントがアクティブであることを確認します。
- 設定を変更する前に、SecureX アカウントに管理者権限があることを確認します。
- グローバルドメインから設定を変更していることを確認します。
- **Cisco SecureX Threat Response** と**イベント生成**サービスが SSE で有効になっていることを確認します。**[Security Services Exchange]** > **[Cloud Services]** でこの設定を確認します。
- 地域クラウドを選択し、Cisco Cloud のイベント設定を有効にしていることを確認します。詳細については、Cisco Cloud にイベントを送信するための Management Center デバイスの設定 （15 ページ）を参照してください。

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

ステップ 2 [SecureX Enablement] で、[Enable SecureX] をクリックします。SecureX のログイン ページが新しいブラウザウィンドウで開きます。

ステップ 3 SecureX ウィンドウに切り替え、SecureX のサインオンアカウントを使用して SecureX にサインインします。

ステップ 4 SecureX ページに表示されるコードが Management Center ページに表示されるコードと一致するかを確認し、[Authorize FMC] をクリックします。



（注） 認証することで、リストされた範囲でSecureXアカウントへのアクセスをSecure Firewall Management Centerに許可することになります。

ステップ 5 Management Center の Web インターフェイスに戻ります。

ステップ 6 SecureX ユーザーが作成した自動化ワークフローが Management Center と情報をやり取りできるようにする場合は、オーケストレーション機能を設定します。オーケストレーション機能を設定するには、次の手順を実行します。

1. [Enable SecureX Orchestration] チェックボックスをオンにします。
2. SecureX ユーザーが API を使用して Management Center リソースと双方向に情報をやり取りするために必要なロールを選択します。[Assigned Role] ドロップダウンリストからロールを選択します。

（注） ロールを割り当てない場合、デフォルトで [Access Admin] ロールが設定されます。

ステップ 7 [保存（Save）] をクリックして、設定を保存します。

[Notifications] > **[Tasks]** を選択すると、タスクの進行状況を表示できます。デバイス登録タスクが正常に完了すると、Management Center ページの下部に SecureX リボンが表示されます。

デバイス登録タスクの進行中に Management Center を使用する必要がある場合は、新しいウィンドウで Management Center を開きます。

次のタスク

- 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、Cisco Success Network を有効にします。
- SecureX インターフェイスで、Firepower 統合モジュールを追加します。詳細については、SecureX オンライン ヘルプを参照してください。

Cisco Success Network の登録設定

Cisco Success Network はユーザー対応のクラウド サービスです。Cisco Success Network を有効にすると、Management Center と Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、Management Center からの対象のデータを選択してそれを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- ネットワーク内の製品の有効性を向上させるために、利用可能な未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカルサポートサービスとモニタリングについて通知します。
- （SecureX と統合している場合）アプライアンスとデバイスのステータスを SecureX タイルにまとめ、すべての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を確認します。
- シスコ製品の改善に役立ちます。

Cisco Support Diagnostics または Cisco Success Network のいずれかを有効にすると、Management Center によって Cisco Cloudとの安全な接続が確立され、維持されます。この接続は、Cisco Success Network および Cisco Support Diagnostics の両方を無効にすることで、いつでもオフにできます。これにより、Management Center が Cisco Cloud から接続解除されます。ただし、Cisco Support Diagnostics を有効にすると、Threat Defense と Management Center の両方が Cisco Cloud との安全な接続を確立して維持します。

Smart Software Manager に Management Center を登録するときは、Cisco Success Network を有効にします。次の手順を使用して、登録ステータスを表示または変更します。

（注） Cisco Success Network は評価モードでは機能しません。

（注） Management Center に有効な Smart Software Manager オンプレミス（以前の Smart Software Satellite Server）設定がある場合、または、Specific License Reservationを使用している場合、Cisco Success Network 機能は無効になっています。

ステップ 1 [統合（Integration）] > [SecureX] をクリックします。

ステップ 2 [シスコクラウドサポート（Cisco Cloud Support）] で [Cisco Success Networkを有効化（Enable Cisco Success Network）] チェックボックスをオンにして、このサービスを有効にします。

（注） 続行する前に、[Cisco Success Networkを有効化（Enable Cisco Success Network）] チェックボックスの横にある情報を読んでください。

ステップ 3 [Save] をクリックします。

Cisco Support Diagnostics の登録設定

Cisco Support Diagnostics は、ユーザーによって有効化されるクラウドベースの TAC サポートサービスです。有効にすると、Management Center と管理対象デバイスと Cisco Cloud のセキュアな接続が確立され、システムヘルスに関する情報がストリーミングされます。

Cisco Support Diagnostics は、Cisco TAC が TAC ケースの対応中にデバイスから重要なデータを安全に収集できるようにすることで、トラブルシューティングの際によりよいユーザーエクスペリエンスを提供します。さらに、シスコは自動問題検出システムによって定期的にヘルスデータを収集および処理し、問題をユーザーに通知します。TAC ケース対応時のデータ収集サービスはサポート契約を持つすべてのユーザーが利用できますが、通知サービスは、特定のサービス契約を結んでいるお客様のみが使用できます。

Cisco Support Diagnostics または Cisco Success Network のいずれかを有効にすると、Management Center によって Cisco Cloudとの安全な接続が確立され、維持されます。この接続は、Cisco Success Network および Cisco Support Diagnostics の両方を無効にすることで、いつでも無効にできます。これにより、これらの機能は Cisco Cloud から接続解除されます。ただし、Cisco Support Diagnostics を有効にすると、Threat Defense と Management Center の両方が Cisco Cloud との安全な接続を確立して維持します。

管理者は、「特定のシステム機能のトラブルシューティング ファイルの作成」 の手順に従ってトラブルシューティング ファイルを生成し、そのファイルを開いて表示することにより、Management Center から収集されたサンプルデータセットを確認できます。

Management Centerは、収集したデータを[統合（Integration）]>[SecureX]ページの[現在のリージョン（Current Region）]で選択されたクラウドリージョンに送信します。>

Management Center を Cisco Smart Software Manager に登録する場合は、Cisco Support Diagnostics を有効にします。次の手順を使用して、Cisco Support Diagnostics の登録ステータスを表示または変更します。

ステップ 1 [統合（Integration）]>[SecureX] をクリックします。

ステップ 2 [シスコクラウドサポート（Cisco Cloud Support）]で[Cisco Support Diagnosticsを有効化（Enable Cisco Support Diagnostics）]チェックボックスをオンにして、このサービスを有効にします。

（注） 続行する前に、[Cisco Support Diagnosticsを有効化（Enable Cisco Support Diagnostics）]チェックボックスの横にある情報を読んでください。

ステップ 3 [save] をクリックします。

次のタスク

Cisco Support Diagnostics を有効にしている場合は、[統合（Integration）]>[SecureX] をクリックし、[クラウドリージョン（Cloud Region）]でクラウドリージョンの設定を確認します。>

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。

Management Center によって管理されるデバイスが SSE の [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 [Edit] 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、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 Management Center から SSE に送信され、デバイス名が Management Center で変更されても SSE で更新されません。

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、想定されるイベントが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。
- 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

- すべての接続イベントをクラウドに送信すると、SecureX と Cisco SecureX Threat Response の統合ではセキュリティ接続イベントのみが使用されます。
- Management Center でグローバルブロックリスト、許可リスト、 Secure Firewall 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。

SecureX 設定の保存に失敗する

Management Center ページで SecureX の設定を保存できない場合、以下を実行します。

- Management Center とクラウドの接続を確認します。
- SecureX の設定はグローバルドメインから変更してください。

タイムアウトが発生し、SecureX の有効化に失敗した

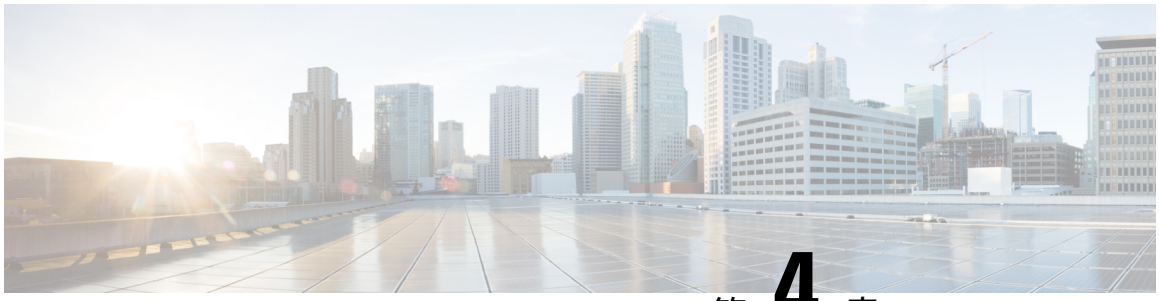
Management Center ページは設定を開始してから認証を受け取るまで 15 分間待機した後にタイムアウトします。15 分以内に認証を完了してください。タイムアウト後に新しい認証リクエストを開始するには、[Enable SecureX] をクリックします。

SecureX 組織の SSE にファイアウォールデバイスを登録できない

Management Center が管理対象デバイスを SecureX 組織の SSE に登録できない場合、**[Notification]** > **[Tasks]** の下にメッセージが表示されます。Management Center では元の設定が復元されます。デバイスの登録に失敗した場合は、次のことを確認します。

- SecureX アカウントに管理者権限があること。
- Management Center が SSE と接続されていること。

SecureX の設定を無効にしてから再度有効にし、ファイアウォールデバイスを SSE にもう一度登録します。



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

リリース 6.3 以降では、syslog を使用してサポート対象のイベントをデバイスから Cisco Cloud へ直接送信できます。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
デバイス	サポートされているバージョンのソフトウェアを実行しているデバイス
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 アクセスに必要なアカウント」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。ただし、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、お使いのシステムにライセンスが必要です。 詳細については、「ライセンス情報」を参照してください。 • 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。 • この環境は、エアギャップ環境に導入できません。
全般	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	クラウドに送信するイベント、イベントの送信方法、使用する地域クラウドを決定する。	Secure Firewall Management Center と SecureX の統合について （1 ページ）のトピックを参照してください。
ステップ	要件を満たす。	syslog を使用した統合の要件 （25 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」を参照してください。
ステップ	Cisco Security Services Proxy （CSSP）サーバーをインストールして構成する。	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。 Security Services Exchange で、ブラウザウィンドウの右上の近くにある [Tools] アイコンから [Downloads] を選択します。

	操作手順	詳細情報
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**
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デバイスを設定する。	「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、Management Center のオンラインヘルプを参照してください。
ステップ	ご使用の製品で、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。	Management Center の [Platform Settings] にある [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	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する。	--
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。	次を参照してください。 • イベントが Security Services Exchange に到達（syslog 経由）しているかの確認 （28 ページ）。 • syslog 統合のトラブルシューティング （29 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」を参照してください。
ステップ	（任意）Security Services Exchange で、重要ではない特定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の詳細については、Security Services Exchange オンラインヘルプ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」を参照してください。

	操作手順	詳細情報
ステップ	SecureX でモジュールを追加する。	SecureX で、[Integration Modules] > [Integration] に移動して、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。

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、Secure Endpoint、Secure Malware Analytics または Cisco Security 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。

[Dashboard] > **[Applications & Integrations]** > **[Security Services Exchange]** の順に選択し、[Launch] をクリックします。

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

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デバイスに表示されることを確認します。

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、デバイスがサポート対象のイベントを検出してから約 15 分かかります。

ステップ 2 Security Services Exchange にアクセスします。詳細については「Security Services Exchange へのアクセス」を参照してください。

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 （29 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 （26 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デバイス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。

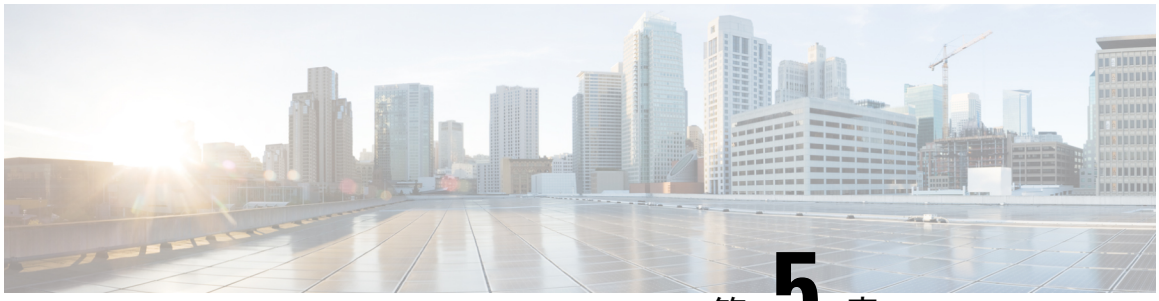
syslog のフィールドに関する質問

syslog のフィールドと説明については、「Threat Defense Syslog Messages」[英語] 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

Management Center 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

その他の参考資料

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。

SecureX のよくある質問については、SecureX のよくある質問のページを参照してください。

SecureX ダッシュボードのタイル

SecureX ダッシュボードのタイルの詳細については、「Cisco SecureX タイルのリスト」を参照してください。

Security Services Exchange 内の操作

Security Services Exchange や 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。