

# Cisco Secure Firewall Management Center (6.6.1) および SecureX 統合ガイド

最終更新：2022 年 5 月 31 日

## Cisco Secure Firewall Management Center および SecureX 統合ガイド

このガイドでは、Secure Firewall Management Center (Management Center) と SecureX の統合の手順について説明します。

### このガイドの対象読者

このガイドは、SecureX プラットフォームを初めて使用する既存の Firepower ユーザーを対象としています。このガイドは、Management Center 管理対象 Secure Firewall Threat Defense (Threat Defense) デバイス (バージョン 6.6.1) と SecureX プラットフォームの直接統合を実行する場合にのみ使用してください。

統合シナリオの詳細については、

<https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/SecureX/firepower-and-securex-integration-guide.html> で『Cisco Firepower and SecureX Integration Guide』を参照してください。

### Secure Firewall Management Center と SecureX について

SecureX は、シスコの統合セキュリティ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 エクスペリエンスです。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。

SecureX は、シスコのセキュリティ製品の購入に含まれており、SecureX ですべての Threat Defense デバイスのデータを表示できます。

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。

### Secure Firewall Management Center と SecureX の直接統合について

管理対象 Threat Defense デバイスが、サポートされているイベントを Cisco Cloud 内の Security Services Exchange (SSE) に直接送信できるように Management Center を設定できます。SSE を使用して、インシデントとして SecureX に表示されるように自動または手動でイベントを昇格できます。

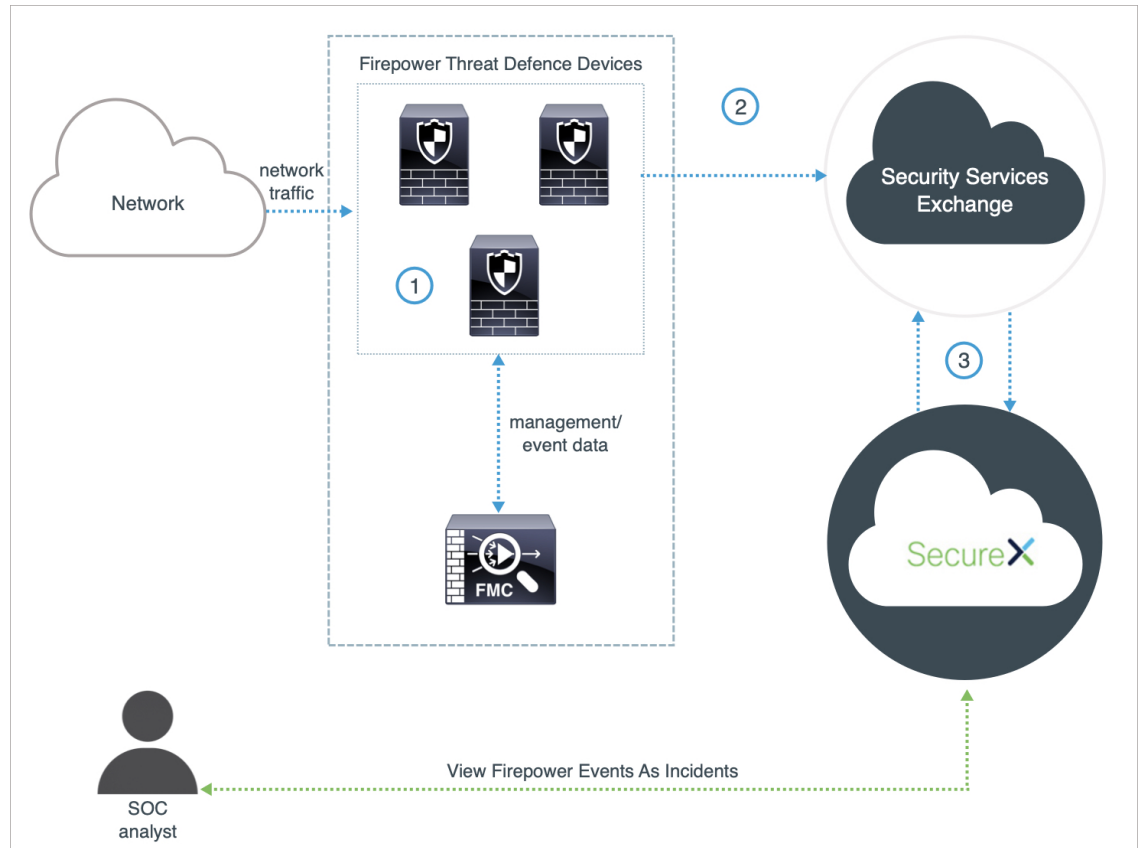
デバイスが現在のソフトウェアバージョンを実行しているかどうかなど、システムのステータスも表示できます。

直接統合では、次のイベントタイプがサポートされます。

- 侵入イベント
- 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のイベント

## 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、サポートされているイベントを SSE に送信します。
③	SecureX は、調査対象の IP アドレスに関する検出情報を SSE に照会し、SOC アナリストに追加のコンテキストを提供します。イベントは、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れます。

## この統合の主要コンポーネント

コンポーネント	説明
SecureX	シスコの統合セキュリティ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。
Security Services Exchange (SSE)	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、およびデータを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。
SecureX サインオン	1つのログイン情報で任意のデバイスからシスコのあらゆるセキュリティ製品に簡単にアクセスできるセキュアログインページ。
Cisco Success Network (CSN)	ASA の使用率情報と統計情報をストリーミングする Security Service Exchange (SSE) クラウドとのセキュアな接続を確立する、ユーザーによって有効にされるクラウドサービス。
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。

## 前提条件

前提条件タイプ	要件
Firepower デバイス	Management Center によって管理される Threat Defense デバイス
FirePOWER のバージョン	6.6.1 (Management Center とその管理対象デバイスの両方)

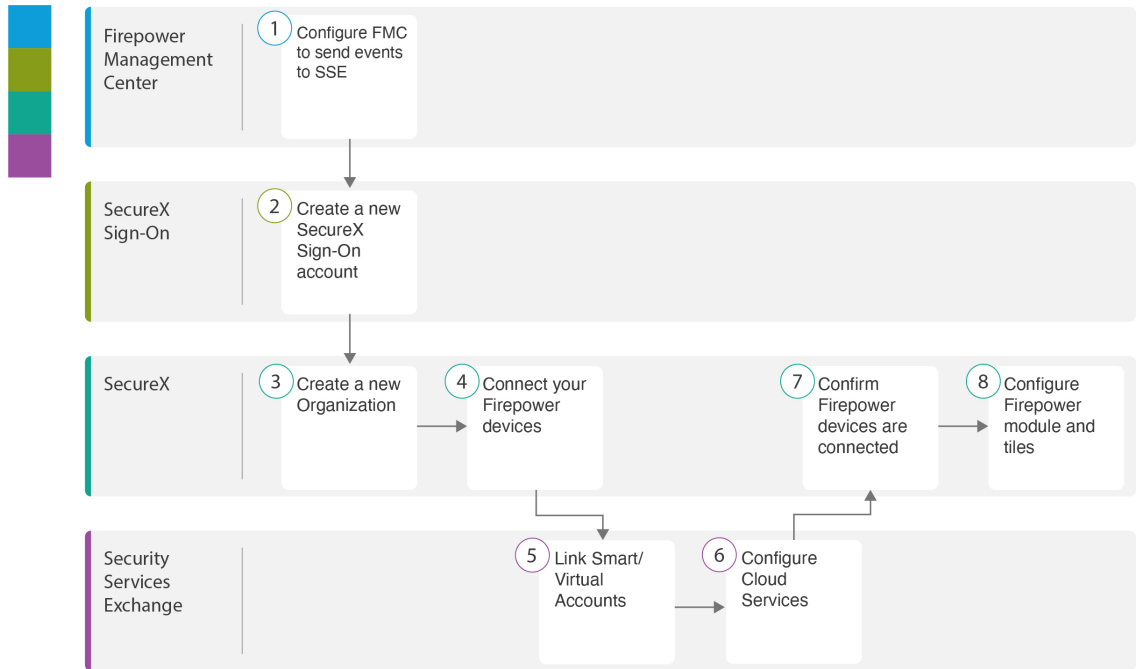
前提条件タイプ	要件
ライセンスング	<p>Cisco Smart Software Manager に Management Center を登録します。</p> <p>Management Center Web インターフェイスで、[System] (⚙) &gt; [Smart Licenses] をクリックして、次のことを確認します。</p> <ul style="list-style-type: none"> <li>• [Usage Authorization] ステータスが [Authorized] になっている。</li> <li>• [Product Registration] ステータスが [Registered] になっている。</li> </ul> <p>Management Center を Cisco Smart Software Manager に登録する手順については、<a href="https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/licensing_the_firepower_system.html">https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/licensing_the_firepower_system.html</a> を参照してください。</p> <p>次の点を考慮してください。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>

前提条件タイプ	要件
アカウント	<ul style="list-style-type: none"> <li>• Firepower 製品のライセンスを取得する Cisco スマートアカウントの管理者権限が必要です。</li> </ul> <p>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。</p> <ol style="list-style-type: none"> <li>1. <a href="https://software.cisco.com">https://software.cisco.com</a> にアクセスします。</li> <li>2. [Manage Smart Account] をクリックします。</li> <li>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。</li> <li>4. [ユーザー (Users) ] タブをクリックします。</li> <li>5. 自分のユーザー ID を検索します。</li> </ol> <ul style="list-style-type: none"> <li>• 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。 <ul style="list-style-type: none"> <li>• 管理者</li> <li>• アクセス管理者</li> <li>• ネットワーク管理者</li> <li>• セキュリティ承認者</li> </ul> </li> </ul> <p>Firepower 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] (⚙) &gt; [Users] をクリックします。</p>

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"> <li>• 北米クラウド : <ul style="list-style-type: none"> <li>• <a href="https://api.sse.cisco.com">api.sse.cisco.com</a></li> <li>• <a href="https://eventing-ingest.sse.itd.cisco.com">https://eventing-ingest.sse.itd.cisco.com</a></li> <li>• <a href="https://mx*.sse.itd.cisco.com">https://mx*.sse.itd.cisco.com</a></li> </ul> </li> <li>• EU クラウド : <ul style="list-style-type: none"> <li>• <a href="https://api.eu.sse.itd.cisco.com">api.eu.sse.itd.cisco.com</a></li> <li>• <a href="https://eventing-ingest.eu.sse.itd.cisco.com">https://eventing-ingest.eu.sse.itd.cisco.com</a></li> <li>• <a href="https://mx*.eu.sse.itd.cisco.com">https://mx*.eu.sse.itd.cisco.com</a></li> </ul> </li> <li>• アジア (APJC) クラウド : <ul style="list-style-type: none"> <li>• <a href="https://api.apj.sse.itd.cisco.com">api.apj.sse.itd.cisco.com</a></li> <li>• <a href="https://mx*.apj.sse.itd.cisco.com">https://mx*.apj.sse.itd.cisco.com</a></li> <li>• <a href="https://eventing-ingest.apj.sse.itd.cisco.com">https://eventing-ingest.apj.sse.itd.cisco.com</a></li> </ul> </li> </ul>
デバイスステータスを表示する SecureX タイルの場合	<p>デバイスが最適なバージョンを実行しているかどうかなどのシステム情報を示す SecureX タイルを表示するには、Management Center Web インターフェイスで Cisco Success Network (CSN) を有効にします。</p> <p>この設定を確認したり有効にしたりするには、Management Center Web インターフェイスの [システム (System) (⚙️)] &gt; [スマートライセンス (Smart Licenses)] ページに移動します。詳細については、Management Center オンラインヘルプで「Cisco Success Network」を検索してください。</p> <p>CSN を有効にした後、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。</p>

## Secure Firewall Management Center と SecureX の統合

Management Center と管理対象 Threat Defense デバイスを SecureX と統合するには、次のタスクを実行します。



	ワークスペース	手順
①	Secure Firewall Management Center	イベントを <a href="#">Security Services Exchange</a> に送信するための <a href="#">Secure Firewall Management Center</a> の設定 (8 ページ)。
②	SecureX サインオン	<a href="#">新しい SecureX サインオンアカウントの設定 (9 ページ)</a> : 新しい SecureX サインオンアカウントを作成します。
③	SecureX	<a href="#">新しい SecureX サインオンアカウントの設定 (9 ページ)</a> : 新しい組織を作成します。
④	SecureX	<a href="#">SecureX サインオンアカウントの有効化 (16 ページ)</a> : Firepower デバイスを接続します。
⑤	Security Services Exchange	<a href="#">SecureX サインオンアカウントの有効化 (16 ページ)</a> : スマート/バーチャルアカウントをリンクします。
⑥	Security Services Exchange	<a href="#">SecureX サインオンアカウントの有効化 (16 ページ)</a> : クラウドサービスを設定します。
⑦	SecureX	<a href="#">SecureX サインオンアカウントの有効化 (16 ページ)</a> : Firepower デバイスが接続されていることを確認します。

	ワークスペース	手順
⑧	SecureX	SecureX での Firepower モジュールとタイルの設定 (24 ページ)

## イベントを Security Services Exchange に送信するための Secure Firewall Management Center の設定

管理対象 Threat Defense デバイスにイベントを直接 SSE に送信させるように 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。

- [システム (System) ] (⚙️) > [設定 (Configuration) ] の順にクリックし、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 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 (つまり、必要なポリシーが作成され、イベントが生成されて [分析 (Analysis) ] タブの Management Center Web インターフェイスに想定どおりに表示されているかどうか) 。

### 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) ] の順にクリックします。

**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。

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。

- 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。

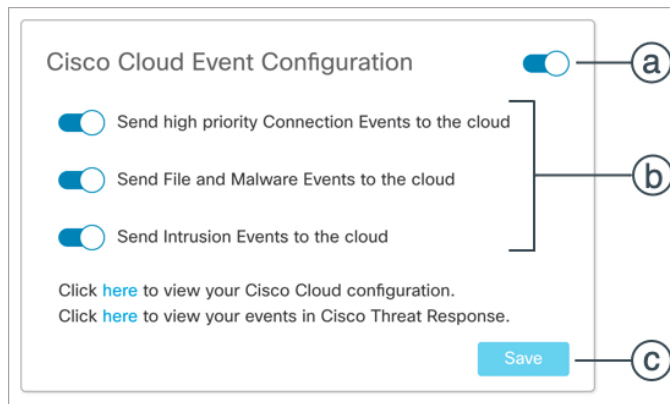


- 異なるクラウド内のデータを集約またはマージすることはできません。
- 複数の地域からデータを集約する必要がある場合は、すべての地域のデバイスが同じ地域のクラウドにデータを送信する必要があります。
- 各地域のクラウド上にアカウントを作成できます。各クラウドのデータは区分されます。

(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、[保存 (Save)] ボタンは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)。これらの機能の詳細については、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。

**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。
3. [保存 (Save)] をクリックします。

(注) 接続イベントを有効にすると、セキュリティインテリジェンス接続イベントのみが Cisco Cloud に送信されます。

## 新しい SecureX サインオンアカウントの設定

SecureX サインオンアカウントを使用すると、1 つのログイン情報で任意のデバイスからシスコのあらゆるセキュリティ製品に簡単にアクセスできます。

Management Center と SecureX を統合する新しい SecureX サインオンアカウントを作成します。

## 始める前に

- 使用する予定の地域クラウドに組織のアカウントがすでに存在するかどうかを確認します。存在する場合は、既存のアカウントを使用し、新しいアカウントの作成プロセスをスキップします。
- 自分または組織がすでに Cisco SecureX Threat Response のアカウントを持っているかどうかを確認します。存在する場合は、既存の（シスコセキュリティアカウントまたは Threat Grid）アカウントを使用して SecureX にログインし、新しいアカウントの作成プロセスをスキップします。

詳細については、

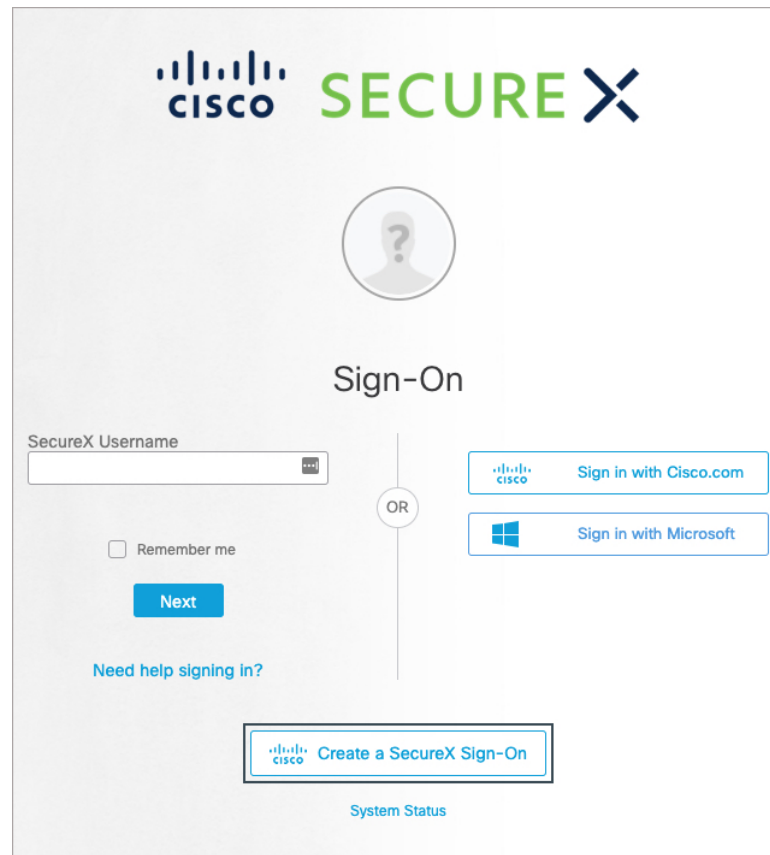
<https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/SecureX/firepower-and-securex-integration-guide.html> で『Cisco Firepower and SecureX Integration Guide』を参照してください。

- 組織内の他のユーザーがすでに地域クラウドのアカウントを持っている場合は、そのアカウントの管理者にお客様のアカウントの追加を依頼します。詳細については、<https://www.cisco.com/c/en/us/support/security/securex/products-installation-and-configuration-guides-list.html> で『Cisco SecureX Getting Started Guide』を参照してください。

## 手順

**ステップ 1 SecureX サインオン** : 新しい SecureX サインオンアカウントにサインアップします。

- a) <https://sign-on.security.cisco.com> にアクセスします。
- b) [SecureXサインオンの作成 (Create a SecureX Sign-On) ] をクリックします。



The image shows the Cisco SecureX Sign-On page. At the top, the Cisco logo and 'SECURE X' are displayed. Below the logo is a circular icon with a question mark. The main heading is 'Sign-On'. There is a text input field for 'SecureX Username' with a 'Show/Hide' icon. Below the input field is a 'Remember me' checkbox and a blue 'Next' button. To the right of the input field, there is an 'OR' separator and two buttons: 'Sign in with Cisco.com' and 'Sign in with Microsoft'. Below the 'Next' button is a link 'Need help signing in?'. At the bottom, there is a button 'Create a SecureX Sign-On' and a link 'System Status'.

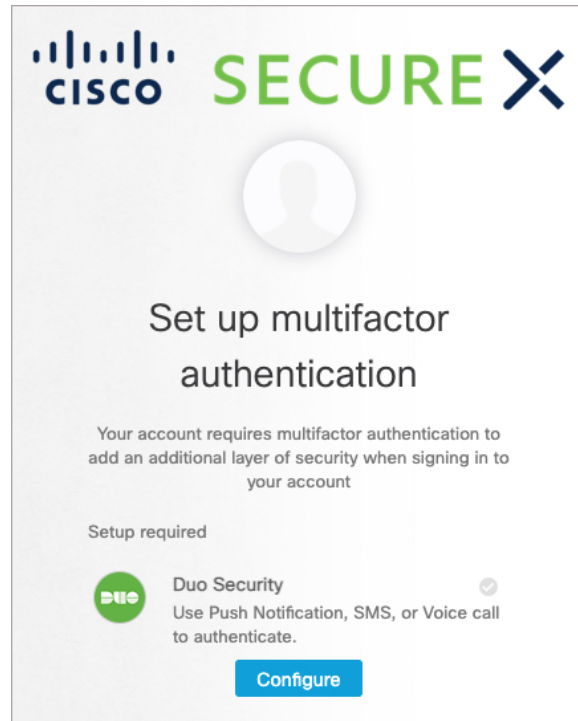
- c) フォームに入力して、[登録 (Register)] をクリックします。

The screenshot shows the Cisco SecureX 'Create Account' registration page. At the top, the Cisco logo and 'SECURE X' are displayed. The main heading is 'Create Account'. Below this, there are several input fields: an email field containing 'droberts@example.com', a password field with masked characters '.....', and three fields for 'First name' (containing 'Dave'), 'Last name' (containing 'Roberts'), and 'Company' (containing 'Macmillan Toys'). A list of password requirements is shown with green checkmarks, indicating all are met: 'At least 8 character(s)', 'At least 1 number(s)', 'At least 1 symbol(s)', 'At least 1 lowercase letter(s)', 'At least 1 uppercase letter(s)', 'Does not contain part of username', 'Does not contain 'First name'', and 'Does not contain 'Last name''. A legend indicates that an asterisk (\*) denotes a required field. A blue 'Register' button is located at the bottom of the form.

- d) 「アカウントを有効化 (Activate Account)」という件名の電子メールを検索し、[アカウントを有効化 (Activate Account)] をクリックします。

**ステップ 2 SecureX サインオン** : Duo Security を設定して多要素認証 (MFA) を設定します。

- a) [多要素認証の設定 (Set up multi-factor authentication)] 画面で、[設定 (Configure)] をクリックします。



- b) [設定の開始 (Start setup)] をクリックし、プロンプトに従ってデバイスを選択して、選択したデバイスとアカウントのペアリングを確認します。

詳細については、『[Duo Guide to MFA and Device Enrollment](#)』を参照してください。デバイスに Duo アプリケーションがすでにインストールされている場合は、このアカウントのアクティベーションコードが送信されます。Duo は 1 台のデバイスで複数のアカウントをサポートします。

(注) セキュリティを強化するため、異なるデバイスを 2 台以上登録しておくことを推奨します。[デバイスの追加 (+ Add another device)] をクリックし、プロンプトに従って別のデバイスを登録します。詳細については、『[Duo Guide to MFA and Device Management](#)』を参照してください。

- c) ウィザードの最後に、[ログインを続行する (Continue to Login)] をクリックします。  
 d) 二要素認証を使用して SecureX サインオンにサインインします。  
 e) デバイスがアカウントとペアリングされたら、[完了 (Finish)] をクリックします。

必要に応じて、MFA に Google Authenticator を使用している既存のユーザは、[Google Authenticator の設定 (Setup Google Authenticator)] をクリックしてプロンプトに従うことで、バックアップ要素としてここに追加できます。

**ステップ 3 SecureX サインオン** : SecureX サインオンアカウントのアカウントリカバリのオプションを設定します。

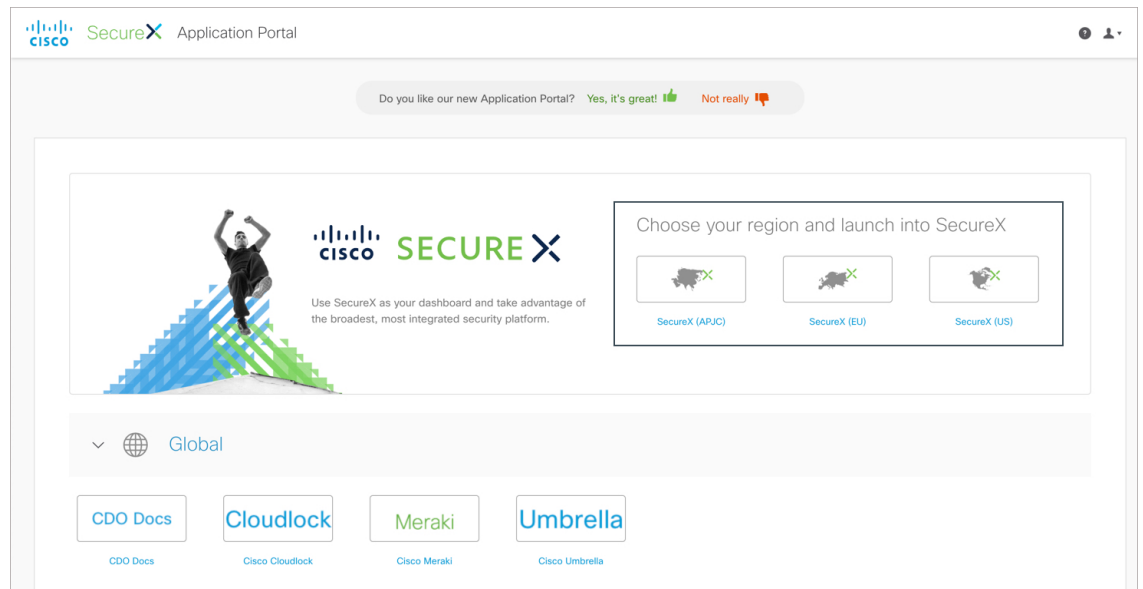
- a) (オプション) SMS を使用してパスワードをリセットしたり、アカウントのロックを解除したりするための電話番号を追加します。  
 b) セキュリティイメージを選択します。

c) [マイアカウントの作成 (Create My Account)] をクリックします。

(注) アカウントリカバリのオプションを設定する前に現在のセッションがタイムアウトした場合、SecureX サインオンは次のログイン時にオプションを設定するように求めます。

**ステップ 4 SecureX** : SecureX で新しい組織を作成します。

a) SecureX を起動する地域を選択します。



b) プロンプトが表示されたら、SecureX サインオンアカウントを使用して認証します。

c) フォームに入力し、[組織の作成 (Create Organization)] をクリックします。

**SecureX**  
Create Your Organization

Please complete the form. Required fields are marked with \*

Organization Name \*  
Macmillan Toys

Country \*  
United States

City  
San Jose

Street 1  
300 East Tasman Dr.

Street 2

Postal Code  
95134

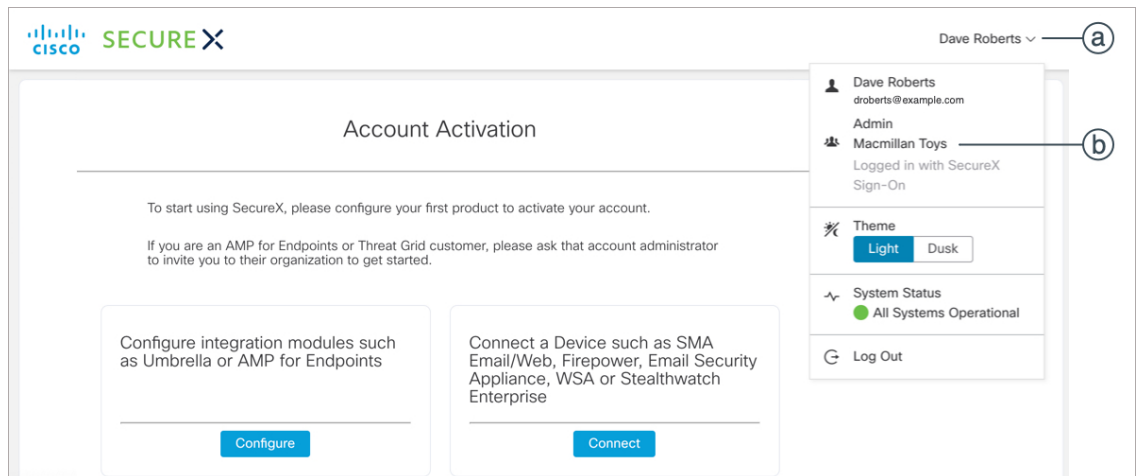
Department  
CISO

Create Organization

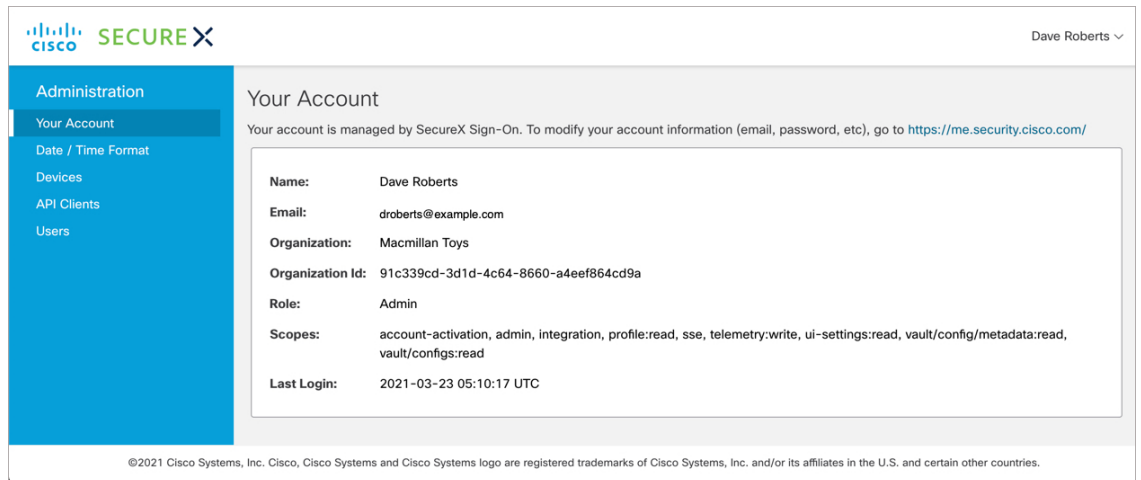
Support: [tac@cisco.com](mailto:tac@cisco.com) | 1-800-553-2447 or 1-408-526-7209

**ステップ 5 SecureX** : SecureX で新しいアカウントの詳細を確認します。

- a) [アカウントの有効化 (Account Activation) ] ページの右上隅にある自分の名前をクリックします。



- b) 組織の名前をクリックします。
- c) アカウントの詳細を確認します。



## SecureX サインオンアカウントの有効化

SecureX の使用を開始するには、少なくとも 1 台の Firepower デバイスを SecureX に接続して、SecureX サインオンアカウントを有効に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、（Firepower 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 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。
- 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、SecureX 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。

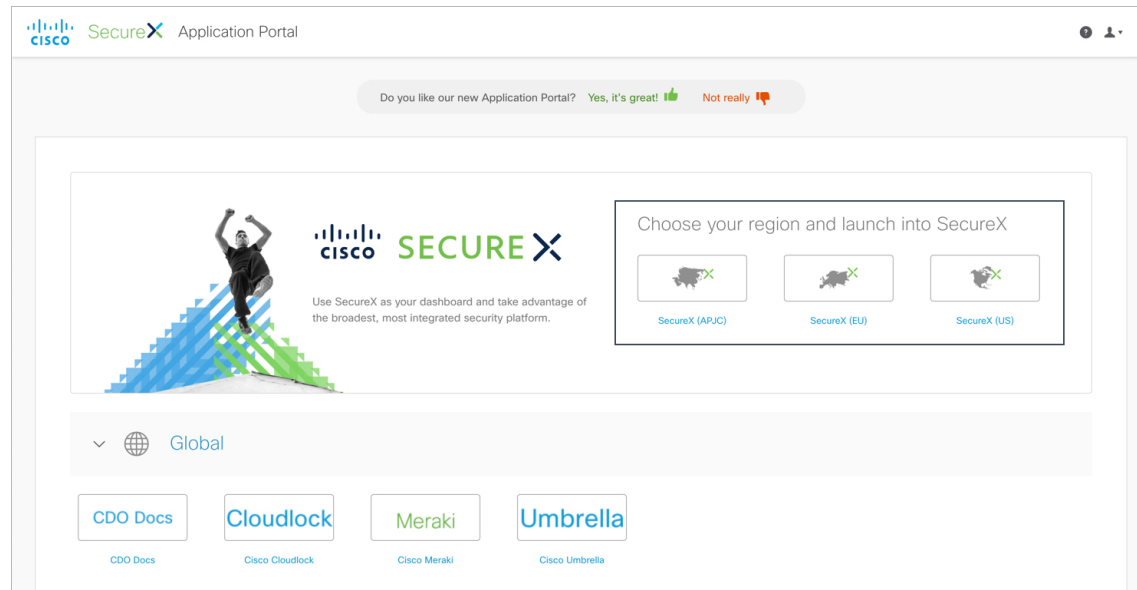


- この手順を実行するには、Cisco.com のログイン情報が必要になります。

## 手順

### ステップ1 SecureX サインオン : SecureX にアクセスします。

- <https://sign-on.security.cisco.com/>に進みます。
- SecureX サインオンアカウントを使用してサインインします。
- プロンプトが表示されたら、Duo Security を使用して認証します。
- SecureX を起動する地域を選択します。



### ステップ2 SecureX : SecureX アカウントの有効化プロセスを開始します。

- [アカウントの有効化 (Account Activation)] ページで、[接続 (Connect)] をクリックします。

**SECURE X**

## Account Activation

To start using SecureX, please configure your first product to activate your account.

If you are an AMP for Endpoints or Threat Grid customer, please ask that account administrator to invite you to their organization to get started.

Configure integration modules such as Umbrella or AMP for Endpoints

Connect a Device such as SMA Email/Web, Firepower, Email Security Appliance, WSA or Stealthwatch Enterprise

1 of 2

- b) [デバイスの接続 (Connect Device) ] ページで、[アカウントのリンク (Link Account) ] をクリックします。

**Register Device**  
If you have on-prem appliances, (ie. SMA, CSSP) register them by:

1. Following the [Registration guide](#).
2. Return to this page.
3. Click Confirm Devices Are Connected

**Register Device**

**Link Accounts**  
If you have devices registered via Cisco Smart Licensing or Cisco Defense Orchestrator, you can connect them by:

1. Following the [Link guide](#).
2. Return to this page.
3. Click Confirm Devices Are Connected

**Link Account**

After connecting a device, return to this page to confirm the device is working by clicking the button below.

**Confirm Device is Connected**

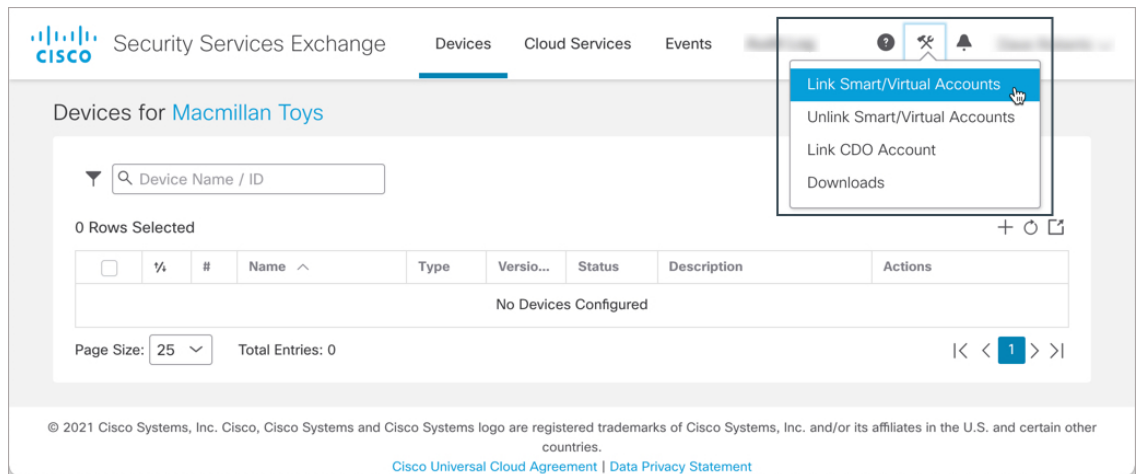
2 of 2

Web ブラウザの新しいタブで SSE が開きます。

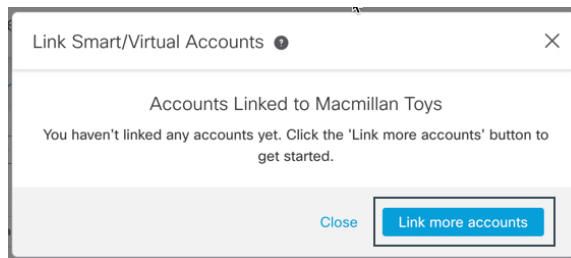
(注) SecureX タブを閉じないでください。

**ステップ 3 Security Services Exchange** : 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 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。

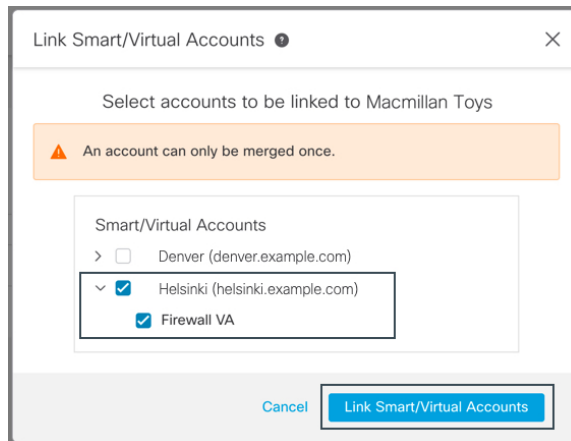
- a) SecureX サインオンアカウントを使用して SSE にサインインします。
- b) 右上隅にある [ツール (Tools)] ボタン (🔧) をクリックし、[スマート/バーチャルアカウントのリンク (Link Smart/Virtual Accounts)] を選択します。



- c) [Link More Accounts] をクリックします。



- d) 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。  
e) 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。



- f) [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。  
g) [OK] をクリックして、先へ進みます。  
h) 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。

Security Services Exchange | Devices | Cloud Services | Events | Audit Log | Dave Roberts

Devices for Macmillan Toys

Device Name / ID

0 Rows Selected

<input type="checkbox"/>	%	#	Name ^	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	[REDACTED]	Cisco Firep...	6.6.1	Registered	[REDACTED] (FMC managed)	[Actions]
<input type="checkbox"/>	>	2	firepower	Cisco Firep...	6.6.1	Registered	[REDACTED] firepower	[Actions]

Page Size: 25 | Total Entries: 2

© 2021 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.  
Cisco Universal Cloud Agreement | Data Privacy Statement

このリストにデバイス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 \(29 ページ\)](#) を参照してください。

- i) [ イベント (Events) ] タブにイベントが表示されていることを確認します。

Security Services Exchange | Devices | Cloud Services | Events | Dave Roberts

Event Stream for Macmillan Toys

Enter filter criteria

03/22/2021, 16:51 - 03/23/2021, 16:51

0 Rows Selected

<input type="checkbox"/>	Talos Disposition	Incident	Destination IP	Event Time	Ingest Time	Message	Proto	Actions
<input type="checkbox"/>	Questionable	No	[REDACTED].100	2021-03-23 16:48:41 U...	2021-03-23 16:48:42 U...	MALWARE-C...	tcp	[Actions]
<input type="checkbox"/>	Trusted	Promoting	103.[REDACTED]	2021-03-23 16:45:57 U...	2021-03-23 16:46:02 U...	MALWARE-C...	tcp	[Actions]
<input type="checkbox"/>	Trusted	No	[REDACTED].46	2021-03-23 16:45:52 U...	2021-03-23 16:45:57 U...	MALWARE-C...	tcp	[Actions]
<input type="checkbox"/>	Trusted	No	69.[REDACTED]	2021-03-23 16:45:47 U...	2021-03-23 16:45:47 U...	MALWARE-C...	tcp	[Actions]
<input type="checkbox"/>	Trusted	No	[REDACTED].201	2021-03-23 16:44:40 U...	2021-03-23 16:44:41 U...	MALWARE-C...	tcp	[Actions]
<input type="checkbox"/>	Trusted	No	50.[REDACTED]	2021-03-23 16:44:40 U...	2021-03-23 16:44:41 U...	SMTP_COM...	tcp	[Actions]
<input type="checkbox"/>	Unknown	No	[REDACTED]	2021-03-23 16:42:43 U...	2021-03-23 16:42:46 U...	INDICATOR...	udp	[Actions]
<input type="checkbox"/>	Trusted	No	[REDACTED].1	2021-03-23 16:42:40 U...	2021-03-23 16:42:41 U...	MALWARE-C...	tcp	[Actions]

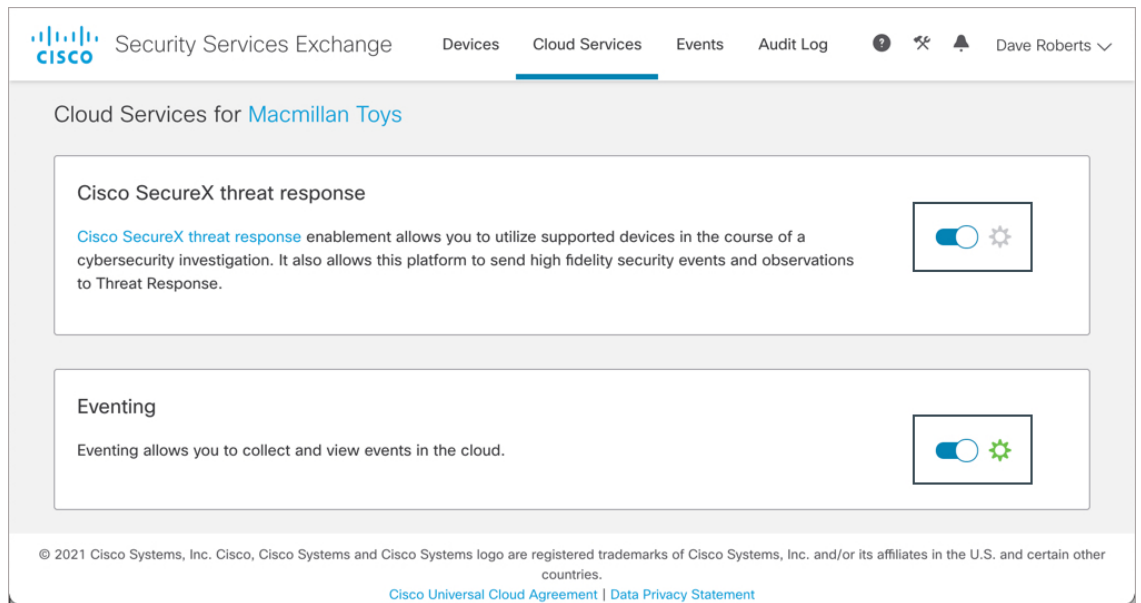
Page Size: 25 | Total Entries: 2,393


© 2021 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.  
Cisco Universal Cloud Agreement | Data Privacy Statement

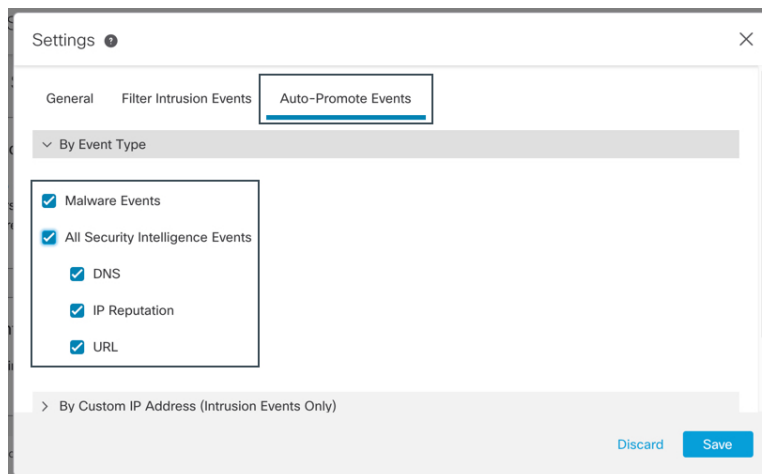
このリストに想定されるイベントが表示されない場合は、[直接統合のトラブルシューティング \(29 ページ\)](#) を参照してください。

#### ステップ 4 Security Services Exchange : SSE のクラウドサービスを設定します。

- [クラウドサービス (Cloud Services) ] タブをクリックします。
- Cisco SecureX Threat Response とイベントサービスが有効になっていることを確認します。



- c) マルウェアおよびセキュリティインテリジェンスイベントを SecureX のインシデントとして昇格するには、[イベント (Eventing)] パネルの  をクリックし、[イベントの自動昇格 (Auto-Promote Events)] タブで必要なイベントタイプを選択してから、[保存 (Save)] をクリックします。



**ステップ 5 SecureX :** SecureX アカウントの有効化プロセスを完了します。

- a) SecureX タブ ([デバイスの接続 (Connect Device)]) ページに戻り、[デバイスが接続されていることを確認する (Confirm Device is Connected)] をクリックします。

Which of these would you like to connect?

### Register Device

If you have on-prem appliances, (ie. SMA, CSSP) register them by:

1. Following the [Registration guide](#).
2. Return to this page.
3. Click Confirm Devices Are Connected

[Register Device](#)

### Link Accounts

If you have devices registered via Cisco Smart Licensing or Cisco Defense Orchestrator, you can connect them by:

1. Following the [Link guide](#).
2. Return to this page.
3. Click Confirm Devices Are Connected

[Link Account](#)

After connecting a device, return to this page to confirm the device is working by clicking the button below.

[Confirm Device is Connected](#)

2 of 2

- b) [SecureXを使用して開始 (Start using SecureX) ]をクリックします。
- c) [管理 (Administration) ]>[デバイス (Devices) ]に移動し、Management Center とその管理対象デバイスがこのページに表示されることを確認します。

Administration

Your Account  
Date / Time Format

Devices

API Clients  
Users

Dashboard Integration Modules Orchestration **Administration**

Devices

[Manage Devices](#) [Reload Devices](#)

Name	Type	Version	Description	ID	IP Address
firepower	Cisco Firepower Management Center for VMWare	6.6.1	firepower	a38f-7a8a45888c40	
	Cisco Firepower Threat Defense for VMWare	6.6.1	(FMC managed)	934b-26fb3ddf8f91	
firepower	Cisco Firepower Management Center for VMWare	6.6.1	firepower	e37c7f7880ea	1

25 per page 1-3 of 3 << 1 / 1 >>

Home Enter logs, IPs, domains, etc.

このリストにデバイス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 \(29 ページ\)](#) を参照してください。

## SecureX での Firepower モジュールとタイルの設定

Cisco SecureX は、シスコのセキュリティ製品およびサードパーティ ソリューション用の統合モジュールを提供しています。SecureX でデータと応答措置を使用できるように Firepower モジュールを設定する必要があります。

セキュリティ環境全体を可視化し、脅威への対応を促進するため、SecureX タイルには Firepower 製品のメトリックとデータが表示されます。SecureX に Firepower 統合モジュールを追加すると、Firepower タイルをダッシュボードに追加できるようになります。

### 始める前に

デバイスが最適なバージョンを実行しているかどうかなどのシステム情報を示す SecureX タイルを表示するには、Management Center で Cisco Success Network (CSN) を有効にします。

この設定を確認したり有効にしたりするには、Management Center Web インターフェイスの [システム (System) (⚙️)] > [スマートライセンス (Smart Licenses)] ページに移動します。詳細については、Management Center 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、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。

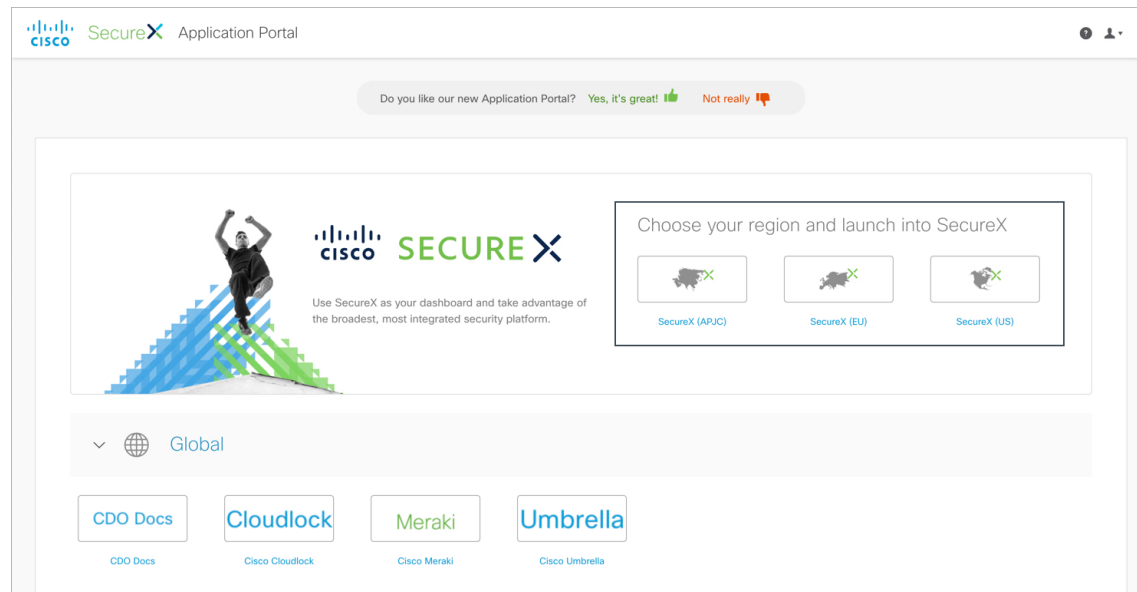
### 手順

---

**ステップ 1 SecureX サインオン** : SecureX にアクセスします。

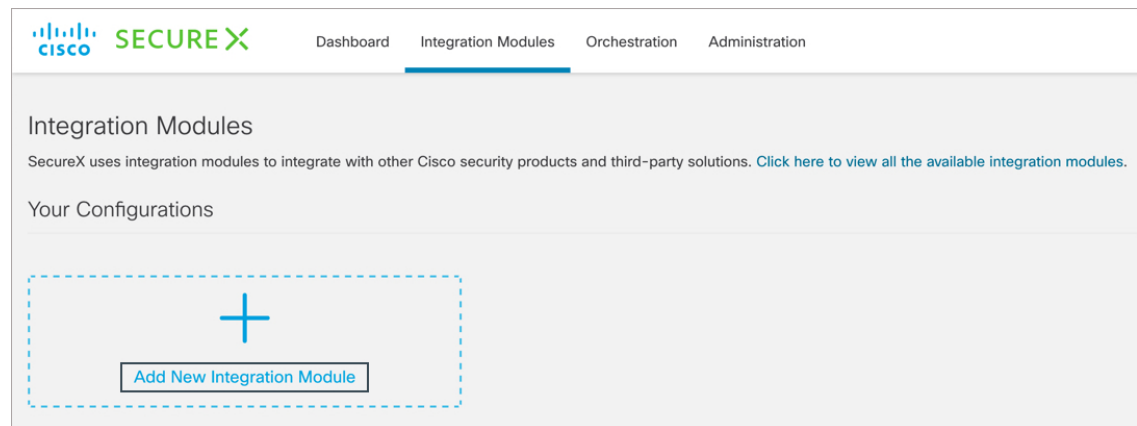
- a) <https://sign-on.security.cisco.com/>に進みます。
- b) SecureX サインオンアカウントを使用してサインインします。
- c) プロンプトが表示されたら、Duo Security を使用して認証します。
- d) SecureX を起動する地域を選択します。



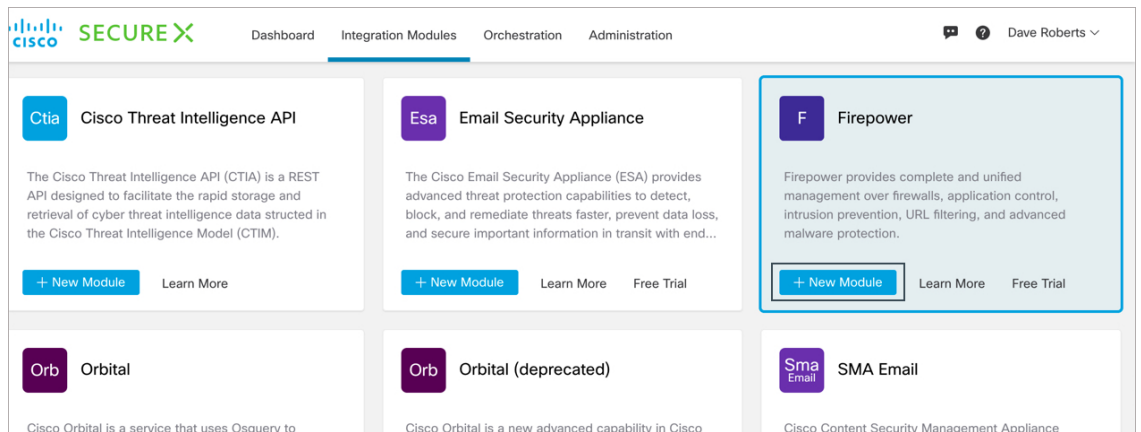


**ステップ 2 SecureX** : 新しい Firepower 統合モジュールを追加します。

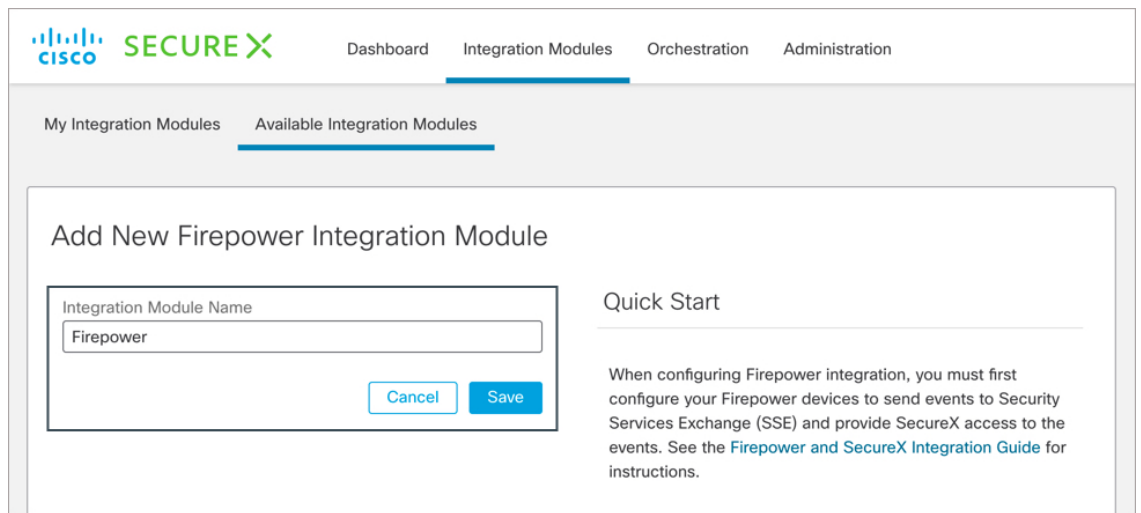
- a) [統合モジュール (Integration Modules) ] タブをクリックします。
- b) [新しい統合モジュールを追加 (Add New Integration Module) ] をクリックします。



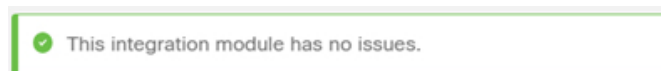
- c) Firepower 統合モジュールに移動し、[+新しいモジュール (+New Module) ] をクリックします。



- d) Firepower 統合モジュールの名前を入力し、[保存 (Save)] をクリックします。



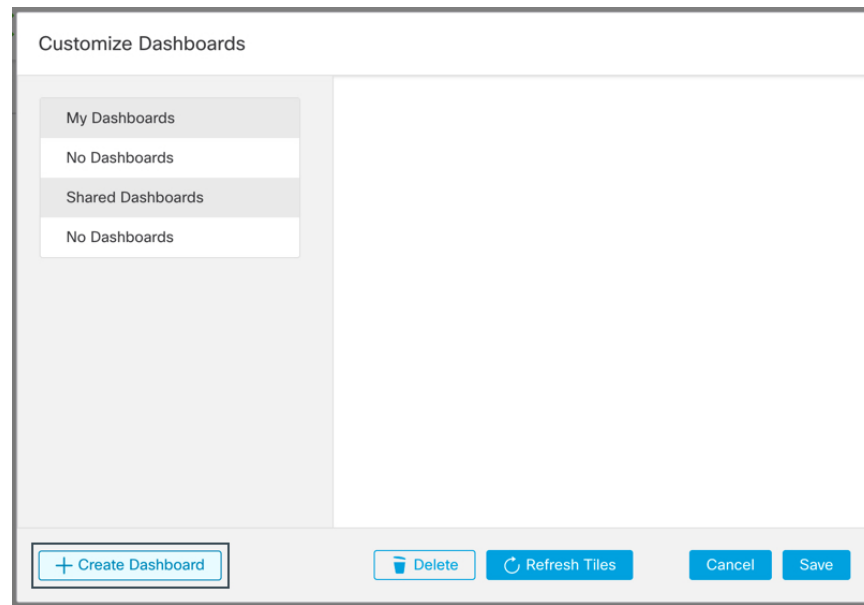
モジュールが正常に設定されたかどうかを判断するために、正常性チェックが実行されます。このプロセスが完了すると、設定に問題がないこと、またはエラーが検出されたことを示すメッセージが表示されます。



新しく追加されたモジュールは、[使用中の統合モジュール (My Integration Modules)] ページ ([統合モジュール (Integration Modules)] タブ) に表示されます。

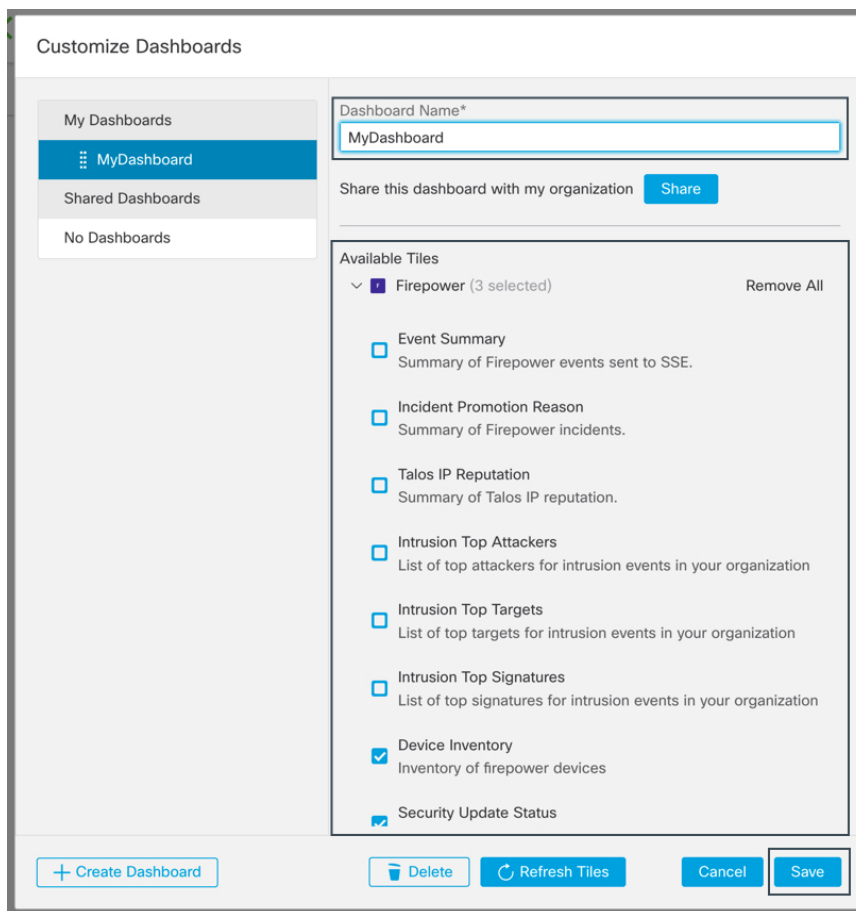
### ステップ 3 SecureX : Firepower タイルを追加します。

- [ダッシュボード (Dashboard)] タブをクリックします。
- [タイルの追加 (Add Tiles)] をクリックします。
- 新しいダッシュボードを作成するには、[ダッシュボードの作成 (Create Dashboard)] をクリックします。



または、既存のダッシュボードを使用できます。

- d) ダッシュボードの名前を入力し、必要な Firepower タイルを選択して、[保存 (Save) ] をクリックします。



タイルを追加した後、サイズを変更して、SecureX ダッシュボード上の目的の位置に移動することができます。

### 次のタスク

お客様が SecureX の管理者ユーザーの場合、

- SecureX 経由で組織に参加するようにユーザーを招待します。
- Firepower ダッシュボードを組織内の他のユーザーと共有します。

手順については、SecureX オンラインヘルプを参照してください。

## 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みます。
- アカウントに関連付けられている地域クラウドの正しい URL にアクセスしていることを確認してください。

### デバイスインターフェイスには統合が有効と表示されているが、[デバイス (Devices)] ページには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。
  - 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。

Management Center 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、Management Center 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。

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

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 FMC で変更されても SSE で更新されません。

### SSEの[デバイス (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 Device Manager によって管理されている Threat Defense デバイスであり、SecureX 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、『Cisco Firepower および SecureX 統合ガイド』 (<https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/SecureX/firepower-and-securex-integration-guide.html>) の「CDO アカウントと SecureX アカウントのマージ」の手順を実行してください。

### 予期していたイベントが[SSEイベント (SSE 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。
- 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。

### 一部のイベントが欠落している

- 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。
- Management Center で、グローバルブロックリストや許可リストおよび 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。

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。



## 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。