



CDO と SecureX を統合する

- [SecureX と CDO \(1 ページ\)](#)

SecureX と CDO

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。統合プラットフォームでの接続技術により、SecureX は測定可能な分析情報、望ましい成果、比類のないチーム間のコラボレーションを実現します。SecureX の概要とこのプラットフォームが提供する機能の詳細については、「[SecureX について](#)」を参照してください。

SecureX に CDO テナントへのアクセスを許可すると、デバイスの合計数、エラーのあるデバイス、競合のあるデバイス、現在同期していないデバイスの数など、デバイスイベントの概要が表示されます。イベントの概要には、現在適用されているポリシーとそれらのポリシーに関連付けられているオブジェクトの集計を示す 2 番目のウィンドウも表示されます。ポリシーはデバイスタイプによって定義され、オブジェクトはオブジェクトタイプによって識別されま

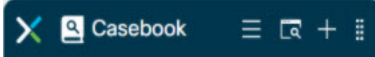
す。

CDO モジュールを SecureX ダッシュボードに追加するには、複数の手順が必要です。詳細については、「[CDO の SecureX への追加](#)」を参照してください。



警告 CDO アカウントと SecureX アカウントをまだマージしていない場合、導入準備されたすべてのデバイスのイベントを表示できないことがあります。SecureX で CDO モジュールを作成する前に、アカウントをマージすることを強くお勧めします。詳細については、「[CDO アカウントと SecureX アカウントのマージ](#)」を参照してください。

SecureX のリボン

SecureX のリボンは、SecureX アカウントを作成するかどうかにかかわらず、CDO で使用できます。ページの下部にある SecureX タブ  をクリックして、リボンを展開します。

リボンを使用するには、SecureX アカウントを検証する必要があります。SecureX へのアクセスに使用するのと同じ認証ログインを使用することを強くお勧めします。リボンが認証されると、CDO から直接 SecureX 機能を利用できるようになります。

詳細については、[SecureX リボンのドキュメント](#)を参照してください。

SecureX のトラブルシューティング

このエクスペリエンスには 2 つの製品が関係します。発生する可能性のある問題の特定、解決、または問い合わせに役立つ「[SecureX のトラブルシューティング](#)」を参照してください。

関連情報：

- [SecureX について](#)
- [CDO アカウントと SecureX アカウントのマージ](#)
- [CDO の SecureX の接続 \(3 ページ\)](#)
- [CDO の SecureX の切断 \(4 ページ\)](#)
- [CDO の SecureX への追加](#)
- [SecureX のトラブルシューティング](#)

CDO アカウントと SecureX アカウントのマージ

SecureX または Cisco Threat Response (CTR) アカウントをすでにお持ちの場合、デバイスを SecureX に登録するには、CDO アカウントと SecureX/CTR アカウントをマージする必要があります。アカウントは、SecureX ポータルにマージできます。CDO モジュールを作成する前に、アカウントをマージすることを強く推奨します。アカウントがマージされるまで、デバイスのイベントを SecureX で表示したり、他の SecureX 機能を利用したりすることはできません。

手順については、SecureX の「[アカウントのマージ](#)」を参照してください。



(注) 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。

関連情報：

- [SecureX と CDO](#)
- [CDO の SecureX への追加](#)

- [SecureX のトラブルシューティング](#)

CDO の SecureX への追加

SecureX が登録済みデバイスにアクセスできるようにし、CDO モジュールを SecureX ダッシュボードに追加して、セキュリティポートフォリオ内の他のシスコプラットフォームとともにデバイスポリシーとオブジェクトの概要を表示します。

はじめる前に

CDO で SecureX を接続する前に、次のアクション項目を確認することを強くお勧めします。

- SecureX アカウントの管理者以上である必要があります。
- CDO テナントの SuperAdmin ユーザーロールを保有している必要があります。
- テナントの通信を容易にするために、Security Service Exchange (SSE) でテナントアカウントをマージします。詳細については、「[CDO アカウントと SecureX アカウントのマージ](#)」を参照してください。
- まだマージしていない場合は、Cisco Secure Sign-On を SAML シングルサインオン ID プロバイダー (IdP) として設定し、Duo Security を多要素認証 (MFA) 用に設定します。CDO と SecureX では、認証方式として多要素認証が使用されます。詳細については、「[SAML シングルサインオンと Cisco Defense Orchestrator の統合](#)」を参照してください。



- (注) 注：複数のテナントがある場合は、SecureX でテナントごとに 1 つのモジュールを作成する必要があります。各テナントには、承認用の一意の API トークンが必要です。

CDO の SecureX の接続

SecureX アカウントと CDO アカウントをマージした後、2 つのプラットフォーム間の通信を認可し、CDO モジュールが SecureX ダッシュボードに追加されるように手動で有効にする必要があります。CDO UI を介して SecureX に接続し、デバイスのポリシー、イベントタイプ、オブジェクトなどの概要を、セキュリティポートフォリオに含まれる他のシスコプラットフォームとともに表示します。



- (注) SecureX ダッシュボードで CDO モジュールがすでに設定されている場合、[テナントを SecureX に接続 (Connect Tenant to SecureX)] オプションにより、重複した CDO モジュールが作成されます。この問題が発生した場合は、「[SecureX のトラブルシューティング](#)」詳細を参照してください。

次の手順を使用して、CDO から API トークンを取得し、CDO モジュールを SecureX に追加します。

-
- ステップ1 CDO にログインします。
 - ステップ2 右上隅のユーザーメニューから、[設定] を選択します。
 - ステップ3 ウィンドウの左側にある [全般設定 (General Settings)] タブを選択します。
 - ステップ4 [テナント設定] セクションを見つけて、[SecureX の接続 (Connect SecureX)] をクリックします。ブラウザウィンドウが SecureX のログインページにリダイレクトします。CDO テナントに関連付ける組織のログイン情報を使用して SecureX にログインします。
 - ステップ5 SecureX に正常にログインすると、ブラウザは自動的に CDO にリダイレクトします。[全般設定 (General Settings)] ページの [ユーザー管理 (User Management)] タブに、SecureX へのログインに使用した組織の名称を含む新しいユーザーが表示されます。このユーザーは読み取り専用で、SecureX にデータを送信するためにのみ使用されます。
-

CDO の SecureX の切断

CDO と SecureX 組織の間の通信リクエストを切断することができます。このオプションでは、SecureX の組織は削除されませんが、CDO から読み取り専用 API ユーザーが削除され、SecureX 組織に関連付けられていたテナントがイベントレポートの送信を停止します。

なお、これにより、CDO の SecureX リボンからテナントがログアウトしたり、リボンが無効になることはありません。リボンからログアウトするには、[Support Case Manager](#) でケースを開いてリボンのログインを手動でリセットする必要があります。このリクエストにより、テナントがリボンからログアウトします。

-
- ステップ1 CDO にログインします。
 - ステップ2 右上隅のユーザーメニューから、[設定] を選択します。
 - ステップ3 ウィンドウの左側にある [全般設定 (General Settings)] タブを選択します。
 - ステップ4 [テナント設定] セクションを見つけて、[SecureX の切断 (Disconnect SecureX)] をクリックします。[全般設定 (General Settings)] ページの [ユーザー管理 (User Management)] タブで、SecureX にデータを送信するために作成された読み取り専用ユーザーが削除されます。
-

CDO タイルの SecureX への追加

CDO モジュールを有効にしたら、CDO タイルを SecureX ダッシュボードに追加できます。製品のモジュールは、CDO からのステータス情報にアクセスし、選択可能な 2 つのタイルを介してダッシュボードにデータを報告します。

次の手順を使用して、CDO タイルを SecureX ダッシュボードに追加します。

ステップ 1 SecureX の [ダッシュボード (Dashboard)] タブ  で、[新しいダッシュボード (New Dashboard)] をクリックします。SecureX ダッシュボードに初めてアクセスする場合は、[タイルの追加 (Add Tiles)] をクリックすることもできます。

ステップ 2 (任意) ダッシュボードの名前を変更します。

ヒント 複数のテナントがある場合は、この名前変更オプションを使用して、CDO タイルが関連付けられているテナントを識別します。

ステップ 3 [使用可能なタイル (Available Tiles)] のリストから CDO を選択し、オプションを展開して使用可能なタイルを表示します。ダッシュボードに含めるタイルをすべて選択します。

- [CDO デバイスの概要 (CDO Device Summary)] : このタイルには、CDO テナントに現在導入準備されているすべてのデバイスとそのステータスの一覧が表示されます。
- [CDO オブジェクトとポリシー (CDO Objects and Policies)] : このタイルには、デバイスに現在適用されているすべてのポリシーと、それらのポリシーに関連付けられているオブジェクトの一覧が表示されます。

(注) CDO の一覧が表示されない場合、SecureX には CDO からの有効な API トークンが保存されていません。詳細については、[CDO タイルの SecureX への追加](#) ことに関するトピックを参照してください。

ステップ 4 [保存 (Save)] をクリックします。

関連情報 :

- [CDO アカウントと SecureX アカウントのマージ](#)
- [SecureX のトラブルシューティング](#)

