顧客をシスコ セキュア インターネット ゲートウェイ（SIG）に安全に接続する

Cisco Defense Orchestrator で Umbrella を管理する

Umbrella は、シスコのクラウドベース Secure Internet Gateway（SIG）プラットフォームです。インターネットベースの脅威に対する防御を複数のレベルで提供します。Umbrellaは、セキュア Web ゲートウェイ、ファイアウォール、DNS レイヤセキュリティ、およびクラウド アクセス セキュリティ ブローカ（CASB）機能を統合して、システムを脅威から保護します。SIG およびDNS 保護を利用することにより、ASA デバイスは、デバイスのローカル DNS インスペクションポリシーと Umbrella クラウドベースの DNS インスペクションポリシーの両方を使用して保護されます。Umbrellaは、着信トラフィックを検査および検出するいくつかの方法を提供することにより、ASA デバイスを FTD 次世代ファイアウォール（NGFW）に匹敵するものにします。

現時点では、CDO は Umbrella 組織との ASA の統合のみをサポートしています。

SASE を使用したブリッジの構築

セキュアアクセス サービスエッジ（SASE）は、ネットワーキング機能とセキュリティ機能を単一のサービスに統合する先進的なフレームワークであり、クラウドエッジで動作して保護と優れたパフォーマンスを実現します。この取り組みにより、場所に関係なくサービスを安全かつ確実に統合する方法が提供され、組織の規模にかかわりなくネットワークを制御および管理できるようになります。複雑さが軽減され、管理が俊敏になれば、展開がシンプル、スケーラブルかつ安全になります。

Umbrella 組織とは

Umbrella 組織は、1 つのライセンスキーに関連付けられたさまざまなユーザーロールを持つユーザーのグループです。 1 人のユーザーが複数の Umbrella 組織にアクセスできます。すべ

ての Umbrella 組織は、Umbrella の個別のインスタンスであり、独自のダッシュボードを持ちます。組織は名前と組織 ID によって識別されます。組織 ID により組織が識別され、仮想アプライアンスなどのコンポーネントの展開に使用されます。また、サポートに組織 ID が必要となる場合があります。

SIG トンネルとは

セキュア インターネット ゲートウェイ（SIG）トンネルは、ASA と Umbrella の間で生成される SIG IPSec（インターネット プロトコル セキュリティ）トンネルのインスタンスであり、インターネットに向かうすべてのトラフィックは Umbrella SIG に転送され、検査およびフィルタリングされます。このソリューションは、セキュリティの中央管理を実現するため、ネットワーク管理者は各ブランチのセキュリティ設定を個別に管理する必要がありません。

トンネルが設定されている Umbrella 組織を導入準備すると、これらのトンネルは CDO のサイト間 VPN ページに一覧表示されます。CDO UI から Umbrella 組織の SASE トンネルを作成するには、「Cisco Umbrella 用の SASE トンネルの設定」を参照してください。

（注） Umbrella 組織とそのピアデバイスを導入準備した場合、サイト間 VPN ページで、その組織に関連付けられているトンネルに接続するすべてのデバイスが 1 つのエントリにまとめられます。[トンネル（Tunnels）]ページを手動で更新し、Umbrella ダッシュボードから加えられた変更を読み取るには、「Umbrella のトンネル設定の読み取り」を参照してください。

CDO と Umbrella の通信方法

Umbrella 組織と、その組織に関連付けられている ASA デバイスを導入準備する必要があります。

ASA デバイスが Umbrella クラウドに関連付けられている場合、その接続には、デバイスとクラウドの間に安全な接続を作成するためのサイト間 VPN SIG トンネルが必要です。CDO は、Umbrella 組織と ASA デバイスの両方と通信します。このデュアル通信方式により、CDO は設定の変更またはトンネルの変更を即座に検出し、Umbrella、ASA、およびトンネルのアウトオブバンドの変更、エラー、または異常な状態について時を移さず警告します。

Umbrella 組織を CDO に導入準備する場合、組織の API キーと秘密を使用して導入準備します。どちらも組織とその組織に関連付けられている ASA デバイスに固有のものを使用します。CDO は Umbrella API を使用して Umbrella クラウドと通信し、組織の導入準備に使用された API キーと秘密を使用して、ASA デバイスに関する情報を要求および送信します。このレベルの通信で、ASA と Umbrella クラウドの間に存在する SIG トンネルが危険にさらされることはありません。

Umbrella 組織が導入準備されると、[デバイスとサービス]ページに、組織に関連付けられている検出済みの ASA デバイスが「ピア」として表示され、デバイスが CDO に導入準備されているかどうかが示されます。ピアデバイスがまだ導入準備されていない場合は、[デバイスの導入準備] をクリックして、そのページから直接導入準備することも可能です。Umbrella 組織に関連付けられている ASA デバイスが CDO に導入準備されると、[デバイスとサービス] ページにその関係が表示され、[VPN トンネル（VPN Tunnels）] ページにデバイスと組織間のトンネルが表示されます。組織に関連付けられている ASA デバイスが CDO に導入準備されていない

場合、デバイスに関連付けられているトンネルが [VPNトンネル（VPN Tunnels）] に表示されるので、このページから直接デバイスを導入準備することができます。

CDO から Umbrella クラウドへのアクセス方法

Umbrella 組織が CDO に正常に導入準備されると、CDO UI から組織のダッシュボードまたは [Umbrellaトンネル（Umbrella Tunnels）] ページをクロス起動できます。

CDO UI から Umbrella クラウドにアクセスするには、「Umbrella ダッシュボードのクロス起動（7 ページ）」と「[Cisco Umbrellaトンネル（Umbrella Tunnels）] ページのクロス起動 （8 ページ）」を参照してください。

前提条件

サポート対象ハードウェアおよびソフトウェア

Umbrella 組織はクラウドベースであるため、バージョンがありません。Umbrella 組織を CDO に導入準備する際、その組織を関連付けることができるのは 1 台の ASA デバイスのみであることに注意してください。

Umbrella 統合の場合、CDO は 9.1.2 以降を実行する ASA デバイスをサポートします。CDO がサポートする ASA デバイスモデルとソフトウェアのリストについては、「クラウドデバイスのサポートの詳細」を参照してください。

ライセンス要件

Umbrella 組織を CDO に正常に導入準備するには、次のいずれかのライセンスパッケージを選択する必要があります。

- Umbrella SIG Essentials
- SIG Advantage

オンボーディング

Umbrella アカウントを正常に管理するには、Umbrella 組織のオンボーディングとそれに関連付けられている ASA デバイスの両方を導入準備する必要があります。Umbrella 組織を導入準備すると、CDO は組織に関連付けられた既存の ASA トンネルを読み取り、これらのトンネルと、作成して組織に関連付けた追加のトンネルの正常性ステータスを監視します。Umbrella 組織を導入準備する前に、一般的なデバイス要件と導入準備の前提条件を確認してください。

Umbrella 組織に関連付けられた ASA デバイスを導入準備する前に、その組織を導入準備した場合は、[サイト間VPN] ページから ASA ピアを表示して、VPN ページからデバイスを導入準備できます。

（注） フェールオーバー用に設定された ASA ペアがある場合は、2 つのピアのうちアクティブデバイス**のみ**を導入準備する必要があります。アクティブデバイスとスタンバイデバイスの両方を CDO に導入準備すると、Umbrella ですでに設定されている SASE トンネルと重複するトンネル情報が生成される場合があります。

ネットワークのモニタリング

CDO は、セキュリティポリシーの影響を要約したレポートを発行し、セキュリティポリシーによってトリガーされた重要なイベントの表示方法を提供します。また CDO は、デバイスに加えた変更をログに記録し、それらの変更にラベルを付ける方法を提供します。これにより、CDO で確定した操作をヘルプチケットやその他の操作要求に関連付けることができます。

ログの変更

変更ログは、CDO で行われた設定変更を継続的にキャプチャします。この単一のビューには、サポートされているすべてのデバイスとサービスにおける変更が含まれます。Umbrella はクラウドベースの製品であるため、変更は即座に展開されます。

変更ログの機能の一部を次に示します。

- デバイス構成に加えられた変更の対照比較。
- すべての変更ログエントリの平易な英語のラベル。
- デバイスの導入準備と削除の記録。
- CDO の外部で発生するポリシー変更の競合の検出。
- インシデントの調査またはトラブルシューティング中に、誰が、何を、いつを回答。
- 完全な変更ログまたは一部のみを CSV ファイルとしてダウンロード可能。

（注） Umbrella 組織に関連付けられた SASE トンネルを作成、編集、または削除すると、Umbrella 組織とそれに関連付けられている ASA デバイスの要求と設定の変更が表示されることに注意してください。

Umbrella ドキュメント

- Umbrella ヘルプ
- Umbrella と Cisco ASA の設定
- トンネル経由での Cisco Umbrella への接続
- Cisco Umbrella API

Umbrella 組織の導入準備

Umbrella ライセンス要件

Cisco Umbrella 組織を CDO に正常に導入準備するには、Cisco Umbrella ダッシュボードから次のいずれかのライセンスパッケージを選択する必要があります。

- Umbrella SIG Essentials
- SIG Advantage

現在有効になっているライセンスを確認するには、Cisco Umbrella ダッシュボードにログインし、**[管理（Admin）]** > **[ライセンス（Licensing）]**に移動します。

Umbrella 組織 ID

組織を CDO に正常に導入準備するには、Umrbrella 組織 ID の場所を特定し、それをログイン資格情報とともに使用する必要があります。

ステップ 1 Cisco Umbrella ダッシュボードにアクセスして、組織にログインします。

ステップ 2 ページの URL には数字の ID が含まれています。たとえば、https://dashboard.umbrella.com/o/**123456**/#/overview の組織 ID は **123456** です。

ステップ 3 URL から組織 ID をコピーします。使用する準備ができるまで、一時的にメモに貼り付けることをお勧めします。

API キーと秘密の生成

Umbrella 組織を CDO に導入準備する前に、新しい API キーを生成し、**API キー**と対応する**シークレット**の**両方**を取得します。API キーをすでに持っているものの、シークレットを保存していない場合は、**[管理（Admin）]** > **[API キー（API Keys）]** 画面に移動し、[更新] をクリックしてキーとシークレットを更新します。それ以外の場合は、次の手順を使用して新しい API キーを作成します。

始める前に

Umbrella からの管理 API キーは、次の Umbrella サービスに使用されます。

- ネットワークおよびドメイン
- ネットワークトンネル
- ユーザおよびロール
- 接続先リスト
- サービス プロバイダー

これらのサービスへの CDO アクセスを許可せずに Umbrella 組織を導入準備することはできません。

ステップ 1 Cisco Umbrella ダッシュボードにアクセスして、組織にログインします。

ステップ 2 Umbrella ダッシュボードの左側のナビゲーションウィンドウで [管理（Admin）] をクリックし、[APIキー（API Keys）] を選択します。

ステップ 3 [API キーの作成（Create API Key）] をクリックします。

ステップ 4 [Umbrella管理（Umbrella Management）] を選択します。**[Next]** をクリックします。

ステップ 5 API キーと対応するシークレットをコピーします。使用する準備ができるまで、一時的にメモに貼り付けることをお勧めします。

Umbrella 組織のオンボーディング

Umbrella 組織を CDO に導入準備するには、次の手順を使用します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 青いプラスボタンをクリックして、デバイスのオンボーディングを開始します。

ステップ 3 [Umbrella組織（Umbrella Organization）] をクリックします。

ステップ 4 Umbrella ダッシュボードから生成した Umbrella ネットワークデバイスの [APIキー（API Key）] と [秘密（Secret）] を入力します。

ステップ 5 **[Next]** をクリックします。

ステップ 6 正しい組織名と組織 ID が表示されていることを確認してください。

ステップ 7 **[Next]** をクリックします。

ステップ 8 （オプション）デバイスに固有の [ラベル（Labels）] を追加します。後で、このラベルでデバイスのリストをフィルタリングできます。

ステップ 9 [ダッシュボードとサービスに移動（Go to Dashboard & Services）] をクリックします。

Umbrella 組織の CDO への再接続

警告 保存されているログイン情報が無効である場合、CDO は、Umbrella 組織への設定変更の展開や Umbrella 組織からの設定変更の読み取りを正常に実行できませんが、その組織に関連付けられた ASA デバイスへの設定変更の展開やそれらのデバイスからの設定変更の読み取りは正常に実行できます。そのため、ログイン情報が更新および検証されると、問題が発生する可能性があります。設定変更を展開する前に、組織のログイン情報を更新することをお勧めします。

Umbrella組織のAPIキーとシークレットが更新されたか、タイムアウトした場合は、デバイスを CDO に手動で再接続する必要があります。再接続するには、次の手順を実行します。

ステップ 1 Umbrella ダッシュボードに移動します。左側のナビゲーションウィンドウで [管理（Admin）] をクリックし、既存の Umbrella 管理の **API キー**を選択します。

ステップ 2 [更新（Refresh）] をクリックします。API キーとシークレットを更新することを確認します。

ステップ 3 API キーと対応するシークレットをコピーします。

ステップ 4 CDO にログインします。

ステップ 5 [デバイスとサービス（Devices & Services）] ページに移動します。

ステップ 6 フィルタまたは検索バーを使用して Umbrella 組織を見つけます。

ステップ 7 [デバイスアクション] ペインで、[再接続（Reconnect）] をクリックします。CDO は、保存されている API キーとシークレットが無効になっていることを確認します。

ステップ 8 API キーとシークレットを適切なポップアップウィンドウに貼り付けます。

ステップ 9 [続行（Continue）] をクリックします。

ステップ 10 新しいキーとシークレットが有効であることを CDO が確認したら、[閉じる（Close）] をクリックします。

Umbrella ダッシュボードのクロス起動

ASA デバイスと Cisco Umbrella 組織が CDO に正常に導入準備されると、CDO UI から組織のダッシュボードをクロス起動できます。

次の手順を使用して、デバイスの Cisco Umbrella ダッシュボードをクロス起動します。

ステップ 1 CDO にログインします。

ステップ 2 [デバイスとサービス（Devices & Services）] をクリックします。

ステップ 3 Cisco Umbrella 組織を検索またはフィルタリングします。フィルタ

ステップ 4 [管理] ペインで [Cisco Umbrella組織の管理（Manage Umbrella Organization）] をクリックします。CDO が新しいタブをブラウザで起動し、選択した組織に関連付けられた Cisco Umbrella ダッシュボードが開きます。

CDO からのデバイスの削除

CDO からデバイスを削除するには、次の手順を使用します。

ステップ 1 CDO にログインします。

ステップ 2 [インベントリ] ページに移動します。

ステップ 3 削除するデバイスを見つけ、そのデバイスの行でデバイスをチェックして選択します。

ステップ 4 右側にある [デバイスアクション] パネルで、[削除] を選択します。

ステップ 5 プロンプトが表示されたら、[OK] を選択して、選択したデバイスの削除を確認します。[キャンセル] を選択して、デバイスを導入準備したままにします。

Umbrella 組織の設定

Umbrella のトンネル設定の読み取り

Umbrella 組織が CDO に導入準備されると、CDO に手動で Umbrella からトンネル設定を要求および更新させることができます。これには、追加、削除、または変更されたトンネルが含まれます。

警告 Umbrella 組織の資格情報が無効と見なされているときにトンネルが CDO から削除された場合、または組織を導入準備してから変更された場合、CDO は、組織に関連付けられた ASA デバイスにのみトンネル設定を展開できます。ログイン情報の更新時に、CDO は Umbrella の設定を読み取り、削除されたすべてのトンネルを再度追加します。Umbrella 組織に存在するものの、いずれの ASA デバイスにも存在しないトンネルがあると、同期の問題が発生し、ASA デバイスが組織のピアとして表示されない場合があります。

ステップ 1 CDO にログインします。
ステップ 2 [デバイスとサービス（Devices & Services）] ページで、[デバイス（Devices）] タブをクリックします。
ステップ 3 [SFCN] タブをクリックします。
ステップ 4 Umbrella 組織を選択して強調表示します。
ステップ 5 [アクション] ペインで、[トンネルの読み取り（Read Tunnels）] を選択します。

[Cisco Umbrella トンネル（Umbrella Tunnels）] ページのクロス起動

ASA デバイスと Cisco Umbrella 組織が CDO に正常に導入準備されると、CDO UI からトンネルの Cisco Umbrella ダッシュボードをクロス起動できます。

次の手順を使用して、デバイスの [Cisco Umbrella トンネル（Umbrella Tunnels）] ページをクロス起動します。

ステップ 1 CDO にログインします。
ステップ 2 [VPN] ウィンドウに移動します。[サイト間VPN] を選択します。
ステップ 3 目的のトンネルを選択して強調表示します。

ステップ 4 [アクション] ペインで、[Cisco Umbrellaのトンネルの管理（Manage Tunnel in Umbrella）] をクリックします。CDO により、ブラウザで新しいタブが起動され、[トンネル（Tunnels）] の概要ページが開きます。

Cisco Umbrella 用の SASE トンネルの設定

次の手順を使用して、Cisco Umbrella 組織の SASE トンネルを作成します。

始める前に

トンネルを作成する Cisco Umbrella 組織と ASA デバイスは、すでに CDO に導入準備されている必要があることに注意してください。

展開したトンネルに関連付けられた ASA または Cisco Umbrella 組織が異常な状態になっている場合、CDOはトンネルを正常に展開できないことがあります。問題が発生した場合は、Cisco TAC にお問い合わせください。

ステップ 1 CDO にログインします。

ステップ 2 [VPN] ウィンドウに移動します。[サイト間VPN] を選択します。

ステップ 3 青色のプラスボタンをクリックし、[SASEトンネルの作成（Create SASE Tunnel）] を選択します。

ステップ 4 Cisco Umbrella ピア情報を入力します。

- [Cisco Umbrellaの選択（Select Umbrella）]：選択した **Cisco Umbrella** 組織を選択します。
- [データセンター（Datacenter）]：ヘッドエンドデータセンターを選択します。Cisco Umbrella 組織に関連付けられている ASA に地理的に近いデータセンターを選択することをお勧めします。

ステップ 5 ASA ピア情報を入力します。

- [ASAデバイスの選択（Select ASA Device）]：ドロップダウンリストから Cisco Umbrella 組織に関連付けられている ASA デバイスを選択し、[選択（Select）] をクリックします。
- [パブリックインターフェイス（Public Facing Interface）]：静的でパブリックにルーティング可能な IPv4 アドレスを選択します。使用されるアドレスは、NAT には使用しないでください。
- [LANアドレス（LAN Address）]：LAN サブネットを制御する LAN インターフェースを選択します。LAN 用に少なくとも 1 つのインターフェースを選択する必要があります。
- [仮想トンネルインターフェイス（Virtual Tunnel Interface）]：Cisco Umbrella 組織と ASA ピアデバイスを選択すると、このフィールドは自動的に入力されます。必要に応じて、新しい VTI として使用される IP アドレスを手動で入力できます。

ステップ 6 Cisco Umbrella 組織と ASA ピアデバイスを選択すると、[パスフレーズ（Passphrase）] が自動的に入力されます。[確認パスフレーズ（Confirm Passphrase）] も自動的に入力されます。必要に応じて、これらのフィールドに手動で入力できます。

ステップ 7 （任意）ポップアップウィンドウの下部にある [変更をASAにすぐに展開（Deploy changes to ASA immediately）] トグルは、デフォルトで有効になっています。有効になっている場合、SASE トンネル設定は、トンネル設定で選択されたASAピアにすぐに展開されます。変更をステージングして後で展開する場合は、オプションを手動で無効に切り替えます。

ステップ 8 [展開（Deploy）] をクリックします。必要に応じて、[展開してもう 1 つ作成（Deploy and Create Another）] をクリックして、この SASE トンネルを同時に展開し、別のトンネルを作成します。展開されたトンネルは [VPNトンネル（VPN Tunnels）] ページに表示されます。[展開して別のSASEトンネルを作成（Deploy and Create Another SASE tunnel）] を選択した場合、CDO は Cisco Umbrella 組織の選択と [変更をASAにすぐに展開（Deploy changes to ASA immediately）] トグル設定の両方を保存し、これらの選択を次のトンネル設定に自動的に適用します。展開する前に、これらの選択を手動で変更できます。

SASE トンネルの編集

次の手順を使用して、既存の SASE トンネルを変更します。

ステップ 1 CDO にログインします。

ステップ 2 [VPN] ウィンドウに移動します。[サイト間VPN] を選択します。

ステップ 3 変更するトンネルを選択します。

ステップ 4 [アクション] ペインで、[編集] を選択します。

ステップ 5 SASE トンネルの次のフィールドを編集します。

- [名前（Name）]：CDO および Cisco Umbrella ダッシュボードに表示される SASE トンネルの名前を変更します。
- [Cisco Umbrellaピアのデータセンター（Umbrella Peer's Datacenter）]：ドロップダウンメニューから新しいヘッドエンドデータセンターを選択します。
- [ASAピアのパブリックインターフェイス（ASA Peer's Public Facing Interface）]ドロップダウンメニューから新しい IPv4 アドレスを選択します。
- [ASAピアのLANインターフェイス（ASA Peer's LAN Interfaces）]：ドロップダウンメニューから 1 つ以上の新しい LAN インターフェイスを選択します。
- [ASA仮想トンネルインターフェイス（VTI）アドレス（ASA Virtual Tunnel Interface (VTI) Address）]：VTI を手動で編集します。
- [パスフレーズ（Passphrase）]：トンネルのパスフレーズを手動で変更します。
- [パスフレーズの確認（Confirm Passphrase）]：このエントリを手動で変更してパスフレーズと照合し、新しい値を確認します。

ステップ 6 （任意）ポップアップウィンドウの下部にある [変更をASAにすぐに展開（Deploy changes to ASA immediately）] トグルは、デフォルトで有効になっています。有効になっている場合、SASE トンネル設定は、トンネル設定で選択されたASAピアにすぐに展開されます。変更をステージングして後で展開する場

合は、オプションを手動で無効に切り替えます。変更をステージングして後で展開することを選択した場合、[インベントリ] ページの ASA ピアステータスは [Deploy Pending（展開保留中）] と表示されます。

ステップ 7 [更新の保存（Save Updates）] を選択します。

Umbrella からの SASE トンネルの削除

CDO UI を使って SASE トンネルを削除するには、次の手順を使用します。

始める前に

SASE トンネルを削除するには、それに関連付けられている ASA が CDO で同期済みのステータスになっている必要があります。デバイスが正常でない場合は、トンネルを削除できません。

CDO から SASE トンネルを削除すると、トンネルは、関連付けられている ASA デバイスと Umbrella 組織の両方から削除されることに注意してください。

警告 Umbrella 組織のログイン情報が無効と見なされているときに CDO からトンネルを削除した場合や、組織を導入準備した後に変更した場合、CDO は、組織に関連付けられた ASA デバイスにのみトンネル設定を展開できます。ログイン情報の更新時に、CDO は Umbrella の設定を読み取り、削除されたすべてのトンネルを再度追加します。Umbrella 組織に存在するものの、いずれの ASA デバイスにも存在しないトンネルがあると、同期の問題が発生し、ASA デバイスが組織のピアとして表示されない場合があります。組織に関連付けられたトンネルを削除する前に、Umbrella のログイン情報を確認することをお勧めします。

ステップ 1 CDO にログインします。

ステップ 2 [VPN] ウィンドウに移動します。[サイト間VPN] を選択します。

ステップ 3 CDO から削除するトンネルを選択します。

ステップ 4 [操作（Actions）] ウィンドウで、[削除（Delete）] をクリックします。

ステップ 5 トンネルを削除することを確認し、[OK] をクリックします。