Cisco Defense Orchestrator へのアプライアンスの接続

この章は、次の項で構成されています。

Cisco Defense Orchestrator の統合の概要

Cisco Defense Orchestrator はクラウドベースのプラットフォームであり、ネットワーク運用スタッフがシスコのセキュリティ デバイスに対するセキュリティ ポリシーを管理することで、エンドツーエンドセキュリティ ポスチャを確立および維持できます。アプライアンスを Cisco Defense Orchestrator に接続し、アプライアンスのセキュリティ ポリシー設定を分析することで、ポリシーの不整合を特定および解決し、ポリシーの変更をモデル化してその影響を検証し、ポリシーの変更を調整してセキュリティ ポスチャの整合性を実現し、その明瞭さを維持することができます。

Cisco Defense Orchestrator モードで機能を設定および使用する方法

Cisco Defense Orchestrator のサブセットに含まれる機能の使用方法は、注記した点を除き、標準モードと同じです。詳細については、Cisco Defense Orchestrator モードでの設定の変更と制約 （2 ページ）を参照してください。

この章は本書のさまざまな個所と関連しており、標準モードと Cisco Defense Orchestrator モードの両方に共通する Web セキュリティ アプライアンスの主要機能の一部は、それらの個所に記載されています。

この章には、標準モードでは適用できない Cisco Defense Orchestrator の設定に関する情報が記載されています。

本書には、Cisco Defense Orchestrator に関する情報は記載されていません。Cisco Defense Orchestrator のドキュメントは、https://docs.defenseorchestrator.com [英語] から入手できます。

Cisco Defense Orchestrator モードでの展開

要件に応じて、次にいずれかの方法を使用して Cisco Defense Orchestrator モードでアプライアンスを設定することができます。

- **システム セットアップ ウィザードを使用する。**新しいアプライアンスがある場合は、この方法を使用します。システムセットアップウィザードを実行している間に、Cisco Defense Orchestrator の動作モードを選択します。この説明については、システムセットアップ ウィザードを使用した Cisco Defense Orchestrator モードでのアプライアンスの設定 （4 ページ） を参照してください。
- **Web インターフェイスで Cisco Defense Orchestrator 設定のページを使用する。**標準モードの既存のデバイスがあり、既存のポリシーを使用している場合は、この方法を使用します。Cisco Defense Orchestrator を使用してこれらのポリシーを管理できるようになります。この説明については、Web インターフェイスを使用した Cisco Defense Orchestrator モードでの標準モードの設定 （5 ページ） を参照してください。

Cisco Defense Orchestrator モードでの設定の変更と制約

ここでは、Cisco Defense Orchestrator への Web セキュリティ アプライアンスのオンボーディング後に発生する設定の変更について説明します。また、設定可能なオプションと制約についても説明します。

（注） 以下に示す制約以外には、Web インターフェイスでの制約はありません。Cisco Defense Orchestrator からの認証はサポートされていません。

オンボーディング後の Web セキュリティ アプライアンスでの制約：

アプライアンスでは、Cisco Defense Orchestrator から管理される機能は設定できません。アプライアンスのオンボーディング時に、これらの機能の設定が Cisco Defense Orchestrator に移行されます。アプライアンスのその他の設定はデフォルトに設定されます。

Cisco Defense Orchestrator から管理される機能がない場合、その他のすべての機能はアプライアンスで使用可能になります。

オンボーディング後は、アクセス ポリシーは Cisco Defense Orchestrator から制御されます。以下に例外を示します。次のアクセス ポリシー機能は Web セキュリティ アプライアンスだけで設定できます。

- アクセス ポリシー：ポリシー定義（Access Policies- Policy Definitions）
  - プロトコルとユーザエージェント（Protocols and User Agents）
  - マルウェア対策とレピュテーション（Anti-Malware and Reputation）
- カスタム URL カテゴリ（外部ライブ フィード カテゴリ）（Custom URL Categories (External Live Feed Category)）

次の機能は Cisco Defense Orchestrator でのみ設定できます。

- カスタム URL カテゴリ（ローカル カスタム カテゴリ）
- URL フィルタリング、アプリケーション、およびオブジェクト（サイズおよびカスタム MIME タイプを除く）
- グローバル アクセス ポリシーと非グローバル アクセス ポリシー
- アクセス ポリシーでは次の操作がサポートされています。
  - 複数のアクセス ポリシーの追加がサポートされています。
  - アクセス ポリシーの追加、並べ替え、削除がサポートされています。
  - URL フィルタリング（定義済み URL カテゴリ フィルタリング）、アプリケーション、およびオブジェクト（オブジェクト タイプ）には次の制限があります。
    - アプリケーションとアプリケーション タイプの帯域幅制限はサポートされていません。
    - アーカイブ済みオブジェクトの場合、検査はサポートされていません。
    - アクセス ポリシーとアイデンティティの詳細なメンバーシップ定義はサポートされていません。
    - 範囲要求転送はサポートされていません。
    - 時間とボリュームのクォータ管理はサポートされていません。
    - URL でのセーフ サーチ、参照例外、サイト コンテンツ レーティングはサポートされていません。

Cisco Defense Orchestrator でのレポートが有効な場合は次のようになります。

- Cisco Defense Orchestrator で要約レポートが使用可能になります。
- Web セキュリティ アプライアンスでもレポート機能が使用可能になります。
- セキュリティ管理アプライアンスではレポート機能は使用可能になりません。

システムセットアップウィザードを使用したCisco Defense Orchestrator モードでのアプライアンスの設定

システム セットアップ ウィザードを使用して、アプライアンスのインストール時に、その新しいアプライアンスを Cisco Defense Orchestrator モードで設定できます。

始める前に

Web セキュリティ アプライアンスを Cisco Defense Orchestrator にオンボードした後に発生する設定の変更について詳しくは、Cisco Defense Orchestrator モードでの設定の変更と制約 （2 ページ）を参照してください。

ステップ 1 ブラウザを開き、Web セキュリティ アプライアンスの IP アドレスを入力します。システム セットアップ ウィザードを初めて実行する際は、デフォルトの IP アドレスを使用します。

```
https://192.168.42.42:8443
```

または

```
http://192.168.42.42:8080
```

ここで、`192.168.42.42` はデフォルト IP アドレス、`8080` は HTTP のデフォルトの管理ポートの設定、`8443` は HTTPS のデフォルトの管理ポートです。

あるいは、アプライアンスが現在設定されている場合は、M1 ポートの IP アドレスを使用します。

ステップ 2 アプライアンスのログイン画面が表示されたら、アプライアンスにアクセスするためのユーザ名とパスフレーズを入力します。アプライアンスには、デフォルトで、次のユーザ名とパスフレーズが付属しています。

- ユーザ名：`admin`
- パスフレーズ：`ironport`

ステップ 3 [システム管理（System Administration）] > [システム セットアップ ウィザード（System Setup Wizard）] を選択します。

ステップ 4 ライセンス契約の条項に同意します。

ステップ 5 [セットアップの開始（Begin Setup）] をクリックします。

ステップ 6 アプライアンス モードとして [Cisco Defense Orchestrator] を選択します。

ステップ 7 必要に応じて、以下のセクションで提供されるリファレンス テーブルを使用して、すべての設定を行います。システム セットアップ ウィザードの参照情報（2-11 ページ）を参照してください。

ステップ 8 レビューしてインストールします。

a) インストールを確認します。
b) 前に戻って変更する場合は、[前へ（Previous）] をクリックします。
c) 入力した情報を使って続行する場合は、[この設定をインストール（Install This Configuration）] をクリックします。

セットアップ中に設定したIPアドレス、ホスト名、DNS設定によっては、この段階でアプライアンスへの接続が失われることがあります。「ページが見つかりません（Page Not Found）」というメッセージがブラウザに表示される場合は、新しいアドレス設定が反映されるようにURLを変更し、ページをリロードします。プロンプトが表示されたら、クレデンシャルを入力します。

ステップ 9 [Cisco Defense Orchestrator ポータル（Cisco Defense Orchestrator Portal）] をクリックします。ブラウザの設定に応じて、ポータルが新しいウィンドウまたはタブに開きます。

ステップ 10 Cisco Defense Orchestrator ポータルで、以下の手順を実行します。

a) Cisco Defense Orchestrator ポータルにログインします。
b) ポータルで Web セキュリティ アプライアンスをオンボードします。
c) 登録トークン（キー）をコピーします。

ステップ 11 Web セキュリティ アプライアンスで Cisco Defense Orchestrator 登録を完了します。次の操作を行ってください。

a) **[ネットワーク（Network）] > [Cisco Defense Orchestrator]** の順に選択します。
b) 登録トークン（キー）を入力し、[登録（Register）] をクリックします。
c) 登録が正常に完了すると、成功メッセージが表示されます。

（注） このステップを実行すると、ポリシーを適用するために使用していたコンテンツ セキュリティ管理アプライアンスがポリシーの変更を Cisco Web セキュリティ アプライアンスに反映できなくなります。

次のタスク

- （任意）アプライアンスが Cisco Defense Orchestrator にレポートを送信するように設定します。Cisco Defense Orchestrator のレポートを有効にする方法 （8 ページ）を参照してください。
- Cisco Defense Orchestrator で、アクセス ポリシーを設定します。https://docs.defenseorchestrator.com/を参照してください。

関連トピック

Cisco Defense Orchestrator モードの問題のトラブルシューティング （9 ページ）

Web インターフェイスを使用した Cisco Defense Orchestrator モードでの標準モードの設定

アプライアンスに既存のポリシーが設定されていて、それらのポリシーを Cisco Defense Orchestrator で管理したい場合は、この手順に従ってください。

始める前に

Web セキュリティ アプライアンスを Cisco Defense Orchestrator にオンボードした後に発生する設定の変更について詳しくは、Cisco Defense Orchestrator モードでの設定の変更と制約 （2 ページ）を参照してください。

ステップ 1 [ネットワーク（Network）] > [Cisco Defense Orchestrator] の順に選択します。

ステップ 2 [Cisco Defense Orchestrator の設定（Cisco Defense Orchestrator Settings）] で [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [有効化（Enable）] を選択し、[送信（Submit）] をクリックします。

ステップ 4 変更を保存します。

（注） このステップを実行すると、ポリシーを適用するために使用していたコンテンツ セキュリティ管理アプライアンスがポリシーの変更を Cisco Web セキュリティ アプライアンスに反映できなくなります。

ステップ 5 [Cisco Defense Orchestrator ポータル（Cisco Defense Orchestrator Portal）] をクリックします。ブラウザの設定に応じて、ポータルが新しいウィンドウまたはタブに開きます。

ステップ 6 Cisco Defense Orchestrator ポータルで、以下の手順を実行します。

a) Cisco Defense Orchestrator ポータルにログインします。
b) ポータルで Web セキュリティ アプライアンスをオンボードします。
c) 登録トークン（キー）をコピーします。

ステップ 7 Web セキュリティ アプライアンスで Cisco Defense Orchestrator 登録を完了します。次の操作を行ってください。

a) **[ネットワーク（Network）]** > **[Cisco Defense Orchestrator]** の順に選択します。
b) 登録トークン（キー）を入力し、[登録（Register）] をクリックします。
c) 登録が正常に完了すると、成功メッセージが表示されます。

次のタスク

- （任意）アプライアンスが Cisco Defense Orchestrator にレポートを送信するように設定します。Cisco Defense Orchestrator のレポートを有効にする方法 （8 ページ）を参照してください。
- Cisco Defense Orchestrator で、アプライアンスのアクセス ポリシーを分析します。https://docs.defenseorchestrator.com/を参照してください。

関連トピック

Cisco Defense Orchestrator モードの問題のトラブルシューティング （9 ページ）

Cisco Defense Orchestrator の無効化

始める前に

Cisco Defense Orchestrator を無効化した後、再び有効化する必要がある場合は、Cisco Defense Orchestrator ポータルから登録トークン（キー）を再生成して、アプライアンスのオンボーディングを再び実行する必要があります。Cisco Defense Orchestrator の有効化 （7 ページ）を参照してください。

ステップ 1 [ネットワーク（Network）] > [Cisco Defense Orchestrator] の順に選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [有効化（Enable）] をオフにします。

ステップ 4 変更内容を送信し、確定します。

Cisco Defense Orchestrator の有効化

始める前に

Cisco Defense Orchestrator ポータルに接続できることを確認します。

ステップ 1 [ネットワーク（Network）] > [Cisco Defense Orchestrator] の順に選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [有効（Enable）] をオンにします。

ステップ 4 変更内容を送信し、確定します。

ステップ 5 [Cisco Defense Orchestrator ポータル（Cisco Defense Orchestrator Portal）] をクリックします。ブラウザの設定に応じて、ポータルが新しいウィンドウまたはタブに開きます。

ステップ 6 Cisco Defense Orchestrator ポータルで、以下の手順を実行します。

a) Cisco Defense Orchestrator ポータルにログインします。

b) ポータルで Web セキュリティ アプライアンスをオンボードします。

c) 登録トークン（キー）をコピーします。

ステップ 7 Web セキュリティ アプライアンスで Cisco Defense Orchestrator 登録を完了します。次の操作を行ってください。

a) [Cisco Defense Orchestrator 登録（Cisco Defense Orchestrator Registration）] セクションに移動します。

b) 登録トークン（キー）を入力し、[登録（Register）] をクリックします。

c) 登録が正常に完了すると、成功メッセージが表示されます。

（注） このステップを実行すると、ポリシーを適用するために使用していたコンテンツ セキュリティ管理アプライアンスがポリシーの変更を Cisco Web セキュリティ アプライアンスに反映できなくなります。

Cisco Defense Orchestrator のレポート

Cisco Defense Orchestrator モードでアプライアンスを展開した後に、Cisco Defense Orchestrator にレポートを送信するようアプライアンスを設定できます。

Cisco Defense Orchestrator レポートを有効にするには、Cisco Defense Orchestrator のレポートを有効にする方法 （8 ページ）を参照してください。セキュリティ管理アプライアンスに関するレポート データを同様に表示および管理することはできません。

Cisco Defense Orchestrator のレポートを有効にする方法

始める前に

Cisco Defense Orchestrator モードでアプライアンスを展開します。この説明については、Cisco Defense Orchestrator モードでの展開 （2 ページ） を参照してください。

ステップ 1 [セキュリティサービス（Security Services）]>[レポート（Reporting）] を選択し、[設定を編集（Edit Settings）] を選択します。

ステップ 2 [ローカル レポート（Local Reporting）] を選択します。

ステップ 3 [Cisco Defense Orchestrator のレポート（Cisco Defense Orchestrator Reporting）] を選択します。

ステップ 4 変更を送信し、保存します。

（注） Cisco Defense Orchestrator のレポートを有効にすると、セキュリティ管理アプライアンスを使用した集中管理は無効になります。ただし、集中管理レポートには引き続き高度な Web セキュリティ レポート アプリケーションを使用することができます。

次のタスク

Cisco Defense Orchestrator でアプライアンスの要約レポートを表示します。https://docs.defenseorchestrator.com/を参照してください。

Cisco Defense Orchestrator モードの問題のトラブルシューティング

Cisco Defense Orchestrator を登録できない

アプライアンスで Cisco Defense Orchestrator モードを有効にした後、Cisco Defense Orchestrator を登録できない場合は、次の手順に従ってください。

ステップ 1 Cisco Defense Orchestrator ポータルから取得した登録キーが正しいことを確認します。

ステップ 2 Cisco Defense Orchestrator ポータルから取得した登録キーが有効であることを確認します。

登録キーの有効期限が切れている場合は、Cisco Defense Orchestrator で新しい登録キーを生成します。詳細については、https://docs.defenseorchestrator.comを参照してください。