デバイスとサービスの導入準備

ライブデバイスとモデルデバイスの両方を CDO に対して導入準備できます。モデルデバイスはアップロードされた構成ファイルであり、CDO を使用して閲覧および編集できます。

ほとんどのライブデバイスおよびサービスでは、Secure Device Connector が CDO をデバイスまたはサービスに接続できるように、オープンな HTTPS 接続が必要となります。

SDC とそのステータスの詳細については、Secure Device Connector（SDC） を参照してください。

この章は、次のセクションで構成されています。

ASA デバイスの導入準備

この手順を使用して、ASA モデルではなく単一のライブ ASA デバイスを CDO に導入準備します。複数の ASA を一度に導入準備する場合は、「一括での ASA の導入準備」を参照してください。

始める前に

デバイスの前提条件

- Cisco Defense Orchestrator の管理対象デバイスへの接続を確認してください。
- ASA の実行構成ファイルは 4.5 MB 未満である必要があります。実行構成ファイルのサイズを確認するには、「ASA 実行設定サイズの確認」を参照してください。
- IP アドレッシング：各 ASA、ASAv、または ASA セキュリティコンテキストには一意の IP アドレスが必要であり、SDC は管理トラフィックを受信するように設定されたインターフェイスでその IP アドレスに接続する必要があります。

証明書の前提条件

ASA デバイスに互換性のある証明書が存在しない場合、デバイスの導入準備が失敗する可能性があります。次の要件が満たされていることを確認します。

- デバイスで TLS バージョン 1.0 以降を使用している。
- デバイスにより提示される証明書が有効期限内であり、発効日が過去の日付である（すなわち、すでに有効になっており、後日に有効化されるようにスケジュールされていない）。
- 証明書は、SHA-256 証明書であること。SHA1 証明書は受け入れられません。
- 次のいずれかが該当すること。
  - デバイスは自己署名証明書を使用し、その証明書は認可されたユーザーにより信頼された最新の証明書と同じである。
  - デバイスは、信頼できる認証局（CA）が署名した証明書を使用し、提示されたリーフ証明書から関連 CA にリンクしている証明書チェーンを形成している。

導入準備プロセス中に証明書エラーが発生した場合は、詳細について証明書エラーのため ASA の導入準備ができないを参照してください。

オープン SSL 暗号の前提条件

互換性のある SSL 暗号スイートがデバイスにない場合、デバイスは Secure Device Connector（SDC）と正常に通信できません。次のいずれかの暗号スイートを使用します。

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256

- DHE-RSA-AES256-SHA256

ASA で使用する暗号スイートがこのリストにない場合、SDC はそれをサポートしていないため、ASA で暗号スイートを更新する必要があります。

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 青色のプラスボタン をクリックして、ASA を導入準備します。

ステップ 3 [ASA] タイルをクリックします。

ステップ 4 [デバイスの特定（Locate Device）] ステップで、次の手順を実行します。

1. [Secure Device Connector] ボタンをクリックし、ネットワークにインストールされている Secure Device Connector を選択します。SDC を使用しない場合、CDO は Cloud Connector を使用して ASA に接続できます。どちらを選択するかは、CDO を管理対象デバイスに接続する方法によって異なります。
2. デバイスに名前を付けます。
3. デバイスまたはサービスのロケーション（IP アドレス、FQDN、または URL）を入力します。デフォルトのポートは 443 です。
4. **[Next]** をクリックします。

ステップ 5 [ログイン情報（Credentials）] ステップで、CDO がデバイスへの接続に使用する、ASA 管理者または同様の最高特権の ASA ユーザーのユーザー名とパスワードを入力し、[次へ] をクリックします。

ステップ 6 （オプション）[完了（Done）] ステップで、デバイスのラベルを入力します。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。詳細については、ラベルとラベルグループに関するトピックを参照してください。

ステップ 7 デバイスまたはサービスにラベルを設定すると、[デバイスとサービス] リストに表示できます。

（注） 設定のサイズ、および他のデバイスまたはサービスの数によっては、設定の分析に時間がかかる場合があります

高可用性ペアの一部である ASA のオンボーディング

ハイアベイラビリティペアの一部である ASA を導入準備する場合は、ASA デバイスの導入準備 （1 ページ） を使用してペアのプライマリデバイスのみを導入準備します。

マルチコンテキストモードでの ASA の導入準備

マルチコンテキストモードについて

物理アプライアンスにインストールされている単一の ASA を、コンテキストと呼ばれる複数の論理デバイスに分割できます。マルチコンテキストモードで設定された ASA で使用される設定には、次の 3 種類があります。

- セキュリティコンテキスト
- 管理コンテキスト
- システム設定

セキュリティ コンテキストについて

各セキュリティコンテキストは、独自のセキュリティポリシー、インターフェイス、および管理者を持つ独立したデバイスとして機能します。複数のセキュリティコンテキストは、複数のスタンドアロンデバイスを持つことに似ています。セキュリティコンテキストは、プライベート クラウド インフラストラクチャにインストールされた仮想マシンイメージという意味での仮想 ASA ではありません。セキュリティコンテキストは、ハードウェアアプライアンスにインストールされた ASA で設定されます。各コンテキストは、そのアプライアンスの物理インターフェイスで設定されます。

マルチコンテキストモードの詳細については、ASA CLI および ASDM のコンフィギュレーション ガイド [英語] を参照してください。

CDO は、各セキュリティコンテキストを個別の ASA として導入準備し、個別の ASA であるかのように管理します。

管理コンテキストについて

管理コンテキストはセキュリティコンテキストと似ていますが、管理コンテキストにログインしたユーザーは、システム管理者権限を持つので、システムコンテキストや他のすべてのコンテキストにアクセスできる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザーに制限する必要があります。

CDO は、各管理コンテキストを個別の ASA として導入準備し、個別の ASA であるかのように管理します。CDO は、アプライアンスの ASA および ASDM ソフトウェアをアップグレードするときにも管理コンテキストを使用します。

システムの設定について

システム管理者は、各コンテキストコンフィギュレーションの場所、割り当てられたインターフェイス、およびその他のコンテキスト操作パラメータをシステム コンフィギュレーションに設定することで、コンテキストを追加および管理します。このコンフィギュレーションは、シ

ングルモードのコンフィギュレーション同様、スタートアップコンフィギュレーションです。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

CDO はシステム設定を導入準備しません。

セキュリティおよび管理コンテキストの導入準備の前提条件

セキュリティおよび管理コンテキストを導入準備するための前提条件は、他の ASA を導入準備する場合と同じです。前提条件のリストについては、ASA デバイスの導入準備 （1 ページ）を参照してください。

マルチコンテキストモードで ASA をサポートする Cisco アプライアンスについては、実行している ASA ソフトウェアバージョンの CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）[英語] の「Multiple Context Mode」の章を参照してください。

シングル コンテキスト ファイアウォールとして実行されている ASA、およびマルチコンテキスト ファイアウォールの管理コンテキストでは、ASDM および CDO アクセスにさまざまなポート番号を使用できます。ただし、セキュリティコンテキストの場合、ASDM および CDO アクセスポートはポート 443 に固定されています。これは ASA の制限です。

ASA セキュリティおよび管理コンテキストの導入準備

セキュリティコンテキストまたは管理コンテキストを導入準備する方法は、他の ASA を導入準備する場合と同じです。導入準備の手順については、ASA デバイスの導入準備 （1 ページ）または一括での ASA の導入準備 （5 ページ）を参照してください。

セキュリティコンテキストのアップグレード

CDO は、マルチコンテキスト ASA の各セキュリティおよび管理コンテキストを個別の ASA として扱い、個別に導入準備します。ただし、マルチコンテキスト ASA のすべてのセキュリティおよび管理コンテキストは、アプライアンスにインストールされている同じバージョンの ASA ソフトウェアを実行します。

ASA のセキュリティコンテキストで使用される ASA および ASDM のバージョンをアップグレードするには、管理コンテキストを導入準備し、そのコンテキストでアップグレードを実行します。詳細については、単一 ASA 上の ASA と ASDM イメージのアップグレード （14 ページ）またはASA および ASDM の一括アップグレード （11 ページ） ASA および ASDM の一括アップグレード （11 ページ）を参照してください。

一括での ASA の導入準備

Cisco Defense Orchestrator（CDO）を使用すると、.csv ファイルですべての ASA に必要な情報を提供することで、ASA を一括で導入準備できます。ASA が導入準備されているときに、フィ

ルタペインを使用して、キューに入っている、ロードされている、完了している、または失敗した導入準備の試行を表示できます。

始める前に

- Cisco Defense Orchestrator の管理対象デバイスへの接続を確認してください。
- 導入準備する ASA の接続情報を含む .csv ファイルを準備します。1 つの ASA に関する情報を独自の行に追加します。行の先頭に#を使用して、コメントを示すことができます。
  - ASA の場所（IP アドレスまたは FQDN）
  - ASA 管理者ユーザー名
  - ASA 管理者パスワード
  - （任意）CDO のデバイス名
  - SDCName フィールドで、CDO を ASA に接続するために使用するネットワーク内の Secure Device Connector（SDC）の名前を指定します。SDC を使用して ASA を CDO に接続しない場合は、「none」と入力することもできます。デバイスを導入準備するときに、SDCName フィールドに「none」と指定すると、Cloud Connector を使用して ASA が導入準備されます。Cloud Connector を使用すると、SDC をインストールせずにデバイスを CDO に接続できます。どちらを選択するかは、CDO を管理対象デバイスに接続する方法によって異なります。
  - （任意）CDO のデバイスラベル
  - ラベルを 1 つ追加するには、ラベル名を最後の CSV フィールドに追加します。
  - デバイスに複数のラベルを追加するには、値を引用符で囲みます。例：`alpha,beta,gamma`。
  - カテゴリと選択肢のラベルを追加するには、2 つの値をコロン（:）で区切ります。例：`Rack:50`。

構成ファイルの例：

```
#Location,Username,Password,DeviceName,SDCName,DeviceLabel
192.168.3.2,admin,CDO123!,ASA3,sdc1,"HA-1,Rack:50"
192.168.4.2,admin,CDO123!,ASA4,sdc1,"HA-1,Rack:50"
ASA2.example.com,admin,CDO123!,ASA2,none,Rack:51
asav.virtual.io,admin,CDO123!,ASA-virtual,sdc3,Test
```

注意 CDO は .csv ファイル内のデータを検証しないため、エントリの正確性を保証する必要があります。

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

ステップ 2 青色のプラスボタン  をクリックして、ASA を導入準備します。

ステップ 3 [導入準備（Onboarding）] ページで、[複数のASA（Multiple ASAs）] タイルをクリックします。

ステップ 4 [参照] をクリックして、ASA エントリを含む .csv ファイルを見つけます。指定したデバイスは、導入準備の準備ができている [ASA一括導入準備（ASA Bulk Onboarding）] テーブルのキューに入れられました。

注意 導入準備プロセスが完了するまで、[ASA一括導入準備（ASA Bulk Onboarding）] ページから移動しないでください。移動すると、導入準備プロセスが停止します。

ステップ 5 [開始（Start）] をクリックします。[ASA一括導入準備（ASA Bulk Onboarding）] テーブルのステータス列に、導入準備プロセスの進行状況が表示されます。デバイスが正常に導入準備されると、ステータスが [完了（Complete）] に変わります。

次のタスク

一括導入準備を一時停止し、後で再開する必要がある場合は、一括導入準備を一時停止、再開する （7 ページ）を参照してください。

.

一括導入準備を一時停止、再開する

導入準備プロセスを一時停止する必要がある場合は、[一時停止（Pause）] をクリックします。CDO は、導入準備を開始したデバイスの導入準備を終了します。一括導入準備プロセスを再開するには、[開始（Start）] をクリックします。CDO は、キューに入った次のデバイスの導入準備を開始します。

[一時停止（Pause）] をクリックしてこのページから移動した場合は、このページに戻って、最初から一括導入準備手順を最初から再度実行する必要があります。ただし、CDO は既に導入準備されたデバイスを認識し、このデバイスを新しい導入準備試行で「重複」としてマークし、リストをすばやく移動して、キューに入ったデバイスを導入準備します。

ASA モデルの作成とインポート

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 [デバイス] タブをクリックします。

ステップ 3 [ASA] タブをクリックします。

ステップ 4 ASA デバイスを選択し、左側のペインの [管理] で、[設定（Configuration）] をクリックします。

ステップ 5 [ダウンロード（Download）] をクリックしてデバイス設定をローカルコンピュータにダウンロードします。

ASA 設定のインポート

注意：導入準備する ASA 実行設定ファイルは 4.5 MB 未満である必要があります。導入準備する前に、設定ファイルのサイズを確認してください。

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、設定をインポートします。

ステップ 3 [オフライン管理用設定のインポート（Import configuration for offline management）] をクリックします。

ステップ 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 [参照] をクリックし、アップロードする設定ファイル（テキスト形式）を選択します。

ステップ 6 設定が確認されると、デバイスまたはサービスにラベルを設定するよう求められます。詳細については、『Labels and Label Groups』を参照してください。

ステップ 7 モデルデバイスにラベルを設定した後、[デバイスとサービス] リストで確認できます。

（注） 設定のサイズ、および他のデバイスまたはサービスの数によっては、設定の分析に時間がかかる場合があります

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。

オフライン管理用にデバイスの設定をインポートする

オフライン管理用にデバイスの設定をインポートすると、ネットワーク内の稼働中のデバイスを操作することなく、デバイスの設定を確認して最適化できます。CDO では、アップロードされたこれらの設定ファイルは「モデル」とも呼ばれます。

以下のデバイスの設定を CDO にインポートできます。

- 適応型セキュリティアプライアンス（ASA）。「ASA モデルの作成とインポート」を参照してください。
- Firepower Threat Defense（FTD）。
- Aggregation Services Routers（ASR）や Integrated Services Routers（ISR）などの Cisco IOS デバイス。

ASA と ASDM のアップグレードの前提条件

Cisco Defense Orchestrator（CDO）では、ASA および ASDM イメージのアップグレードに役立つウィザードが提供されます。個別の ASA、複数の ASA、アクティブ/スタンバイ構成の ASA、およびシングルコンテキストモードまたはマルチコンテキストモードで実行されている ASA にインストールされているイメージが対象です。

CDO は、アップグレード可能な ASA および ASDM イメージのリポジトリを保持します。CDO のイメージリポジトリからアップグレードイメージを選択すると、CDO は必要なすべてのアップグレード手順をバックグラウンドで実行します。このウィザードに従って、互換性のある ASA ソフトウェアおよび ASDM イメージを選択してインストールし、デバイスを再起動してアップグレードを完了するプロセスを実行できます。CDO で選択したイメージが ASA にコピーおよびインストールされているものであることを検証することにより、アップグレードプロセスを保護します。CDO は、定期的に ASA バイナリのインベントリを確認し、最新の ASA および ASDM イメージが利用可能になったときに、それらをリポジトリに追加します。これは、ASA にインターネットへのアウトバウンドアクセスがある場合に最適なオプションです。

CDO のイメージリポジトリには、一般的に利用可能な（GA）イメージのみが含まれています。リストに特定の GA イメージがない場合は、[サポートに連絡（Contact Support）] ページから Cisco TAC または電子メールサポートにお問い合わせください。確立されたサポートチケット SLA によってリクエストを処理し、リストにない GA イメージをアップロードします。

ASA にインターネットへのアウトバウンドアクセスがない場合は、必要な ASA イメージおよび ASDM イメージを Cisco.com からダウンロードして独自のリポジトリに保存し、アップグレードウィザードにそれらのイメージへのカスタム URL を入力できます。そうすると、CDO はそれらのイメージを使ってアップグレードを実行します。とはいえ、このケースでは、アップグレードするイメージを自分で決定することになります。CDO は、イメージの完全性チェックやディスク容量チェックを実施しません。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。

設定要件

- ASA で DNS を有効にする必要があります。
- CDO のイメージリポジトリからアップグレードイメージを使用する場合、ASA はインターネットにアクセスできる必要があります。
- ASA は CDO に正常に導入準備されている必要があります。
- ASA で CDO に同期している必要があります。

- ASA はオンラインになっている必要があります。
- カスタム URL アップグレードの場合：『Cisco ASA Upgrade Guide』を使用して、使用している ASA と互換性のある ASA および ASDM のバージョンを確認してください。
- カスタム URL アップグレードの場合：イメージリポジトリに ASA イメージおよび ASDM イメージをダウンロードしてください。
- カスタム URL アップグレードの場合：ASA がイメージリポジトリにアクセスできることを確認してください。
- カスタム URL アップグレードの場合：ASA および ASDM イメージ用に ASA に十分なディスク容量があることを確認してください。
- カスタム URL アップグレードの場合：URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。

1000 および 2000 シリーズの設定の前提条件

- 2000 シリーズ デバイスの FXOS モードは、**アプライアンス**モードに設定する必要があります。詳細については、「アプライアンスまたはプラットフォームモードへの Firepower 2100 の設定」を参照してください。
- デバイスは、ASA バージョン 9.13(1) **以降**を実行している必要があります。
- ASA ソフトウェアをアップグレードする前に、FXOS バンドルをアップグレードする必要があります。詳細については、「Firepower 2100 ASA and FXOS Compatibility」を参照してください。

ASA を実行中の 4100 および 9300 シリーズ

CDO は、4100 または 9300 シリーズ デバイスのアップグレードをサポートしていません。これらのデバイスは CDO の外部でアップグレードする必要があります。

アップグレードのガイドライン

- CDO は、アクティブ/スタンバイ「フェールオーバー」ペアとして設定された ASA をアップグレードできます。CDO は、アクティブ/アクティブ「クラスタ化」ペアで設定された ASA をアップグレードできません。

ソフトウェアおよびハードウェア要件

アップグレード可能な ASA および ASDM の最小バージョン：

- ASA：ASA 9.1.2
- ASDM：最小バージョンなし

サポート対象のハードウェアバージョン

- 「ASA ソフトウェアおよびハードウェアサポート」を参照してください。

ASA および ASDM の一括アップグレード

ステップ 1 ASA および ASDM イメージのアップグレードに関するアップグレード要件と重要な情報については、「ASA と ASDM のアップグレードの前提条件」を参照してください。

（注） ASA 1000 または 2000 シリーズデバイスをアップグレードする場合は、「ASA と ASDM のアップグレードの前提条件」を必ずお読みください。

ステップ 2 （任意）ナビゲーションバーで[デバイスとサービス]をクリックし、変更リクエストラベルを作成して、このアクションによってアップグレードされたデバイスを変更ログで識別します。

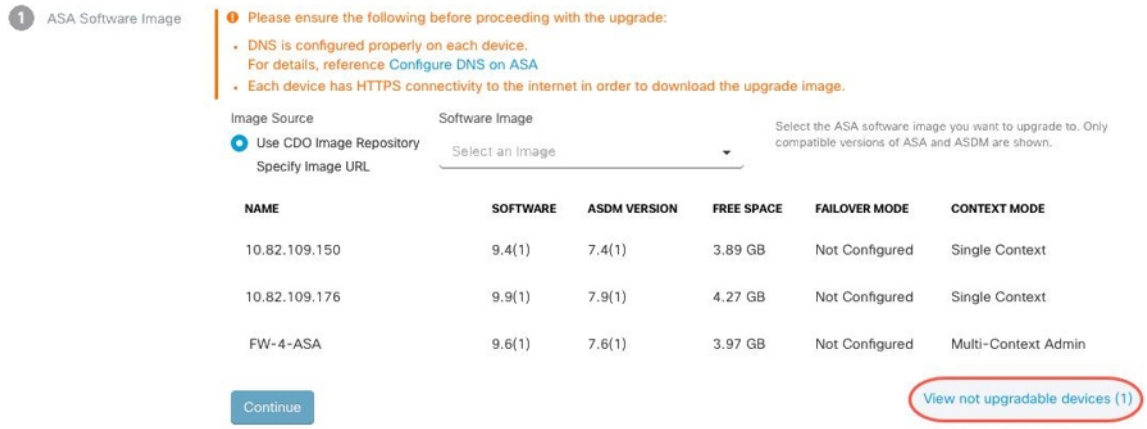
ステップ 3 [デバイス] タブをクリックします。

ステップ 4 フィルタを使用して、一括アップグレードに含めるデバイスのリストを絞り込みます。フィルタ

ステップ 5 フィルタ処理されたデバイスのリストから、アップグレードするデバイスを選択します。

ステップ 6 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 7 [デバイスの一括アップグレード（Bulk Device Upgrade）]ページに、アップグレード可能なデバイスが表示されます。選択したどのデバイスもアップグレードできない場合、CDO にはアップグレードできないデバイスのリンクが表示されます。



ステップ 8 ステップ 1 で、[CDOイメージリポジトリの使用（Use CDO Image Repository]）] をクリックしてアップグレードする ASA ソフトウェアイメージを選択し、[続行] をクリックします。

このリストは、選択したソフトウェアバージョンにアップグレードできる、選択したASAの数を示しています。次の例では、すべてのデバイスをバージョン9.9(1.2)にアップグレードでき、2つのデバイスを9.8(2)にアップグレードでき、1つのデバイスを9.6(1)にアップグレードできます。

選択したソフトウェアバージョンのいずれかが、選択したいずれのデバイスとも互換性がない場合、CDOは警告を表示します。次の例では、CDOは10.82.109.176デバイスを、すでに実行されているバージョンより前のバージョンにアップグレードできません。

NAME	SOFTWARE	ASDM VERSION	FREE SPACE	FAILOVER MODE	CONTEXT MODE
✔ 10.82.109.150	9.4(1)	7.4(1)	3.89 GB	Not Configured	Single Context
✔ FW-4-ASA	9.6(1)	7.6(1)	3.97 GB	Not Configured	Multi-Context Admin
✖ 10.82.109.176	9.9(1)	7.9(1)	4.27 GB	Not Configured	Single Context

ステップ 9 ステップ 2 で、アップグレードする ASDM イメージを選択します。アップグレード可能な ASA と互換性のある ASDM の選択肢のみが表示されます。

ステップ 10 ステップ3で、選択内容を確認し、ASAへのイメージのダウンロードのみを実行するか、あるいはイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 11 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。

（注） アップグレードが失敗すると、CDO からメッセージが表示されます。アップグレードの失敗は、多くの場合、ネットワークの問題によって ASA イメージと ASDM イメージの ASA への転送が阻害されることが原因です。

ステップ 12 後で CDO にアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）] チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 13 （マルチコンテキストモードの場合）管理コンテキストとセキュリティコンテキストが起動すると、セキュリティコンテキストに「新しい証明書が検出されました（New certificate detected）」というメッセージが表示されることがあります。このメッセージが表示された場合は、すべてのセキュリティコンテキストの証明書を受け入れます。アップグレードによって生じる他のすべての変更も受け入れます。

ステップ 14 [通知（notifications）] タブで一括アップグレードアクションの進行状況を確認します。[ジョブ（Jobs）] ページ一括アップグレードジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青色の [レビュー（Review）] リンクをクリックして [ジョブ] ページに移動します。[ジョブ（Jobs）] ページ

ステップ 15 変更リクエストラベルを作成してアクティブ化した場合は、他の設定変更を誤ってこのイベントに関連付けないように、忘れずにラベルをクリアしてください。

独自のリポジトリからのイメージを含む複数のASAのアップグレード

ステップ 1 ASA および ASDM イメージのアップグレードに関するアップグレード要件と重要な情報については、「ASA と ASDM のアップグレードの前提条件」を参照してください。

ステップ 2 （オプション）[デバイスとサービス] をクリックし、変更リクエストラベルを作成して、このアクションによってアップグレードされたデバイスを変更ログで識別します。

ステップ 3 [デバイス] タブをクリックします。

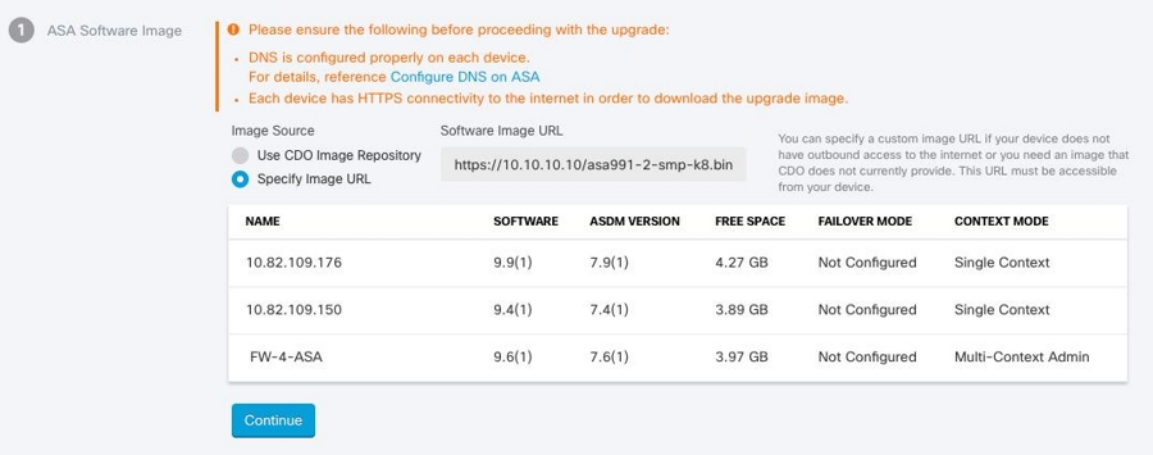
ステップ 4 フィルタ を使用して、一括アップグレードに含めるデバイスのリストを絞り込みます。

ステップ 5 フィルタ処理されたデバイスのリストから、アップグレードするデバイスを選択します。

ステップ 6 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 7 手順 1 で、[イメージURLの指定（Specify Image URL）] をクリックし、アップグレードする ASA イメージを [ソフトウェアイメージURL（Software Image URL）] フィールドで選択して、[続行] をクリックします。URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。

（注） 下の図は、[ソフトウェアイメージURL（Software Image URL）] フィールドに表示された HTTPS URL を示しています。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。



ステップ 8 手順 2 で、[イメージURLの指定（Specify Image URL）] をクリックし、アップグレードする ASDM イメージを [ソフトウェアイメージURL（Software Image URL）] フィールドで選択して、[続行] をクリックします。

ステップ 9 手順 3 で、選択内容を確認し、ASA へのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 10 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。

（注） アップグレードに失敗すると、CDO にメッセージが表示されます。アップグレードの失敗は、多くの場合、ネットワークの問題によって ASA イメージと ASDM イメージの ASA への転送が阻害されることが原因です。

ステップ 11 後で CDO にアップグレードを実行させる場合は、[アップグレードのスケジュール設定（Schedule Upgrade）] チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定（Schedule Upgrade）] ボタンをクリックします。

ステップ 12 （マルチコンテキストモードの場合）管理コンテキストとセキュリティコンテキストが起動すると、セキュリティコンテキストに「新しい証明書が検出されました（New certificate detected）」というメッセージが表示されることがあります。そのメッセージが表示された場合は、すべてのセキュリティコンテキストの証明書を受け入れます。アップグレードによって生じる他のすべての変更も受け入れます。

ステップ 13 通知タブで一括アップグレードアクションの進行状況を確認します。一括アップグレードジョブのアクションがどのように成功または失敗したかについての詳細な情報が必要な場合は、青い [確認] リンクをクリックして [ジョブ] ページに移動します。

ステップ 14 変更リクエストラベルを作成してアクティブ化した場合は、他の設定変更を誤ってこのイベントに関連付けないように、忘れずにラベルをクリアしてください。

次のタスク

アップグレードに関する注意事項

- [デバイスとサービス]ページを開き、テーブルの [設定ステータス（Configuration Status）] 列を表示して、アップグレードのバッチの進行状況を監視することもできます。
- [デバイスとサービス] ページでデバイスを選択し、[アップグレード] ボタンをクリックすると、一括アップグレードに含まれていた単一のデバイスでの進行状況を表示できます。CDOに、該当するデバイスの [デバイスのアップグレード] ページが表示されます。

単一 ASA 上の ASA と ASDM イメージのアップグレード

単一の ASA 上で ASA および ASDM イメージをアップグレードするには、次の手順に従います。

ステップ 1 ASAおよびASDMイメージのアップグレードに関するアップグレード要件と重要な情報については、「ASA と ASDM のアップグレードの前提条件」を参照してください。

（注） ASA 1000 または 2000 シリーズ デバイスをアップグレードする場合は、「ASA と ASDM のアップグレードの前提条件」を必ずお読みください。

ステップ 2 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 3 [デバイス] タブをクリックします。

ステップ 4 （オプション）変更リクエストラベルを作成して、このアクションによってアップグレードされたデバイスを変更ログで識別します。

ステップ 5 アップグレードするデバイスを選択します。

ステップ 6 [デバイスアクション（Device Actions）] ペインで、[アップグレード（Upgrade）] をクリックします。

ステップ 7 [デバイスのアップグレード] ページで、ウィザードに表示される指示に従います。

1. 手順 1 で、[CDOイメージリポジトリの使用（Use CDO Image Repository]）] をクリックしてアップグレードする ASA ソフトウェアイメージを選択し、[続行] をクリックします。

   （注） ASA および ASDM を独自のリポジトリに保存されたイメージにアップグレードする場合、[メージURLの指定] を選択して、[ソフトウェアイメージのURL] フィールドに ASA または ASDM イメージの URL を入力します。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。

   （オプション）後で CDO にアップグレードを実行させる場合は、[アップグレードのスケジュール設定]チェックボックスをオンにします。フィールドをクリックして、将来の日時を選択します。日時の選択が完了したら、[アップグレードのスケジュール設定]ボタンをクリックします。

2. 手順 2 で、アップグレードする ASDM イメージを選択します。アップグレード可能な ASA と互換性のある ASDM の選択肢のみが表示されます。

3. 手順 3 で、選択内容を確認し、ASA へのイメージのダウンロードのみを実行するか、それともイメージをコピーしてインストールしデバイスを再起動するかを決定します。

ステップ 8 準備ができたら、[アップグレードの実行（Perform Upgrade）] をクリックします。

ステップ 9 （マルチコンテキストモードの場合）管理コンテキストとセキュリティコンテキストが起動すると、セキュリティコンテキストに「新しい証明書が検出されました（New certificate detected）」というメッセージが表示されることがあります。このメッセージが表示された場合は、すべてのセキュリティコンテキストの証明書を受け入れます。アップグレードによって生じる他のすべての変更も受け入れます。デモを確認しますか？この手順のスクリーンキャストをご覧ください。

次のタスク

アップグレードに関する注意事項

- アップグレードするイメージを選択した後で気が変わった場合は、ソフトウェアイメージに関連付けられている [アップグレードをスキップ（Skip Upgrade）] チェックボックスをオンにします。イメージはデバイスにコピーされず、デバイスがイメージでアップグレードされることもありません。
- アップグレードの実行手順で、イメージをASAにコピーすることだけを選択した場合は、後で[デバイスのアップグレード]ページに戻り、[今すぐアップグレード（Upgrade Now）] をクリックしてアップグレードを実行できます。コピータスクが完了すると、[デバイスとサービス] ページにそのデバイスの「アップグレードの準備ができました」というメッセージが表示されます。
- イメージのコピー、インストール、デバイスの再起動のプロセス中は、デバイスでアクションを実行できません。イメージをインストールしてから再起動するデバイスは、[デバイスとサービス] ページで「アップグレード中」と表示されます。

- アップグレードプロセス中、つまりイメージのインストールおよびデバイスの再起動を行っている間は、デバイスでアクションを実行することはできません。
- イメージをデバイスにコピーすることのみを選択した場合、デバイス上でアクションを実行できます。イメージをコピーしているデバイスは、[デバイスとサービス] ページで [イメージをコピーしています] と表示されます。
- 自己署名証明書を持つデバイスをアップグレードすると、問題が発生する可能性があります。詳細については、「新しい証明書の検出」を参照してください。

アクティブ/スタンバイペアの ASA と ASDM イメージのアップグレード

アクティブ/スタンバイ フェールオーバー モードで ASA のペアをアップグレードする前に、以下の前提条件を確認してください。ASA の設定方法、およびフェールオーバーモードでの動作方法についての詳細については、ASA のマニュアルの「Failover for High Availability」を参照してください。

デモを確認する場合は、この手順のスクリーンキャストをご覧ください。

前提条件

- ASA および ASDM イメージのアップグレードに関する要件と重要な情報については、「ASA と ASDM のアップグレードの前提条件」を参照してください。
- プライマリ（アクティブ）およびセカンダリ（スタンバイ）の ASA は、アクティブ/スタンバイ フェールオーバー モードで設定されています。
- プライマリ ASA は、アクティブ/スタンバイペアのアクティブデバイスです。プライマリ ASA が非アクティブの場合、CDO はアップグレードを実行しません。
- プライマリとセカンダリの ASA ソフトウェアバージョンは同じです。

ワークフロー

これは、CDO が ASA のアクティブ/スタンバイペアをアップグレードするプロセスです。

ステップ 1 CDO は、ASA および ASDM イメージを両方の ASA にダウンロードします。

（注） ユーザーは、ASA および ASDM イメージのダウンロードを選択できますが、すぐにはアップグレードできません。ASA および ASDM イメージが以前にダウンロードされている場合、CDO はそれらのイメージを再度ダウンロードせず、次の手順でアップグレードワークフローを続行します。

ステップ 2 CDO は、最初にセカンダリ ASA をアップグレードします。

ステップ 3 アップグレードが完了し、セカンダリ ASA が [スタンバイ準備完了（Standby-Ready）] 状態に戻ると、CDO はフェールオーバーを開始し、セカンダリ ASA がアクティブ ASA になります。

ステップ 4 CDO は、現在のスタンバイ ASA であるプライマリ ASA をアップグレードします。

ステップ 5 プライマリ ASA が [スタンバイ準備完了（Standby-Ready）] 状態に戻ると、CDO はフェールオーバーを開始し、プライマリ ASA がアクティブ ASA になります。

警告 自己署名証明書を持つデバイスをアップグレードすると、問題が発生する可能性があります。詳細については、「新しい証明書の検出」を参照してください。

アクティブ/スタンバイペアの ASA と ASDM イメージのアップグレード

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] をクリックします。

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 アップグレードするデバイスを選択します。

ステップ 5 [デバイスアクション] ペインで、[アップグレード] をクリックします。

デバイスのフェールオーバー モードがアクティブ/スタンバイであることに注意してください。

ステップ 6 [デバイスのアップグレード] ページで、ウィザードに表示される指示に従います。

（注） ASA および ASDM を独自のリポジトリに保存されたイメージにアップグレードする場合、[メージURLの指定] を選択して、[ソフトウェアイメージのURL] フィールドに ASA または ASDM イメージの URL を入力します。FTP、TFTP、HTTP、HTTPS、SCP、および SMB のいずれかのプロトコルを使用して、リポジトリからイメージを取得できます。URL シンタックスの詳細については、「カスタム URL のアップグレード」を参照してください。

カスタム URL のアップグレード

ASA を新しい ASA ソフトウェアおよび ASDM イメージでアップグレードする場合、Cisco Defense Orchestrator（CDO）のイメージリポジトリに格納されているイメージを使用するか、ユーザー独自のイメージリポジトリに格納されているイメージを使用することができます。ASA にインターネットへのアウトバウンドアクセスがない場合、ユーザー独自のイメージリポジトリを維持することが、CDO を使用して ASA をアップグレードするための最良のオプションです。

CDO は ASA の copy コマンドを使用してイメージを取得し、それを ASA のフラッシュドライブ（disk0:/）にコピーします。[イメージURLの指定（Specify Image URL）] フィールドに、copy コマンドの URL 部分を指定します。たとえば、copy コマンド全体が次のようになっているとします。

```
ciscoasa# copy ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin disk:/0
```

この場合、[イメージURLの指定（Specify Image URL）] フィールドに

```
ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin
```

と入力します。

CDO は、アップグレードイメージを取得する http、https、ftp、tftp、smb、および scp の各方式をサポートします。

URL 構文の例

ASA copy コマンドの URL 構文の例を次に示します。これらの URL の例では、以下を想定しています。

- **イメージリポジトリのアドレス**：10.10.10.10
- **イメージリポジトリにアクセスするためのユーザー名**：admin
- **パスワード**：adminpass
- **パス**：images/asa
- **イメージファイル名**：asa991-smp-k8.bin

http[**s**]**://** [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename*]

```
https://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin
HTTP[s] example without a username and password:
https://10.10.10.10:8080/images/asa/asa991-smp-k8.bin
```

ftp:// [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename* [**;type=** *xx*]]
type は次のいずれかのキーワードになります。**ap**（ASCII パッシブモード）、**an**（ASCII通常モード）、**ip**（デフォルト：バイナリパッシブモード）、**in**（バイナリ通常モード）。

```
ftp://admin:adminpass@10.10.10.10:20/images/asa/asa991-smp-k8.bin
FTP example without a username and password:
ftp://10.10.10.10:20/images/asa/asa991-smp-k8.bin
```

tftp:// [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename* [**;int=** *interface_name*]]

```
tftp://admin:adminpass@10.10.10.10/images/asa/asa991-smp-k8.bin outside
TFTP example without a username and password:
tftp://10.10.10.10/images/asa/asa991-smp-k8.bin outside
```

（注） パス名にスペースを含めることはできません。パス名がスペースを含む場合は、**copy tftp** コマンドの代わりに **tftp-server** コマンドでパスを設定します。**;int=** *interface* オプションは、ルートルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバーに到達します。

smb:/[[*path* **/**] *filename*]：UNIX サーバーのローカルファイルシステムを示します。

```
smb:/images/asa/asa991-smp-k8.bin
```

scp:// [[*user* [**:** *password*] **@**] *server* [**/** *path*] **/** *filename* [**;int=** *interface_name*]]]：**;int=** *interface* オプションはルートルックアップをバイパスし、常に指定したインターフェイスを使用してセキュアコピー（SCP）サーバーに到達します。

```
 scp://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
SCP example without a username and password:
scp://10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
```

URL 構文を含む完全な copy コマンドについては、『Cisco ASA Series Command Reference, A - H Commands』ガイドを参照してください。

カスタム URL を使用した ASA および ASDM イメージのアップグレードの詳細については、「ASA と ASDM のアップグレードの前提条件」を参照してください。