設定の展開

この章では、1 つ以上の管理対象デバイスに設定の変更をダウンロードする方法について説明します。

設定の展開について

すべてのデバイス設定は Management Center によって管理され、管理対象デバイスに展開されます。

展開が必要な設定変更

システムは、失効したポリシーに赤色のステータステキストでマークを付けます。このテキストには、ポリシーの更新を必要とするターゲットデバイスの数が示されます。失効ステータスをクリアするには、ポリシーをデバイスに再展開する必要があります。

展開が必要

展開が必要な設定変更には、次のものがあります。

- アクセス コントロール ポリシー自体の変更：アクセス コントロール ルール、デフォルト アクション、ポリシー ターゲット、セキュリティ インテリジェンス フィルタリング、前処理などの詳細オプションの変更。
- アクセス コントロール ポリシーが呼び出すポリシーの変更：SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイル ポリシー、アイデンティティ ポリシー、または DNS ポリシー。

- 呼び出されるアクセス コントロール ポリシーで使用される再利用可能オブジェクトまたは設定の変更：
  - ネットワーク、ポート、VLAN タグ、URL、地理位置情報オブジェクト
  - セキュリティ インテリジェンス リストおよびフィード
  - アプリケーション フィルタまたはディテクタ
  - 侵入ポリシーの変数セット
  - ファイル リスト
  - 復号関連のオブジェクトとセキュリティ ゾーン
- システム ソフトウェア、侵入ルール、または脆弱性データベース（VDB）の更新。

Webインターフェイスの複数の場所からこれらの設定の一部を変更できることに留意してください。たとえば、オブジェクトマネージャ（**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**）を使用してセキュリティゾーンを変更できますが、デバイスの設定（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**）でインターフェイスのタイプを変更すると、ゾーンも変更され、展開が必要になります。

展開が不要

次の更新では、展開は**必要ありません**。

- セキュリティ インテリジェンス フィードへの自動更新およびコンテキストメニューを使用したセキュリティインテリジェンスのグローバルのブロックリストまたはブロックしないリストへの追加
- URL フィルタリング データへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

展開のプレビュー

[プレビュー（Preview）]には、デバイス上に展開するポリシーとオブジェクトのすべての変更のスナップショットが表示されます。ポリシーの変更には、新しいポリシー、既存のポリシーの変更、および削除されたポリシーが含まれます。オブジェクトの変更には、ポリシーで使用される追加および変更されたオブジェクトが含まれます。未使用のオブジェクトの変更は、デバイスに展開されていないため表示されません。

デバイスへの展開が保留されている変更の設定変更ログを表示するには、展開ジョブの横にある [プレビュー（Preview）] アイコンをクリックします。変更ログには、次のものが含まれます。

- **比較ビュー**：最後の展開以降に加えられたすべてのデバイス設定変更の対照比較を表示します。
- **詳細ビュー**：デバイスに適用される保留中の CLI コマンドを表示します。

展開プレビューの表示の詳細については、設定変更の展開（18ページ）を参照してください。

プレビューには、インターフェイスまたはプラットフォーム設定ポリシーが初めて追加されたときに、変更されていない場合でも、他の設定済みの設定とともに、すべてのデフォルト値が表示されます。同様に、高可用性関連のポリシーと設定のデフォルト値は、高可用性ペアが設定または中断した後の最初のプレビューで、変更されていない場合でも表示されます。

自動ロールバックによる変更を表示するには、展開設定の編集を参照してください。

サポートされない機能

- オブジェクトがデバイスまたはインターフェイスに関連付けられている場合にのみ、オブジェクトの追加と属性の変更がプレビューに表示されます。オブジェクトの削除は表示されません。
- プレビューは、次のポリシーではサポートされていません。
  - ハイ アベイラビリティ
  - ネットワーク検出
  - ネットワーク分析
  - デバイス設定
- ルールレベルのユーザー情報は、侵入ポリシーでは利用できません。
- プレビューには、ポリシー間のルールの順序変更は表示されません。

  DNSポリシーの場合、順序が変更されたルールは、ルールの追加および削除のようにプレビューリストに表示されます。たとえば、ルールの順序でルールを位置1から位置3に移動すると、そのルールが位置1から削除されて新しいルールとして位置3に追加されたように表示されます。同様に、ルールを削除すると、その下のルールは位置が変更されるため、編集済みのルールとして表示されます。変更は、ポリシーに示される最終順序で表示されます。
- プレビューは、次のHAシナリオではサポートされていません。
  - デバイスがスタンドアロンモードになっていてチェーンが作成された場合、自動展開がトリガーされます。その特定のジョブでは、プレビューはサポートされません。**[プレビュー（Preview）]**（）にカーソルを合わせると、HAブートストラップ展開であり、プレビューはサポートされないことを示すメッセージが表示されます。
  - **設定グループ**：デバイスが最初はスタンドアロンであったフローについて検討します。その後、3つの展開が行われました。4つ目の展開では、デバイスはHAブートストラップ展開でした。その後、ユーザーはデバイス5、6、および7を展開します。展開7はHA解除展開であり、ユーザーはデバイス8、9、および10を展開します。

    このフローでは、4がHA展開だったため、3と5の間のプレビューはサポートされません。同様に、8と3の間のプレビューもサポートされません。プレビューは、3から1と、7、6、5、4と、10、9、8でのみサポートされます。

- デバイスが切断されている（HA が解除されている）場合、新しいデバイスは新規デバイスと見なされます。

選択的ポリシーの展開

Management Center では、展開が予定されているデバイス上の変更すべてのリスト内で特定のポリシーを選択し、選択したポリシーのみを展開することができます。選択的な展開は、次のポリシーに対してのみ使用できます。

- アクセス コントロール ポリシー
- 侵入ポリシー
- マルウェアおよびファイル ポリシー
- DNS ポリシー
- アイデンティティ ポリシー
- SSL ポリシー
- QoS ポリシー
- プレフィルタ ポリシー
- ネットワーク検出
- NAT ポリシー
- ルーティングポリシー
- VPN ポリシー

ポリシーを選択的に展開するには、特定の制限があります。次の表の内容に従って、選択的ポリシー導入を使用できる場合について理解します。

表 *1 :* 選択的展開の制限事項

タイプ	説明	シナリオ
フル展開	特定の展開シナリオではフル展開が必要であり、Management Center はこのようなシナリオでの選択的展開をサポートしていません。このようなシナリオでエラーが発生した場合、デバイス上の展開へのすべての変更を選択して続行することもできます。	フル展開が必要なシナリオは次のとおりです。 • Threat Defense または Management Center をアップグレードした後の最初の展開。 • Threat Defense を復元した後の最初の展開。 • Threat Defense インターフェイスの設定を変更した後の最初の展開。 • 仮想ルータの設定を変更した後の最初の展開。 • Threat Defense デバイスが新しいドメインに移動された場合（グローバルからサブドメインへ、またはサブドメインからグローバルへ）。
関連付けられたポリシーの展開	Management Center は、相互に関連する相互依存ポリシーを特定します。相互に関連するポリシーのいずれかを選択すると、残りの相互に関連するポリシーが自動的に選択されます。	関連付けられたポリシーが自動的に選択されるシナリオは次のとおりです。 • 新しいオブジェクトが既存のポリシーに関連付けられている場合。 • 既存のポリシーのオブジェクトが変更された場合。 複数のポリシーが自動的に選択されるシナリオは次のとおりです。 • 新しいオブジェクトが既存のポリシーに関連付けられていて、同じオブジェクトがすでに他のポリシーに関連付けられている場合、関連付けられているすべてのポリシーが自動的に選択されます。 • 共有オブジェクトが変更されると、関連付けられているすべてのポリシーが自動的に選択されます。

タイプ	説明	シナリオ
相互依存ポリシーの変更（色分けされたタグを使用して表示）	Management Center は、ポリシー間および共有オブジェクトとポリシー間の依存関係を動的に検出します。オブジェクトまたはポリシーの相互依存性は、色分けされたタグを使用して表示されます。	色分けされた相互依存ポリシーまたはオブジェクトが自動的に選択されるシナリオは次のとおりです。 • すべての期限切れのポリシーに相互に依存する変更がある場合。 たとえば、アクセス コントロール ポリシー、侵入ポリシー、および NAT ポリシーが失効している場合などです。アクセス コントロール ポリシーと NAT ポリシーはオブジェクトを共有するため、すべてのポリシーが展開用に一緒に選択されます。 • すべての期限切れのポリシーがオブジェクトを共有し、そのオブジェクトが変更された場合。

タイプ	説明	シナリオ
アクセスポリシーグループの仕様	[ポリシーの表示または非表示（Show or Hide Policy）]（  ）をクリックすると、アクセスポリシーグループのポリシーが、[アクセスポリシーグループ（Access Policy Group）] の下のプレビューウィンドウにまとめて表示されます。	アクセスポリシーグループのポリシーのシナリオと想定される動作は次のとおりです。 • アクセス コントロール ポリシーが失効している場合、そのアクセス コントロール ポリシーが展開用に選択されると、ファイルポリシーと侵入ポリシーを除き、このグループにあるすべての期限切れポリシーが展開されます。 ただし、アクセス コントロール ポリシーが失効している場合でも、依存関係に変更がない限り、アクセス コントロール ポリシーが選択されているかどうかに関係なく、侵入ポリシーとファイルポリシーを個別に選択または選択解除できます。たとえば、新しい侵入ポリシーがアクセス コントロール ルールに割り当てられると、依存関係に変化が生じることになります。その結果、アクセス コントロール ポリシーと侵入ポリシーのいずれかが選択されると、その両方が自動的に選択されます。 • アクセス コントロール ポリシーが失効していない場合は、このグループ内の他の古いポリシーを個別に選択して展開することができます。

システムユーザー名

Management Center では、次の動作に関してユーザー名が「**system**」と表示されます。

- ロールバック（Rollback）
- アップグレード
- Threat Defense バックアップおよび復元
- SRU の更新
- LSP の更新
- VDB の更新

アプリケーションディテクタの自動有効化

アプリケーション制御の実行時に必要なディテクタが無効になっている場合、システムは、ポリシーの展開時にシステムによって提供される適切なディテクタを自動的に有効にします。存在しない場合、システムはそのアプリケーション対応で最近変更されたユーザ定義のディテクタを有効にします。

ネットワーク検出ポリシーの変更によるアセットの再検出

ネットワーク検出ポリシーに変更を展開する場合、システムは、監視対象ネットワーク内のホストのネットワーク マップから MAC アドレス、TTL、およびホップ情報を削除してから、再検出を行います。また、影響を受ける管理対象デバイスは、まだ Management Center に送信されていない検出データを破棄します。

Snort 再起動のシナリオ

管理対象デバイス上の Snort プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作 （11 ページ）を参照してください。 また、Snort プロセスが再起動するかどうかに関係なく、展開時にリソース需要が高まった結果、いくつかのパケットがインスペクションを実行せずにドロップされることがあります。

次の表に示すいずれかのシナリオでは、Snort プロセスが再起動されます。

表 *2: Snort* 再起動のシナリオ

再起動のシナリオ	詳細情報
Snort プロセスの再起動が必要な特定の設定を展開した場合。	展開またはアクティブ化された際に Snort プロセスを再起動する設定 （13 ページ）
Snort プロセスを直ちに再起動するように設定を変更した場合。	変更により Snort プロセスがただちに再起動する場合 （15 ページ）
現在展開されている自動アプリケーション バイパス（AAB）設定のトラフィックをアクティブにした場合。	自動アプリケーションバイパスの設定
「RAM ディスクへの接続イベントのロギング」機能の有効化または無効化。	『Troubleshoot Drain of FMC Unprocessed Events』の「**Log to Ramdisk**」を参照してください。

関連トピック

アクセス コントロール ポリシーの詳細設定

展開またはアクティブ化された際に Snort プロセスを再起動する設定 （13 ページ）

デバイスの再起動の警告

展開時、展開ページの [検査の中断（Inspect Interruption）] 列に、構成を展開したときに Threat Defense デバイスで Snort プロセスが再起動するかどうかが表示されます。Snort プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。トラフィックが中断されるか中断中にインスペクションなしで受け渡されるかどうかは、デバイスがトラフィックを処理する方法によって変わります。展開の続行、展開のキャンセル、および設定の変更を実行できます。または、展開によるネットワークへの影響が最小となる時間まで展開を遅らせることができます。

[インスペクションの中断（Inspect Interruption）] 列に [あり（Yes）] と表示されているときにデバイス設定リストを展開すると、Snortプロセスを再起動する特定の設定タイプが [検査の中断（Inspect Interruption）]（） と共に表示されます。このアイコンにマウスポインタを合わせると、設定を展開するときにトラフィックが中断される可能性があるというメッセージが表示されます。

次の表に、インスペクション中断の警告を[展開（Deploy）] ページに表示する方法を示します。

表 *3:* インスペクション中断のインジケータ

タイプ	インスペクションの中断	説明
Threat Defense	[検査の中断（Inspect Interruption）]（）はい（Yes）	少なくとも1つの設定は、展開するとデバイスでインスペクションが中断します。また、デバイスがトラフィックを処理する方法によって、トラフィックが中断されることがあります。デバイス設定リストを展開して、詳細を確認できます。
	--	展開されている設定は、デバイスのトラフィックを中断しません。
	不明	システムは、展開されている設定がデバイスのトラフィックを中断するかどうか特定できません。 最初の展開の前の、ソフトウェア アップグレードの後に、または場合によってはサポート コール中に、不明ステータスが表示されます。
	[エラー（Error）]（）	内部エラーにより、システムはステータスを特定できません。 操作をキャンセルして再度 [展開（Deploy）] をクリックすると、システムは [インスペクションの中断（Inspect Interruption）] ステータスを特定しなおすことができます。問題が解決しない場合は、サポートにご連絡ください。
センサー	--	センサーとして識別されるデバイスは Threat Defense デバイスではありません。システムは、構成を展開するとこのデバイスのトラフィックが中断されるかどうかを特定しません。

すべてのデバイスタイプの Snort プロセスを再起動する全設定の詳細については、展開またはアクティブ化された際にSnortプロセスを再起動する設定（13ページ）を参照してください。

ポリシー適用中のトラフィックの検査

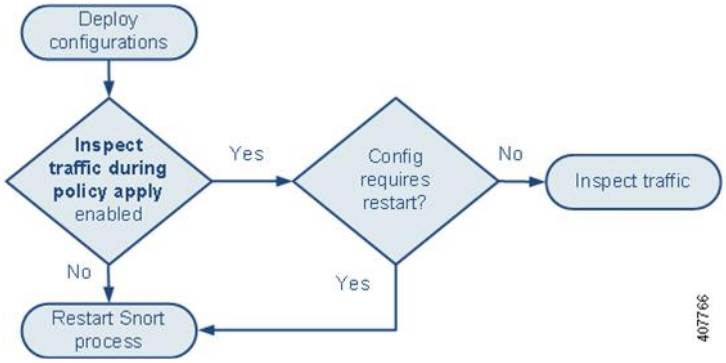
[ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] は、管理対象デバイスが設定変更の展開時にトラフィックを検査できるようにするための詳細アクセス コントロール ポリシーの一般設定です。これは、展開する設定で Snort プロセスの再起動が不要な場合に限ります。このオプションは、次のように設定できます。

- [有効（Enabled）]：特定の設定で Snort 処理を再起動する必要な場合を除き、トラフィックは展開時に検査されます。

  展開する設定に Snort の再起動が必要でなければ、システムは現在展開されているアクセス コントロール ポリシーを使用してトラフィックを検査し、導入中に、展開しているアクセス コントロール ポリシーに切り替えます。

- [無効（Disabled）]：展開時にトラフィックは検査されません。Snort プロセスは展開時に必ず再起動されます。

次の図に、[ポリシー適用時にトラフィックを検査（Inspect traffic during policy apply）] を有効にした場合と無効にした場合の Snort の再起動の仕組みを示します。



注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。Snort の再起動によるトラフィックの動作 （11 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（13 ページ）を参照してください。

Snort の再起動によるトラフィックの動作

次の表に、Snort プロセスが再起動した場合のさまざまなデバイスのトラフィックの処理方法を示します。

表 *4 : Threat Defense* および *Threat Defense Virtual* の再起動によるトラフィックの動作

インターフェイスの設定	再起動によるトラフィックの動作
inline: **Snort Fail Open: Down**: disabled	ドロップされる

インターフェイスの設定	再起動によるトラフィックの動作
inline: **Snort Fail Open: Down**: enabled	検査なしで受け渡される Snort がダウンしていることをシステムが認識するまでに、一部のパケットがバッファ内で数秒間遅延することがあります。この遅延は、負荷分散によって異なります。ただし、バッファされたパケットは最終的に渡されます。
ルーテッド、トランスペアレント（EtherChannel、冗長、サブインターフェイスを含む）：**preserve-connection** は enabled（**configure snort preserve-connection enable**、デフォルト） 詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。	既存の TCP/UDP フロー：Snort がダウンしている間、1 つでもパケットが着信すると、検査なしで渡されます。 新規 TCP/UDP フローとすべての非 TCP/UDP フロー：ドロップされる **preserve-connection** が有効になっている場合でも、次のトラフィックはドロップされることに注意してください。 • プレーンテキスト、パススルー プレフィルタ トンネル トラフィック (**Analyze** ルール アクションまたは**Analyze all tunnel traffic** デフォルト ポリシー アクションと一致) • アクセスコントロールルールと一致せず、デフォルトアクションによって代わりに処理される接続。 • 復号された TLS/SSL トラフィック • セーフ サーチ フロー • キャプティブ ポータル フロー
ルーテッド、トランスペアレント（EtherChannel、冗長、サブインターフェイスを含む）：**preserve-connection** は disabled（**configure snort preserve-connection disable**）	ドロップされる
inline: tap mode	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし

（注） Snort が再起動中に Snort プロセスがダウンした場合のトラフィックの処理に加え、Snort プロセスがビジーの場合、[Snort フェールオープン（Snort Fail Open）] の [ビジー（Busy）] オプション（インラインセットを設定します。を参照）の設定によってはトラフィックが検査なしで転送されたり、ドロップされたりすることがあります。デバイスは、フェールセーフ オプションまたは Snort フェールオープン オプションの両方ではなくいずれかをサポートします。

（注） 設定の導入時に Snort プロセスがビジーになったが、ダウンしなかった場合、CPU の合計負荷が 60 % を超えると一部のパケットがルーテッド、スイッチド、またはトランスペアレント インターフェイスでドロップする場合があります。

警告 Snort ルールの更新中は、システムを再起動しないでください。

Snort が十分な速度でパケットを処理できない場合、Snort ビジードロップが発生します。処理の遅延が原因で Snort がビジー状態にあるかどうか、またはコールブロッキングが原因でスタックしているかどうかは、Lina で認識されません。伝送キューがいっぱいになると、Snort ビジードロップが発生します。送信キューの使用率に基づいて、Lina はキューがスムーズに処理されている場合にアクセスを試みます。

展開またはアクティブ化された際に Snort プロセスを再起動する設定

AAB 以外の構成を展開すると、Snort プロセスが再起動されます。AAB の展開自体には再起動が伴いませんが、パケットの遅延が大きすぎると、現在展開されている AAB 設定がアクティブになり、Snort プロセスが部分的に再起動されます。

アクセス コントロール ポリシーの詳細設定

- [ポリシー適用時にトラフィックのインスペクションを実行する（Inspect traffic during policy apply）] が無効な場合に展開します。
- SSL ポリシーを追加または削除します。

ファイルポリシー（File Policy）

次のいずれかの構成の最初または最後を展開します。これらのファイルポリシー構成を展開しても再起動は発生しませんが、非ファイルポリシー構成を展開すると再起動が発生する可能性があることに注意してください。

- 次のいずれかの操作を行います。
  - 展開されたアクセス コントロール ポリシーに 1 つ以上のファイル ポリシーが含まれている場合は、[アーカイブを検査する（Inspect Archives）] を有効または無効にします。

- [アーカイブを検査する（Inspect Archives）] が有効になっている場合は、最初のファイルポリシールールを追加するか、または最後のファイルポリシールールを削除します（[アーカイブを検査する（Inspect Archives）] が有意味であるためには 1 つ以上のルールが必要であることに注意してください）。

- [ファイルを検出（Detect Files）] または [ファイルをブロック（Block Files）] ルールで、[ストア ファイル（Store files）] を有効または無効にします。
- [マルウェアクラウドのルックアップ（Malware Cloud Lookup）] または [マルウェアをブロック（Block Malware）] ルールアクションと、分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[ダイナミック分析（Dynamic Analysis）] または [ローカル マルウェア分析（Local Malware Analysis）]）またはストアファイルオプション（[マルウェア（Malware）]、[不明（Unknown）]、[クリーン（Clean）] または [カスタム（Custom）]）を組み合わせた最初のアクティブファイルルールを追加するか、または最後のアクティブ ファイル ルールを削除します。

これらのファイルポリシー構成をセキュリティゾーンまたはトンネルゾーンに展開するアクセス コントロール ルールによって再起動が発生するのは、構成が次の条件を満たす場合だけであることに注意してください。

- アクセス コントロール ルールに含まれる送信元または宛先セキュリティゾーンは、ターゲットデバイス上のインターフェイスに関連付けられたセキュリティゾーンと一致する必要があります。
- アクセス コントロール ルールに含まれる宛先ゾーンが [任意（any）] でないかぎり、ルールに含まれる送信元トンネルゾーンは、プレフィルタポリシーに含まれるトンネルルールに割り当てられているトンネルゾーンと一致する必要があります。

ID ポリシー

- SSL 復号が無効になっている場合（つまり、アクセス コントロール ポリシーに SSL ポリシーが含まれていない場合）は、最初のアクティブ認証ルールを追加するか、または最後のルールを削除します。

  アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルールアクションが含まれるか、[パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルールアクションが含まれます。

ネットワーク検出（Network Discovery）

- ネットワーク検出ポリシーを使用して、HTTP、FTP、または MDNS プロトコル経由で権限のないトラフィックベースのユーザ検出を有効または無効にします。

デバイス管理

- MTU：デバイス上のすべての非管理インターフェイスの中で最大の MTU 値を変更します。
- 自動アプリケーションバイパス（AAB）：現在展開されている AAB 構成は、Snort プロセスの誤動作またはデバイスの誤設定により、単一のパケットが過度の処理時間を使用した場合にアクティブになります。その結果、Snort プロセスが部分的に再起動され、非常に大きい遅延が緩和されるか、または完全なトラフィックの停止が防止されます。この部分的な再起動により、デバイスがトラフィックをどのように処理するかに応じて、いくつかのパケットがインスペクションなしで通過するか、またはドロップされます。

変更点

- システムアップデート：新しいバージョンの Snort バイナリまたはデータ収集ライブラリ（DAQ）を含むソフトウェアアップデートの後に初めて構成を展開します。
- VDB：Snort 2 を実行している管理対象デバイスでは、管理対象デバイスに適用可能な変更を含む、脆弱性データベース（VDB）更新のインストール後に初めて構成を展開すると、検出エンジンの再起動が必要になるため、一時的にトラフィックが中断する可能性があります。そのため、インストールを開始するために Management Center を選択すると、警告メッセージが表示されます。展開ダイアログは、VDB 変更が保留中の場合、Threat Defense デバイスに関する追加の警告を表示します。Management Center にのみ適用される VDB の更新では検出エンジンの再起動が行われないため、更新を展開できません。

  Snort 3 を実行している管理対象デバイスでは、脆弱性データベース（VDB）更新のインストール後に初めて構成を展開すると、一時的にアプリケーションの検出が中断する可能性がありますが、トラフィックは中断しません。

関連トピック

設定変更の展開 （18 ページ）
Snort 再起動のシナリオ （8 ページ）

変更により Snort プロセスがただちに再起動する場合

以下の変更を行うと、展開プロセスを経ることなく Snort プロセスが直ちに再起動されます。再起動がトラフィックにどのような影響を与えるかは、ターゲットデバイスがトラフィックを処理する方法によって異なります。詳細はSnort の再起動によるトラフィックの動作 （11 ページ）を参照してください。

- アプリケーションまたはアプリケーションディテクタに関する次の操作のいずれかを実行します。
  - システムまたはカスタム アプリケーション ディテクタを有効または無効にします。
  - アクティブ化されたカスタム ディテクタを削除します。
  - アクティブ化されたカスタム ディテクタを**保存して再アクティブ化**します。
  - ユーザ定義のアプリケーションを作成します。

この操作を続けると管理対象のすべてのデバイスで Snort プロセスが再起動するという警告メッセージが表示され、キャンセルが可能になります。再起動は、現在のドメインまたはその子ドメインのいずれかの管理対象デバイスで発生します。

- Threat Defense ハイアベイラビリティペアを作成または解除します。

  ハイアベイラビリティペアの作成を続行すると、プライマリデバイスとセカンダリデバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

ポリシー管理の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- ネットワーク管理者
- セキュリティ承認者

設定変更を展開するためのベストプラクティス

次に、設定変更の展開に関するガイドラインを示します。

信頼性の高い管理接続

Management Center とデバイスの間の管理接続は、それ自身とデバイスの間の安全な TLS-1.3 暗号化通信チャネルです。

セキュリティ上の理由から、サイト間 VPN などの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPN がダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

注意 デバイスの管理接続は、デバイス自体で終端する VPN トンネルを経由させないことをお勧めします。VPNがダウンする原因となる設定変更を展開すると、管理接続が切断され、デバイスに直接接続しないと設定を回復できなくなります。

管理トラフィックが VPN 終端インターフェイスから出る場合は、必ず、VPN トンネルから管理トラフィックを除外してください。

同時展開の最大数

同じジョブで Management Center に許可される最大デバイス数の 25% を超えるデバイスに展開しないでください。たとえば、FMCv300 の場合、最大ジョブサイズは 75 デバイス（300 の 25%）です。これより多いデバイスに同時に展開すると、パフォーマンスの問題が発生する可能性があります。

共有ポリシーの展開

最大限のパフォーマンスを実現するには、同じポリシーを使用するデバイスに展開します。ポリシーを共有するデバイスのグループごとに個別の展開ジョブを作成してください。

展開時間とメモリの制限

展開に要する時間は、次のような複数の要因によって異なります（ただし、これに限られません）。

- デバイスに送信する設定。たとえば、ブロックするセキュリティ インテリジェンス エントリの数を大幅に増やすと、展開にかかる時間が長くなることがあります。
- デバイスのモデルとメモリ。低メモリ デバイスでは、展開にかかる時間が長くなることがあります。

デバイスの機能を超えないように注意してください。ターゲットデバイスでサポートされるルールまたはポリシーの最大数を超えると、システムが警告を表示します。最大数は多くの要因に依存し、メモリとデバイス上のプロセッサ数だけでなく、ポリシーとルールの複雑さにも依存します。ポリシーとルールの最適化の詳細については、アクセス制御ルールのベストプラクティスを参照してください。

メンテナンスウィンドウの使用によるトラフィック中断の影響の軽減

メンテナンスウィンドウまたは中断の影響が最小限になる時間に展開することを強くお勧めします。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snort の再起動によるトラフィックの動

作 （11 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定（13 ページ）を参照してください。

Threat Defense デバイスの場合、[展開（Deploy）] ダイアログの [検査の中断（Inspect Interruption）] 列に、展開するとトラフィックフローまたは検査が中断する可能性があることについて警告が表示されます。展開を続行、キャンセル、または延期できます。詳細については、デバイスの再起動の警告 （9 ページ）を参照してください。

関連トピック

Snort 再起動のシナリオ （8 ページ）

設定の展開

導入を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を導入する必要があります。導入のステータスは、メッセージ センターで確認できます。

導入を行うと、以下のコンポーネントが更新されます。

- デバイスとインターフェイスの設定
- デバイス関連ポリシー：NAT、VPN、QoS、プラットフォーム設定
- アクセス コントロールおよび関連するポリシー：DNS、ファイル、アイデンティティ、侵入、ネットワーク分析、プレフィルタ、SSL
- ネットワーク検出ポリシー
- 侵入ルールの更新
- これらの要素のいずれかに関連付けられている設定とオブジェクト

システムにポリシーを自動的に導入させるには、導入タスクをスケジュールするか、あるいは侵入ルールの更新をインポートする際に導入するようにシステムを設定します。特に、侵入ポリシーの更新によって侵入およびネットワーク分析に関するシステム定義の基本ポリシーを変更できるようにしている場合は、ポリシーの導入を自動化すると役立ちます。侵入ルール更新によって、アクセス コントロール ポリシーの前処理およびパフォーマンスの詳細設定オプションのデフォルト値が変更されることもあります。

設定変更の展開

設定を変更した後に、影響を受けるデバイスに展開します。メンテナンスの時間帯か、またはトラフィックフローとインスペクションに対する中断の影響が最小限になる時間に展開することを強くお勧めします。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断するSnortプロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snortの再起動によるトラフィックの動作 （11ページ）および展開またはアクティブ化された際にSnortプロセスを再起動する設定（13ページ）を参照してください。

始める前に

- すべての管理対象デバイスが同じバージョンのセキュリティ ゾーン オブジェクトを使用していることを確認してください。セキュリティ ゾーン オブジェクトを編集した場合：同期させるすべてのデバイスでインターフェイスのゾーン設定を編集するまでは、デバイスに設定変更を展開しないでください。すべての管理対象デバイスに同時に展開する必要があります。
- 展開の変更をプレビューするには、REST APIアクセスを有効にします。REST APIアクセスを有効にするには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Enabling REST API Access*」 の手順に従います。

（注） 展開時にデバイスCLIでデバイス設定が読み取られている場合、その展開プロセスは失敗します。展開中に **show running-config** などのコマンドを実行しないでください。

手順

ステップ1 Management Center メニュー バーで、[展開（Deploy）] をクリックします。

ステップ2 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして[展開（Deploy）]をクリックするか、[すべて展開（Deploy All）] をクリックしてすべてのデバイスを展開します。それ以外の場合は、追加の展開オプションを設定するために、[高度な展開（Advanced Deploy）] をクリックします。

この手順の残りの部分は、[高度な展開（Advanced Deploy）] 画面に適用されます。

図 *1*: 迅速な展開

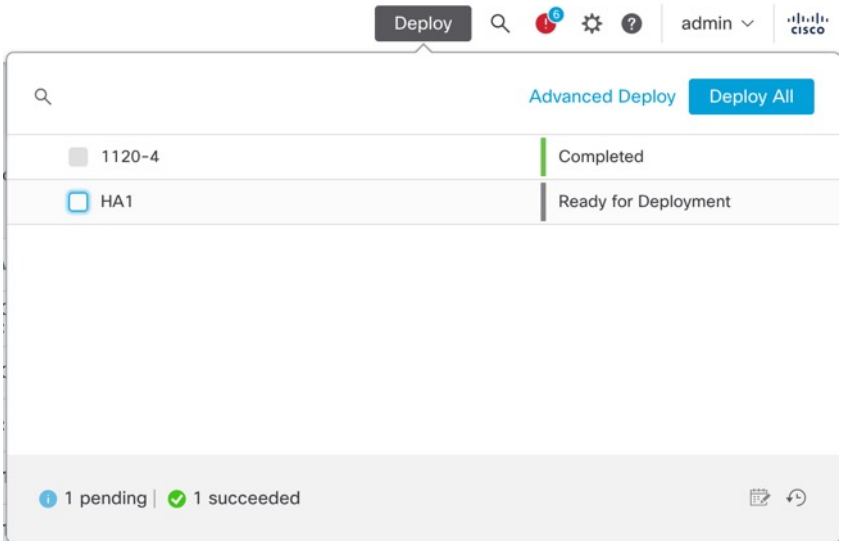
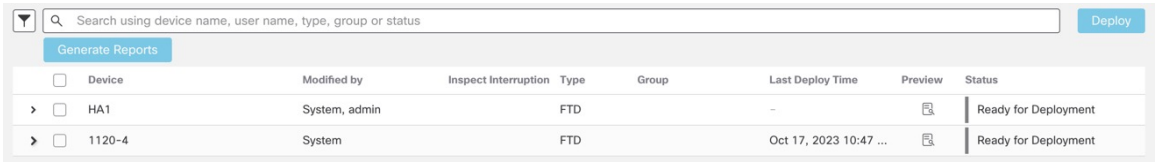
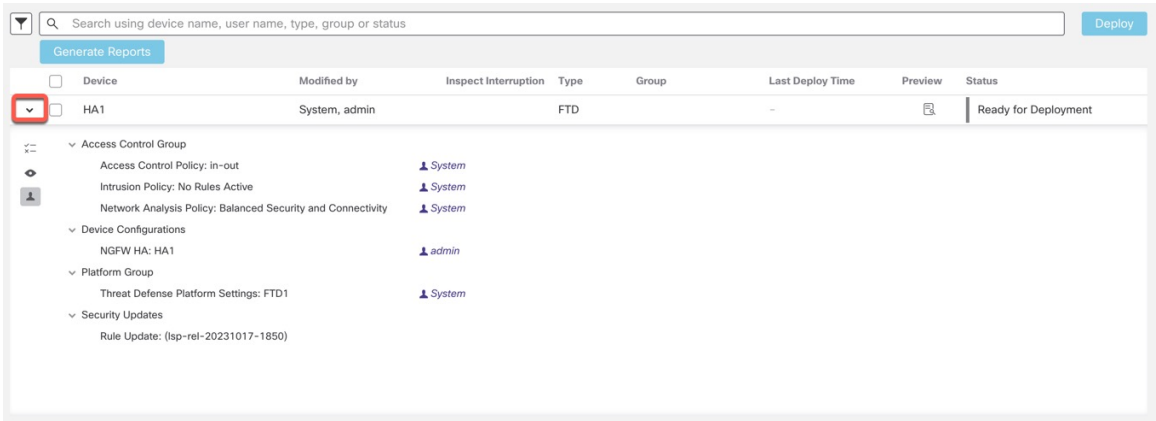


図 *2*: 高度な展開



ステップ 3 展開するデバイス固有の設定変更を表示するには、**[展開矢印（Expand Arrow）]**（ › ） をクリックします。

図 *3*: 拡張



- [変更者（Modified by）] 列には、ポリシーまたはオブジェクトを変更したユーザの一覧が表示されます。デバイスリストを展開すると、ポリシーリストごとのポリシーを変更したユーザが表示されます。**システム**ユーザー（ログインユーザーではなく）が表示される場合の詳細については、システムユーザー名 （7 ページ）を参照してください。

（注） 削除されたポリシーおよびオブジェクトのユーザ名は表示されません。

- [インスペクションの中断（Inspect Interruption）] 列には、展開時にデバイスでトラフィックインスペクションの中断が発生する可能性があるかどうかが示されます。

  ステータスに [あり（Yes）] と表示されている場合は、展開によって Threat Defense デバイスでインスペクションと、場合によってはトラフィックが中断され、展開されたリストには中断の原因となった特定の設定が [検査の中断（Inspect Interruption）]（） で示されます。

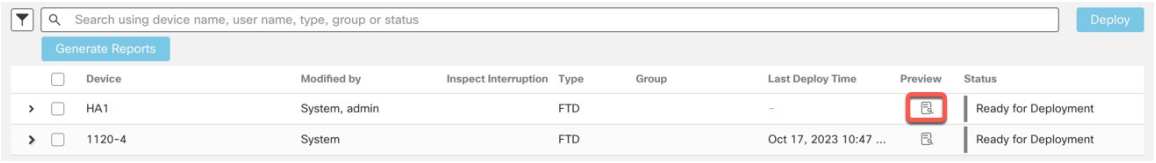
  デバイスのこの列のエントリが空白の場合は、展開時にそのデバイス上でのトラフィックインスペクションが中断されないことを示します。

  Threat Defense デバイスへの展開時にトラフィックの検査を中断させたり、トラフィック自体を中断させる可能性のある構成の特定に役立つ例については、デバイスの再起動の警告 （9 ページ） を参照してください。

- [最終変更時刻（Last Modified Time）] 列は、最後に設定変更を行った時刻を指定します。
- [プレビュー（Preview）] 列では、次の展開の変更をプレビューできます。
- [ステータス（Status）] 列には、各展開のステータスが表示されます。詳細については、展開ステータスの表示 （26 ページ）を参照してください。

ステップ 4 [プレビュー（Preview）] 列で **[プレビュー（Preview）]**（） をクリックして、展開できる設定変更を表示します。

図 *4:* プレビュー

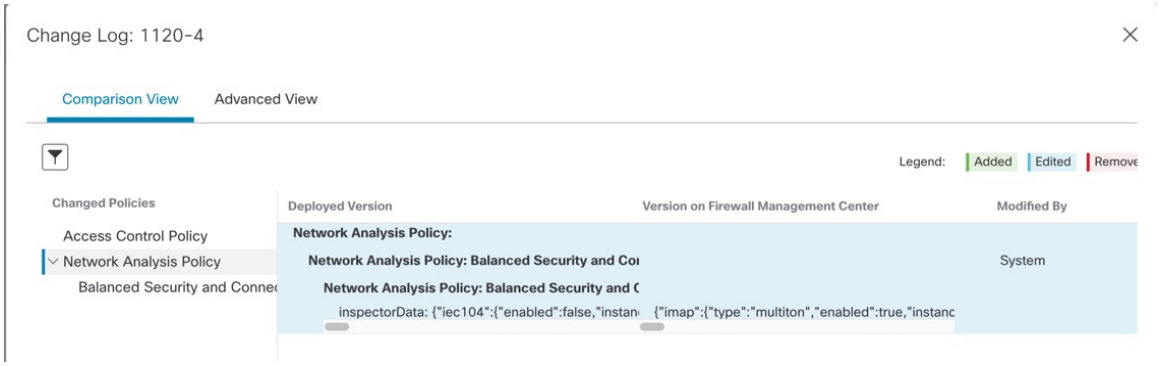


（注） **システム**（） > **[構成（Configuration）]** > **[情報（Information）]** で Management Center の名前を変更した場合、展開プレビューではこの変更が指定されませんが、展開が必要です。

プレビューでサポートされていない機能については、展開のプレビュー （2 ページ） を参照してください。

[比較ビュー（Comparison View）] タブには、すべてのポリシーおよびオブジェクトの変更が一覧表示されます。左ペインには、デバイス上で変更された異なるポリシータイプすべてがツリー構造でまとめて表示されます。

図 5: 比較ビュー



[フィルタ（Filter）] アイコン（）を使用すると、ユーザーレベルおよびポリシーレベルでポリシーをフィルタ処理できます。

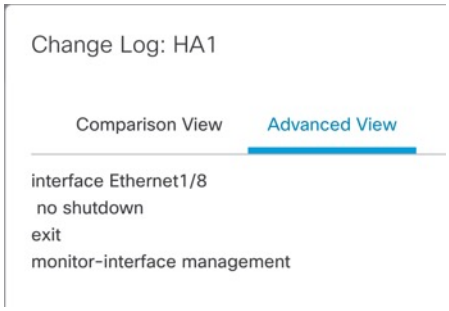
右側のペインには、ポリシー内のすべての追加、変更、または削除、あるいは左側のペインで選択したオブジェクトのリストが表示されます。右側のペインの2つの列には、最後に展開された設定（[展開済みのバージョン（Deployed Version）] 列）と、展開予定の変更（[Firewall Management Center でのバージョン（Version on Firewall Management Center）] 列）が示されます。最後に展開された設定は、デバイスからではなく、Management Center で最後に保存された展開のスナップショットから取得されます。設定の背景色は、ページの右上にある凡例に従って色分けされています。

[変更者（Modified By）] 列には、設定を変更または追加したユーザーの一覧が表示されます。ポリシーレベルでは、Management Center はポリシーを変更したすべてのユーザーを表示し、ルールレベルでは、Management Center はルールを変更した最後のユーザーのみを表示します。

[レポートのダウンロード（Download Report）] ボタンをクリックすると、変更ログのコピーをダウンロードできます。

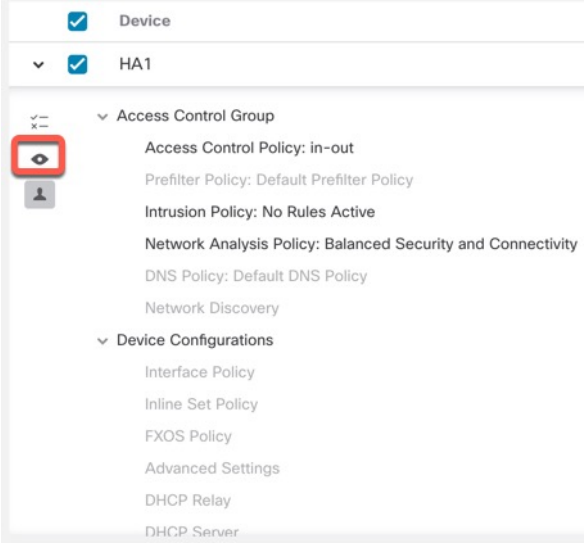
[詳細ビュー（Advanced View）] タブには、適用される CLI コマンドが表示されます。このビューは、Threat Defense のバックエンドで使用される ASA CLI に精通している場合に役立ちます。

図 6: 詳細ビュー



ステップ 5 [ポリシーの表示または非表示（Show or Hide Policy）]（） を使用して、関連付けられている未変更のポリシーを選択的に表示したり、非表示にしたりできます。

図 7: ポリシーの表示または非表示



ステップ 6 デバイス名の横にあるチェックボックスをオンにしてすべての設定変更を展開するか、[ポリシーの選択（Policy selection）]（） をクリックして、展開する個々のポリシーまたは設定を選択します（残りの変更は展開されずに保留されます）。

また、このオプションを使用して、特定のポリシーまたは設定に対する相互依存の変更を表示することもできます。Management Center は、ポリシー間（たとえば、アクセス コントロール ポリシーと侵入ポリシー間など）および共有オブジェクトとポリシーの間の依存関係を動的に検出します。相互依存の変更は、依存関係のある展開の変更を識別するために色分けされたタグを使用して示されます。展開変更のいずれかを選択した場合、相互依存の変更が自動的に選択されます。

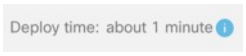
詳細については、選択的ポリシーの展開 （4 ページ）を参照してください。

（注）
- 共有オブジェクトの変更が展開されている場合は、影響を受けるポリシーも一緒に展開する必要があります。展開時に共有オブジェクトを選択すると、影響を受けるポリシーが自動的に選択されます。
- 選択的展開は、スケジュールされた展開と REST API を使用した展開はサポートされていません。これらの場合は、すべての変更を完全に展開することのみを選択できます。
- 警告とエラーの事前展開チェックは、選択したポリシーだけでなく、失効しているすべてのポリシーでも実行されます。したがって、警告またはエラーのリストには、選択していないポリシーも表示されます。
- 同様に、[展開（Deployment）] ページの[インスペクションの中断（Inspect Interruption）] 列の表示では、選択したポリシーだけでなく、失効しているすべてのポリシーも考慮されます。[インスペクションの中断（Inspect Interruption）] 列の情報については、デバイスの再起動の警告 （9 ページ） を参照してください。

ステップ 7 展開するデバイスまたはポリシーを選択したら、[概算見積（Estimate）] をクリックして展開期間の大まかな見積を取得します。

図 *8*: 概算見積

図 *9*: 展開時間



時間の長さは概算（70% の精度を含む）であり、導入にかかる実際の時間はいくつかのシナリオで異なる場合があります。20 までのデバイスへの展開では、概算見積の信頼性が高いです。

選択したデバイスで最初に成功した展開が保留中であるため、概算見積が使用できない場合、データが使用できないことを示します。この状況は、Management Center の再イメージ化の後、バージョンアップグレードの後、または高可用性フェールオーバーの後に発生する可能性があります。

（注） 概算見積書がヒューリスティック手法に基づいているため、ポリシーの一括変更（一括ポリシーの移行の場合）および選択的な展開の場合、概算見積書は不正確で信頼性が高くありません。

ステップ 8 [展開（Deploy）] をクリックします。

ステップ 9 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証メッセージ（Validation Messages）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、警告またはエラーの前にある矢印アイコンをクリックします。

次の選択肢があります。

- [展開（Deploy）]：警告状態を解決せずに展開を続行します。警告を無視して変更を展開するには、[警告を無視する（Ignore warnings）] チェックボックスをオンにします。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

次のタスク

- （オプション）展開ステータスをモニタします。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Viewing Deployment Messages*」を参照してください。
- 展開に失敗した場合は、設定変更を展開するためのベストプラクティス （16 ページ）を参照してください。
- 展開中に、展開に特定の設定変更がある場合、展開の失敗によってトラフィックが中断されることがあります。たとえば、クラスタ環境で、サイト IP と同じサブネットにない IP アドレスの誤った設定がインターフェイスで設定されているとします。このエラーにより

展開が失敗し、デバイスでロールバック操作の処理中に設定のクリアが試みられます。これらのイベントは、まとめて展開の失敗につながり、トラフィックが中断されます。

展開が失敗したときにトラフィックの中断を引き起こす可能性がある設定変更については、次の表を参照してください。

設定の変更	存在するか	トラフィックへの影響
アクセス コントロール ポリシーでの **Threat Defense サービス**の変更	対応	対応
VRF	対応	対応
Interface	対応	対応
QoS	対応	対応

（注） 展開中にトラフィックを中断する構成の変更は、Management Center と Threat Defense の両方がバージョン 6.2.3 以降である場合にのみ有効です。

関連トピック

Snort 再起動のシナリオ （8 ページ）

デバイスへの既存の設定の再展開

既存（変更なし）の設定を単一の管理対象デバイスに強制展開できます。メンテナンス ウィンドウで、またはトラフィック フローとインスペクションに対する中断の影響が最小限になる時間に、展開することを強くお勧めします。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。Snort の再起動によるトラフィックの動作 （11 ページ）および展開またはアクティブ化された際に Snort プロセスを再起動する設定 （13 ページ）を参照してください。

始める前に

設定変更を展開するためのベストプラクティス （16 ページ）で説明されているガイドラインを確認してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 強制導入するデバイスの横にある **[編集（Edit）]**（ ） をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [全般（General）] セクション見出しの横にある **[編集（Edit）]**（ ） をクリックします。

ステップ 5 **[展開を強制（Force Deploy）]** ( ) をクリックします。

（注） 強制導入は、Threat Defense に導入されるポリシールールの完全な生成をともなうため、通常の導入よりも時間がかかります。

ステップ 6 [展開（Deploy）] をクリックします。

システムでは、展開中の設定で発生したエラーや警告が識別されます。[続行（Proceed）] をクリックすると、警告状態を解決せずに続行できます。ただし、システムがエラーを示している場合は、続行できません。

次のタスク

- （オプション）展開ステータスをモニタします。Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Viewing Deployment Messages*」を参照してください。
- 展開が失敗した場合は、設定変更を展開するためのベストプラクティス （16 ページ）を参照してください。

関連トピック

Snort 再起動のシナリオ （8 ページ）

展開の管理

展開ステータスの表示

[展開（Deployment）] ページの [ステータス（Status）] 列には、各デバイスの展開ステータスが表示されます。展開が進行中の場合は、展開の進行状況のライブステータスが表示されます。そうでない場合は、次のステータスのいずれかが表示されます。

- [保留中（Pending）]：展開するデバイスに変更があることを示します。
- [警告（Warnings）] または [エラー（Error）]：展開前のチェックで展開に関する警告またはエラーが検出されたことを示しており、展開には進んでいません。警告がある場合は展開を続行できますが、エラーがある場合は続行できません。

（注） [ステータス（Status）] 列には、[展開（Deployment）] ページの 1 つのユーザセッションに対してのみ、警告またはエラーのステータスが表示されます。ページから移動したり、ページを更新したりすると、ステータスは [保留中（Pending）] に変わります。

- [失敗（Failed）]：以前の展開の試行が失敗したことを示します。ステータスをクリックして詳細を表示します。
- [キュー内（In queue）]：展開が開始されたもののシステムが展開プロセスをまだ開始していないことを示します。
- [完了（Completed）]：展開が正常に完了したことを示します。

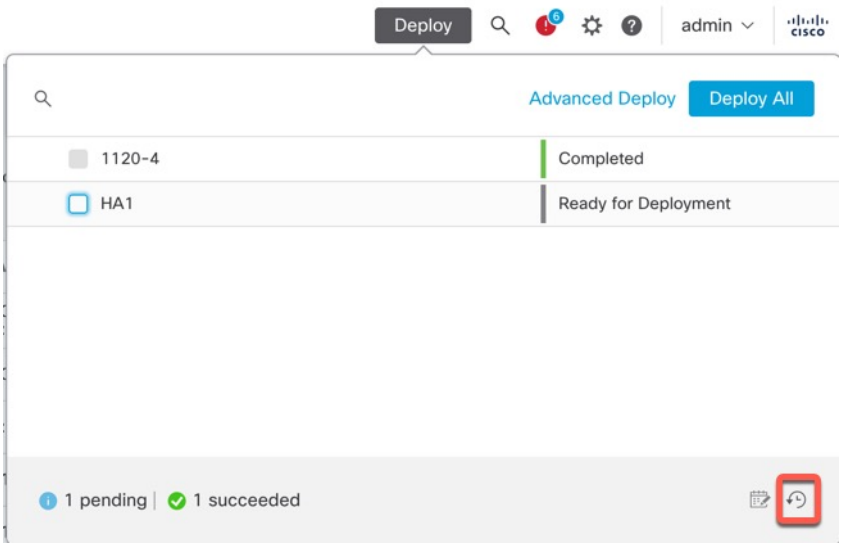
展開履歴の表示

展開履歴では、過去 10 回の成功した展開、最近 5 回の失敗した展開、および最近 5 回のロールバック展開がキャプチャされます。

手順

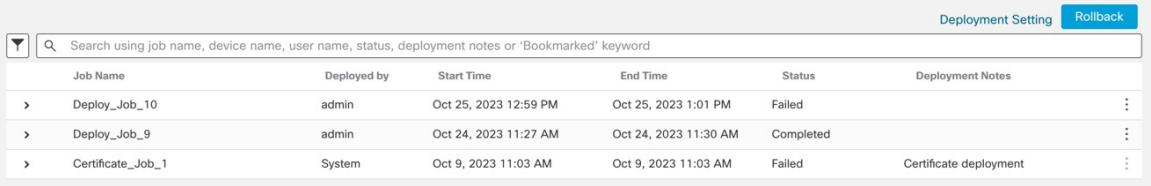
ステップ 1 Management Center メニューバーで、[展開（Deploy）] をクリックし、**[Deployment History]**（） をクリックします。

図 *10 : [展開履歴（Deployment History）] アイコン*



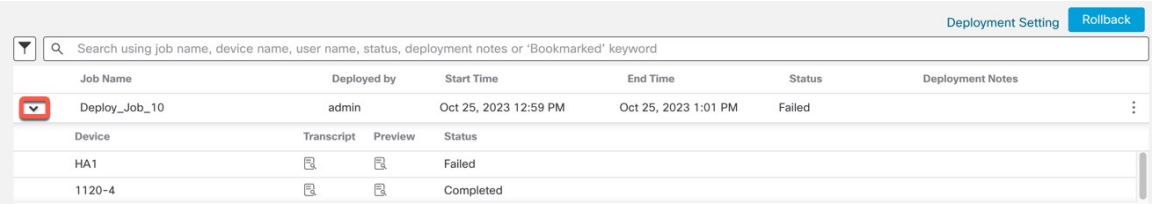
以前のすべての展開およびロールバックジョブのリストが、新しい順に表示されます。

図 *11* : *[*展開履歴（***Deployment History***）*]* ページ



ステップ 2 必要な展開ジョブの横にある **[展開矢印（Expand Arrow）]**（ › ） をクリックして、ジョブに含まれるデバイスとその展開ステータスを表示します。

図 *12* : 拡張



- [展開に関する注（Deployment Notes）] 列で注意事項を確認します。

  展開に関する注は、ユーザーが展開の一部として追加できるカスタムの注です。これらの注はオプションです。

ステップ 3 （オプション）**[トランスクリプトの詳細（Transcript Details）]**（  ）をクリックして、デバイスに送信されたコマンドと受信した応答を表示します。

図 *13* : *[*トランスクリプトの詳細（***Transcript Details***）*]* アイコン

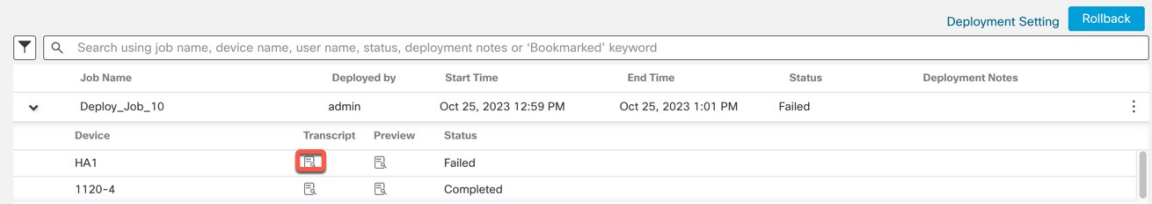
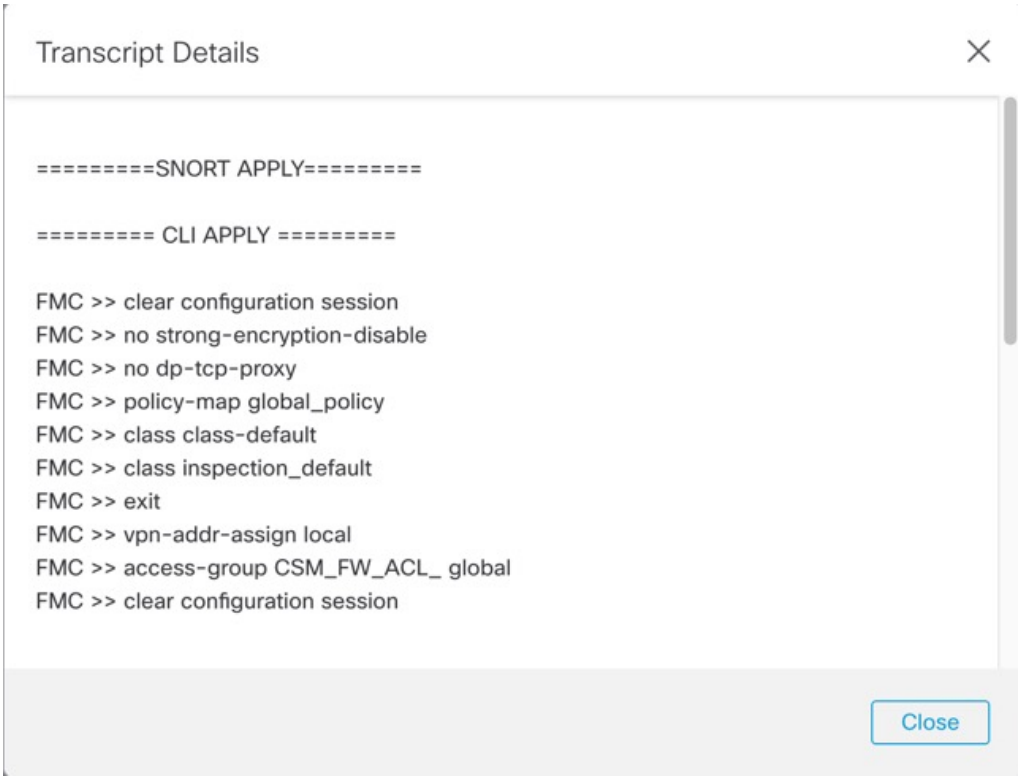


図 *14* : トランスクリプトの詳細



トランスクリプトには、次のセクションが含まれています。

- [Snortを適用（Snort Apply）]：Snort 関連ポリシーから障害または応答が発生すると、メッセージがこのセクションに表示されます。通常、このセクションは空です。
- [CLIを適用（CLI Apply）]：このセクションは、デバイスに送信されたコマンドを使用して設定される機能を対象にしています。

  （注） ロールバック操作のトランスクリプトでは、CLI コマンドの情報は提供されません。ロールバックコマンドを表示するには、展開ロールバックトランスクリプトの表示 （37 ページ）を参照してください。

- [インフラストラクチャメッセージ（Infrastructure Messages）]：このセクションには、さまざまな導入モジュールのステータスが表示されます。

[CLIを適用（CLI Apply）]セクションでは、展開トランスクリプトには、デバイスに送信されたコマンド、およびデバイスから返された応答が含まれます。これらの応答は、通知メッセージやエラーメッセージの場合があります。失敗した展開では、コマンドを含むエラーを示すメッセージを探します。これらのエラーを調べることは、FlexConfig ポリシーを使用してカスタマイズされた機能を設定している場合に特に有用になる場合があります。これらのエラーは、コマンドを設定しようとしている FlexConfig オブジェクトのスクリプトを修正するのに役立つ場合があります。

（注） 管理対象機能に送信されるコマンドと、FlexConfig ポリシーから生成されるコマンドとの間のトランスクリプトには違いはありません。

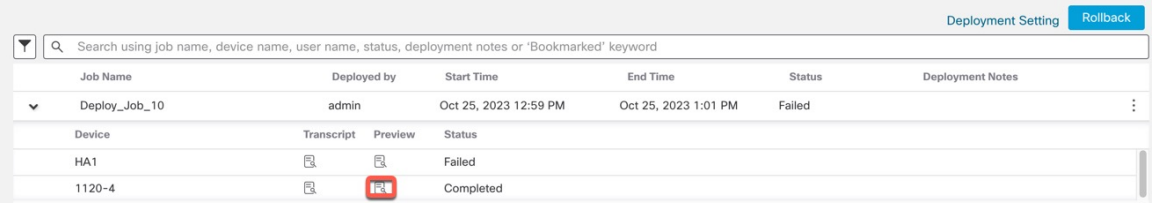
たとえば、次のシーケンスは、論理名が **outside** の GigabitEthernet0/0 を設定するコマンドを Management Center が送信したことを示しています。デバイスは、自動的にセキュリティレベルを 0 に設定したことを応答しました。Threat Defense がセキュリティレベルを使用することはありません。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

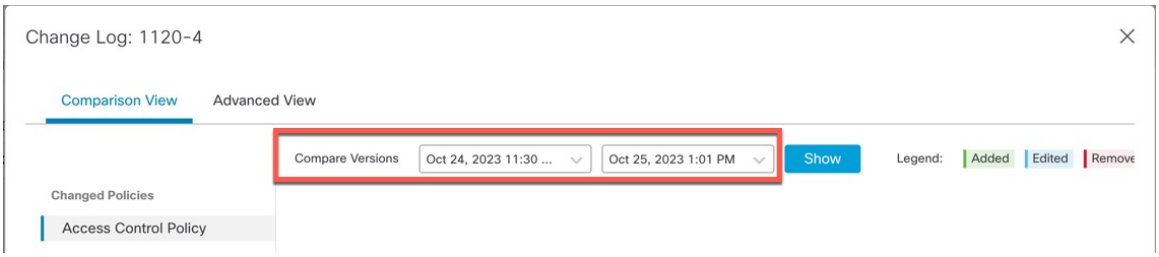
ステップ 4 （オプション）**[プレビュー（Preview）]**（） をクリックして、デバイスに展開されたポリシーとオブジェクトの変更を表示し、以前に展開されたバージョンと比較します。

図 *15 : [プレビュー（Preview）] アイコン*



1. 2 つのバージョンを比較して変更ログを表示するには、ドロップダウンボックスで必要なバージョンを選択し、[表示（Show）] ボタンをクリックします。ドロップダウンボックスには、展開ジョブの名前と展開の終了時間が表示されます。

   図 *16 : バージョンの比較*



   （注） ドロップダウンボックスには、失敗した展開も表示されます。

2. [変更者（Modified by）] 列には、ポリシーまたはオブジェクトを変更したユーザーの一覧が表示されます。

   1. ポリシーレベルでは、Management Center はポリシーを変更したすべてのユーザーの名前を表示します。
   2. ルールレベルでは、Management Center はルールを変更した最後のユーザーを表示します。

3. [レポートのダウンロード（Download Report）] をクリックして、変更ログのコピーをダウンロードすることもできます。

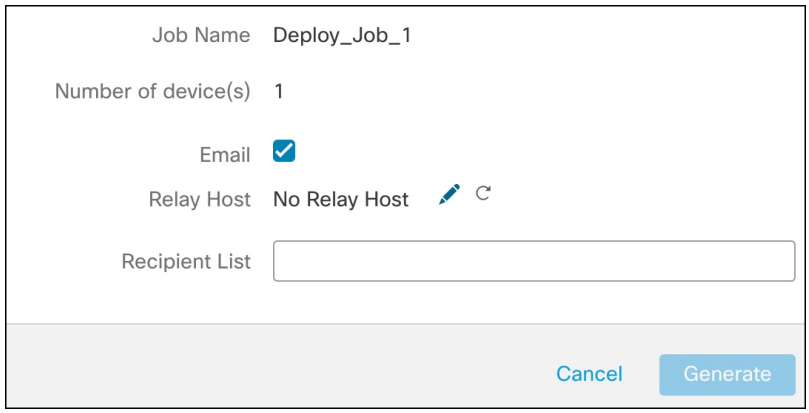
（注）
- 展開履歴のプレビューは、証明書の登録、HA操作、および失敗した展開ではサポートされていません。
- デバイスが登録されている場合でも、作成されたジョブ履歴レコードのプレビューはサポートされていません。

ステップ5 （任意）各展開ジョブに対して、**その他**（⋮）アイコンをクリックして、他のアクションを実行します。

- [ブックマーク（Bookmark）]：展開ジョブをブックマークします。
- [展開に関する注意の編集（Edit Deployment Notes）]：展開ジョブに追加した、展開に関するカスタムの注意を編集します。
- [レポートの生成（Generate Report）]：監査に使用できる展開レポートを生成します。このレポートには、プレビューとトランスクリプト情報を持つジョブプロパティが含まれており、レポートは PDF ファイルでダウンロードできます。

1. [レポートの生成（Generate Report）] をクリックして、展開レポートを生成します。

図 *17*: レポートの作成



2. [レポートの生成（Generate Report）]ポップアップウィンドウで、[電子メール（Email）] チェックボックスをオンにします。
3. メールリレーホストが設定されている場合は、レポートを電子メールで送信することもできます。メールリレーホストが設定されていない場合は、[編集（Edit）]（✎）アイコンを使用してメールリレーホストを設定または変更します。詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Configuring a Mail Relay Host and Notification Address」を参照してください。
4. [受信者リスト（Recipient List）] では、複数の電子メールアドレスをセミコロンで区切って入力することができます。

5. [生成（Generate）] をクリックしてレポートを生成します。このレポートは電子メールで受信者に送信されます。
6. [通知（Notifications）] タスクタブで、進捗状況を追跡できます。レポートの生成が完了したら、[通知（Notifications）] タスクタブのリンクをクリックしてPDF レポートをダウンロードします。

設定バージョン数の設定

Management Center は、デバイス設定履歴ファイルを設定バージョンとしてディスクに保存します。デバイスで保持するコンフィギュレーションバージョンの数を指定できます。この設定により、ディスク上のデバイス設定ファイルのサイズを予測し、許容範囲内に保つことができます。設定バージョンの数を減らすと、バックアップサイズが小さくなり、Management Center の高可用性同期速度が向上します。

Management Center の高可用性展開では、コンフィギュレーションバージョンの設定はアクティブな Management Centerでのみ使用できます。

始める前に

この機能は、バージョン 7.4.0 ではサポートされていません。

手順

ステップ 1 Management Center のメニューバーで、[展開（Deploy）]**[Deployment History]**（） を選択します。

ステップ 2 [展開設定（Deployment Setting）] をクリックします。

ステップ 3 [保持するバージョン数（Number of Versions to Retain）] ドロップダウンリストから、デバイスに対で保持する設定バージョンの数を選択します。

（注） バージョンの数を減らすと、選択したバージョンサイズと一致するように最も古い設定バージョンが削除されます。削除したバージョンをロールバックまたはプレビューすることはできません。

- [最大許容ディスクサイズ（Maximum Permitted Disk Size）]：設定バージョンを保存する最大サイズは 20 GB です。Management Center は、設定バージョンのサイズを定期的に計算し、設定バージョンのサイズが 20 GB を超えた場合に正常性アラートを送信します。正常性アラートを解決するには、設定バージョンのサイズが 20 GB 未満になるように [保持するバージョン数（Number of Versions to Retain）] を選択します。
- [現在の設定バージョンのサイズ（Current Configuration Version Size）]：以前の展開における Management Center の設定ファイルのサイズ。

- [予測される設定バージョンのサイズ（Estimated Configuration Version Size）]：Management Centerの設定ファイルの概算サイズ。これは、保持することを選択した設定バージョン数に基づいて計算されます。

ステップ 4 [保存（Save）] をクリックします。

展開のロールバック

デバイスを以前に展開した設定にロールバックできます。ポリシーの展開後に、デバイスを通過するトラフィックが意図しない方法で影響を受けた場合は、ロールバックにより、展開に失敗する前の状態にデバイスを戻すオプションが提供されます。

ロールバック中断を伴う操作です。既存のすべての接続とルートがドロップされ、トラフィックが中断されます。

中断を伴う設定の特定

展開がうまくいかず、意図しない方法でトラフィックの中断が発生した場合は、その状態の原因となっている展開の変更を特定し、展開が成功するように修正することを推奨します。

設定を比較するには、以下の方法を参照してください。

ロールバック前

1. **[展開（Deploy）]**>**[展開履歴（Deployment History）]** を選択し、最後に展開された（トラフィックの中断を引き起こした）ジョブを展開して、[プレビュー（Preview）] アイコン（）をクリックします。

   プレビューページには展開を比較するオプションがあり、以前の展開と比較した、展開の特定の変更を識別するために役立ちます。

2. 問題の原因となっている変更を特定したら、設定を修正し、デバイスに再展開します。

ロールバック後

1. ロールバック操作が成功したら、**[展開（Deploy）]**>**[展開（Deployment）]** を選択し、ロールバックされたデバイスの横にある [プレビュー（Preview）] アイコンをクリックします。
2. ロールバックされた設定と、展開が保留されている Management Center の最新の変更との間の変更点が表示されます。
3. 問題の原因となっている変更を特定したら、設定を修正し、デバイスに再展開します。

ロールバックのガイドラインと制約事項

- 現在展開されているバージョンより前の 10 個のバージョンのいずれかにロールバックできます。これより前のバージョンへのロールバックはサポートされていません。サポートされていないバージョンの場合、ロールバックアイコンはグレー表示になります。

- 再度ロールバックする前に、展開を実行する必要があります。
- ロールバックを実行すると、ロールバックされたデバイスは Management Center で期限切れとしてマークされます。設定に加えた変更は、次の展開のために保留されています。保留中の変更を表示するには、**[展開（Deploy）] > [展開（Deployment）]** を選択し、ロールバックされたデバイスの横にある [プレビュー（Preview）] アイコンをクリックします。
- [オブジェクトグループの検索（Object Group Search）] 設定が無効になっている場合、大きなアクセスリストを持つデバイスでは、ロールバック操作の完了に時間がかかることがあります。[オブジェクトグループの検索（Object Group Search）] 設定を確認するには、**[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスを選択して [詳細設定の編集（Edit Advanced Settings）] をクリックします。
- Firepower 4100/9300 の場合は、現在の Chassis Manager インターフェイス設定がどのロールバックバージョンでも同じであることを確認してください。そうでない場合、ロールバック インターフェイスの設定が実際のインターフェイスと一致しない可能性があります。
- マネージャ アクセス インターフェイス（マネージャまたはデータインターフェイス）がロールバックバージョンと現在のバージョンで異なる場合、ロールバックはサポートされません。
- 独立した証明書の登録も、[展開履歴（Deployment History）]ページに展開ジョブとして表示されます。ただし、これらのバージョンにロールバックすることはできません。証明書の登録後に作成された展開バージョンからのロールバックでは、証明書の関連付けも元に戻ります。ロールバック後の次の展開では、展開を続行する前に、証明書を手動で関連付けます。
- Management Center をアップグレードすると、デバイスをアップグレードしなかった場合でも、以前のソフトウェアリリースからのすべてのロールバックバージョンがデバイスで使用できなくなります。
- デバイスをアップグレードする場合は、現在のソフトウェアリリースのバージョンにのみロールバックできます。
- 展開頻度が [1回（Once）] に設定された FlexConfig オブジェクトがあるデバイスの展開がロールバックされた場合、プレビューページに古いと表示されていても、そのオブジェクトを再展開することはできなくなります。ロールバック後は、次の展開の前に、FlexConfig オブジェクトを手動で割り当て解除してから、デバイスに再割り当てする必要があります。
- ロールバックは以下の高可用性シナリオではサポートされていません。
  - ロールバックするバージョンに高可用性ブートストラップ設定が含まれている場合。つまり、スタンドアロンデバイスの高可用性を最初に形成したときの展開です。
  - 現在スタンドアロンモードのデバイスが、以前の展開バージョンで高可用性ペアの一部だった場合。
- クラスタリングについては、以下のガイドラインを参照してください。

- 現在スタンドアロンモードのデバイスが、以前の展開バージョンでクラスタの一部だった場合、ロールバックはサポートされません。
- （Secure Firewall 3100/4200 およびプライベートクラウドの Threat Defense Virtual）クラスタリングブートストラップ設定を変更したり、ノードを追加または削除したりすると、それらの変更より前のバージョンにロールバックすることはできません。

ロールバック後に元に戻されない設定

ロールバックは、いくつかを除いて、デバイス上のすべての設定を元に戻します。詳細については、次の表を参照してください。

ロールバック中に元に戻される設定	ロールバック中に元に戻されない設定
• すべてのポリシー設定 • インターフェイス設定 • SRU 設定 • VDB 設定 • LSP 設定 • VPN 設定 • FXOS 設定	• Snort バイナリ （注） Snort 3 バージョンポリシーから Snort 2 バージョンポリシーへのロールバック、およびその逆のロールバックがサポートされています。 • Geo DB

ロールバックの実行

デバイスを以前に展開した設定にロールバックできます。ポリシーの展開後に、デバイスを通過するトラフィックが意図しない方法で影響を受けた場合は、ロールバックにより、展開に失敗する前の状態にデバイスを戻すオプションが提供されます。

ロールバックは、選択したデバイス上の設定だけを元に戻します。

手順

ステップ 1 [展開（Deploy）] > **[Deployment History]**（） を選択します。

以前のすべての展開ジョブのリストが、新しい順に表示されます。

ステップ 2 [ロールバック（Rollback）] をクリックします。

ステップ 3 [ジョブ（Job）] をクリックして [選択したジョブ（Selected Job）] ドロップダウンリストからジョブを選択するか、[デバイスリスト（Device List）] をクリックして、表示されるデバイスのリストをフィルタ処理します。

ステップ 4 （任意）[デバイスの検索（Search Device）] 検索ボックスにデバイス名を入力して、デバイスリストをフィルタ処理します。

ステップ 5 ロールバックするデバイスの横にあるボックスをオンにし、[ロールバックバージョン（Rollback Version）] ドロップダウンリストから各デバイスのバージョンを選択します。

図 *18* : 選択したジョブリスト

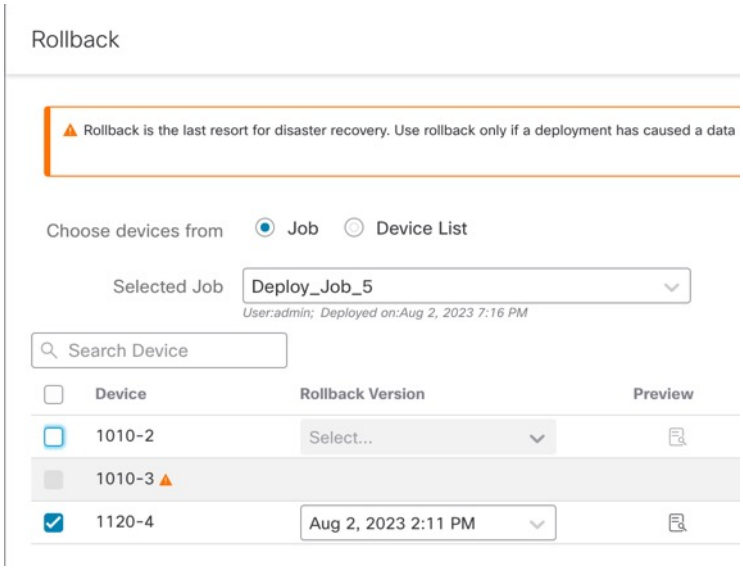
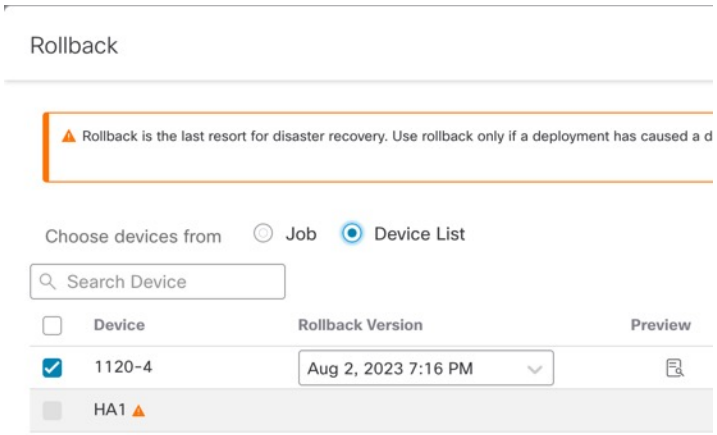


図 *19* : *Device List*



特定のロールバックバージョンのジョブ名と関連する展開に関する注もリストされています。

ステップ 6 （任意）プレビューアイコン（）をクリックして、選択したバージョンで展開される変更を表示します。

ステップ 7 [ロールバック（Rollback）] をクリックします。

次のタスク

ロールバックのステータスを確認するには、**[展開（Deploy）]** > **[展開（Deployment）]** を選択します。デバイス名の横にあるロールバックステータスを確認できます。

展開ロールバック トランスクリプトの表示

ロールバック トランスクリプトは、デバイスから返される応答とともに、デバイスに送信されるコマンドの文章バージョンです。ロールバック操作が失敗した場合、[展開（Deploy）]>[展開履歴（Deployment History）] ページのトランスクリプトに失敗の理由が示されます。ただし、成功したロールバック操作で実行されたCLIコマンドを知るには、ロールバック操作の完了後に以下の手順に従ってください。この情報は、次回の展開までしか利用できないことに注意してください。

（注） CLIコマンド情報は、ロールバックの完了後に利用でき、次回の展開までのみ利用できます。ロールバック操作後の最初の展開では、ロールバック関連のすべての情報が消去されます。

（注） ロールバック展開では、[展開に関する注（Deployment Notes）] がロールバックジョブとして自動的に更新されます。[展開履歴（Deployment History）]ページで、ユーザーは[検索（Search）]オプションを使用してロールバックジョブを簡単にフィルタ処理できます。

手順

ステップ 1 Secure Firewall Management Center メニューバーで、**[システム（System）]** > **[正常性（Health）]** > **[モニター（Monitor）]** を選択します。

ステップ 2 左ペインからロールバックしたデバイスを選択します。

ステップ 3 [システムとトラブルシューティングの詳細を表示（View System & Troubleshooting Details）] リンクをクリックします。

ステップ 4 [詳細なトラブルシューティング（Advanced Troubleshooting）] をクリックします。

ステップ 5 [脅威防御 CLI（Threat Defense CLI）] をクリックします。

ステップ 6 [コマンド（Command）] ドロップダウンボックスから [show] を選択します。

ステップ 7 [パラメータ（Parameter）] フィールドに **`running`** と入力します。

ステップ 8 [実行（Execute）] をクリックします。

複数のデバイスのポリシー変更レポートのダウンロード

複数の Threat Defense デバイスの、最後の展開以降に行われたポリシーとオブジェクトの変更に関するレポートをダウンロードします。以下のレポートを含む zip ファイルの形式でレポートをダウンロードできます。

- ポリシー内の追加、更新、または削除、あるいはデバイスに展開されるオブジェクトをプレビューする各デバイスの保留中の変更レポート。詳細は、設定変更の展開 （18ページ）および「展開のプレビュー」を参照してください。
- レポートステータスに基づいて各デバイスを分類する統合レポート。

手順

ステップ 1 [展開（Deploy）] > [高度な展開（Advanced Deploy）] を選択します。

ステップ 2 保留中のポリシー変更レポートを生成するデバイスの横にあるチェックボックスをオンにし、[保留中の変更レポート（Pending Changes Reports）] をクリックします。

ステップ 3 [保留中の変更レポート（Pending Changes Reports）] をクリックします。レポートはバックグラウンドで生成されます。

ステップ 4 Management Center メニューバーで、[通知（Notification）] > [タスク（Tasks）] を選択して、レポート生成タスクを表示します。 >

レポート要求タスクが完了すると、タスク通知内にダウンロードリンクが表示されます。

ステップ 5 レポートをダウンロードするには、[レポートのダウンロード（Download Report）] をクリックします。

ポリシーの比較

変更後のポリシーが組織の標準に準拠することを確かめたり、システムパフォーマンスを最適化したりする目的で、2つのファイルポリシーの間の違いや、保存済みポリシーと実行中のポリシーの間の違いを調べることができます。

比較できるポリシーのタイプは次のとおりです。

- DNS
- ファイル
- ヘルス
- アイデンティティ
- 侵入（Snort 2 ポリシーのみ）
- ネットワーク分析

- SSL

比較ビューには、両方のポリシーが並べて表示されます。2 つのポリシー間の差異は、次のように強調表示されます。

- 青色は強調表示された設定が2つのポリシーで異なることを示し、差異は赤色で示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

始める前に

特定のポリシーに対するアクセス権と必要なライセンスがあり、ポリシーを設定するための正しいドメインにいる場合にのみ、ポリシーを比較できます。

手順

ステップ 1 比較するポリシーの管理ページにアクセスします。

- [DNS]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[DNS]**
- [ファイル（File）]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[マルウェアとファイル（Malware & File）]**
- [状況（Health）]：**システム**（⚙） > **[正常性（Health）]** > **[ポリシー（Policy）]**
- [ID（Identity）]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アイデンティティ（Identity）]**
- [侵入（Intrusion）]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[侵入（Intrusion）]**

  （注） Snort 2 ポリシーのみを比較できます。

- [ネットワーク分析（Network Analysis）]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]**、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policies]**

  （注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** > **[復号（Decryption）]**

ステップ 2 [ポリシーの比較（Compare Policies）] をクリックします。

ステップ 3 [比較対象（Compare Against）] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[他のポリシー（Other Policy）] を選択します。
- 同じポリシーの2つのリビジョンを比較するには、[その他のリビジョン（Other Revision）] を選択します。

- 現在のアクティブポリシーを他のポリシーに対して比較するには、[実行中の設定（Running Configuration）] を選択します。

ステップ 4 選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合、[ポリシーA（Policy A）] ドロップダウンリストと [ポリシーB（Policy B）] ドロップダウンリストから比較するポリシーを選択します。
- 実行中の設定を別のポリシーと比較する場合、[ポリシーB（Policy B）] ドロップダウンリストから 2 番目のポリシーを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 比較の結果を確認します。

- [比較ビューア（Comparison Viewer）] : 比較ビューアを使用して、ポリシーの違いを個別に検索するには、タイトルバーの上にある [前へ（Previous）] または [次へ（Next）] をクリックします。
- [比較レポート（Comparison Report）] : 2 つのポリシーの違いを示す PDF レポートを生成するには、[比較レポート（Comparison Report）] をクリックします。

現在のポリシーレポートの生成

ほとんどのポリシーには、2 種類のレポートを生成することができます。単一のポリシーに関するレポートには、現在保存されているポリシー設定の詳細が記載されます。一方、比較レポートには、2つのポリシー間の違いだけがリストされます。単一ポリシー レポートは、ヘルス ポリシーを除くすべてのポリシー タイプについて生成できます。

（注） 侵入ポリシー レポートには基本ポリシーの設定とポリシー階層の設定が結合され、どちらが基本ポリシーまたはポリシー レイヤのどちらに基づく設定であるかは区別されません。

始める前に

特定のポリシーに対するアクセス権と必要なライセンスがあり、ポリシーを設定するための正しいドメインにいる場合にのみ、ポリシーレポートを生成できます。

手順

ステップ 1 レポートを生成するポリシーの管理ページにアクセスします。

- アクセス制御—**[ポリシー（Policies）] > [アクセス制御（Access Control）]**
- [DNS] : **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [DNS]**
- [ファイル（File）] : **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [マルウェアとファイル（Malware & File）]**

- [状況（Health）]：**システム**（⚙） > **[正常性（Health）]** > **[ポリシー（Policy）]**
- [ID（Identity）]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アイデンティティ（Identity）]**
- [侵入（Intrusion）]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[侵入（Intrusion）]**
- NAT：**[デバイス（Devices）]** > **[NAT]**
- [ネットワーク分析（Network Analysis）]：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]**、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。 または **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policies]**

  （注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

- [SSL]：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** > **[復号（Decryption）]**

ステップ 2 レポートの生成対象とするポリシーの横にある [レポート（Report）]（📄） をクリックします。

設定の展開の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
デバイスのロールバックのために保持する展開履歴ファイルの数を設定します。	任意（Any）	任意（Any）	デバイスのロールバックのために保持する展開履歴ファイルの数を最大 10（デフォルト）まで設定できるようになったため、Management Center のディスク容量を節約できます。 新規/変更された画面：[展開（Deploy）] > **[Deployment History]**（🕘） > [展開設定（Deployment Setting）] > [構成バージョン設定（Configuration Version Setting）] その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。

機能	最小 Management Center	最小 Threat Defense	詳細
前回の展開以降の設定変更に関するレポートを表示および生成します。	任意（Any）	任意（Any）	前回の展開以降の設定変更に関する次のレポートを生成、表示、および（zip ファイルとして）ダウンロードできます。 • ポリシー内の追加、変更、または削除、あるいはデバイスに展開されるオブジェクトをプレビューする各デバイスのポリシー変更レポート。 • ポリシー変更レポート生成のステータスに基づいて各デバイスを分類する統合レポート。 これは、Management Center または Threat Defense デバイスのいずれかのアップグレード後に特に役立ち、展開する前にアップグレードによって加えられた変更を確認できます。 新規/変更された画面：**[展開（Deploy）]** > **[高度な展開（Advanced Deploy）]**。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。
設定の変更を展開するときに、レポートを生成して電子メールで送信します。	7.2	いずれか	任意の展開のレポートを生成できるようになりました。 新規/変更された画面：**[展開（Deploy）]** > **[Deployment History]**（）アイコン > その他（） **[レポートの生成（Generate Report）]**

機能	最小 Management Center	最小 Threat Defense	詳細
展開プレビューとプレビュー時のユーザー情報。	7.0	いずれか	[展開（Deployment）] ページには、次の新たに追加された機能があります。 • [展開（Deployment）] ページの [変更者（Modified By）] 列には、各ポリシーリストに対してポリシーを変更したユーザーが一覧表示されます。 • 展開のフィルタサポート：[展開（Deployment）] ページに表示されるフィルタアイコンには、展開が保留されているデバイスのリストをフィルタ処理するオプションが用意されています。フィルタアイコンには、選択されたデバイスとユーザー名に基づいてリストをフィルタ処理するオプションがあります。 • 展開履歴のプレビュー：[プレビュー（Preview）] をクリックして、デバイスに展開されたポリシーとオブジェクトの変更を表示し、以前に展開されたバージョンと比較します。展開履歴では、最近 10 回の成功した展開、最近 5 回の失敗した展開、および最近 5 回のロールバック展開がキャプチャされます。 • 展開に関する注：[展開に関する注（Deployment Notes）] は、ユーザーが展開の一部として追加できるカスタムおよびオプションの注です。[展開履歴（Deployment History）] ページで [展開に関する注（Deployment Notes）] 列を表示できます。 • 展開のロールバックは、Snort 3 ポリシーでも利用できます。
Threat Defense デバイスでの展開のロールバック。	6.7	6.7	ロールバックは、Threat Defense デバイス上の既存の展開を削除し、以前に展開された構成でデバイスを再構成するために提供されている展開機能です。 新規/変更されたページ：**[展開（Deploy）]** > **[展開履歴（Deployment History）]** ページには、ロールバックアイコンのある新しい [ロールバック（Rollback）] 列が用意されています。ジョブを展開すると、同様のロールバックアイコンが表示されるため、デバイスレベルでロールバックを開始できます。

機能	最小 Management Center	最小 Threat Defense	詳細
新しい展開 Web インターフェイス。	6.6	いずれか	Management Center メニューバーの [展開（Deploy）] ボタンが [展開（Deploy）] メニューに変更されました。その下に 2 つの新しいサブメニューオプションがあります。[展開（Deployment）] と [展開履歴（Deployment History）] です。[展開（Deployment）] ページは改善が施されたとともに新しい機能が追加され、新しい [展開履歴（Deployment History）] ページには、以前のすべての展開の凡例が表示されます。 [展開（Deployment）] ページには、次の新たに追加された機能があります。 • 展開のステータス：[展開（Deployment）] ページの [ステータス（Status）] 列には、各デバイスの展開ステータスが表示されます。 • 展開の概算見積：[展開（Deployment）] ページでは、デバイス、ポリシー、または設定を選択した後にのみ、[概算見積（Estimate）] リンクを使用できます。[概算見積（Estimate）] リンクをクリックすると、展開期間の概算見積を取得できます。 • 展開のプレビュー：プレビューには、デバイス上に展開するポリシーとオブジェクトのすべての変更のスナップショットが表示されます。ポリシーの変更には、新しいポリシー、既存のポリシーの変更、および削除されたポリシーが含まれます。オブジェクトの変更には、ポリシーで使用される追加および変更されたオブジェクトが含まれます。 • 選択的ポリシーの展開：Management Center では、展開が予定されているデバイス上の変更すべてのリスト内で特定のポリシーを選択し、選択したポリシーのみを展開することができます。

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。