



Cisco Secure Firewall Management Center での Snort 2 から Snort 3 への移行

- [Snort 2 から Snort 3 への移行 \(1 ページ\)](#)
- [Snort 3 への移行の利点 \(1 ページ\)](#)
- [ビジネスシナリオの例 \(2 ページ\)](#)
- [Snort 2 から Snort 3 への移行のベストプラクティス \(2 ページ\)](#)
- [前提条件 \(2 ページ\)](#)
- [エンドツーエンドの移行ワークフロー \(3 ページ\)](#)
- [Threat Defense で Snort 3 を有効にする \(3 ページ\)](#)
- [単一の侵入ポリシーの Snort 2 ルールの Snort 3 への変換 \(4 ページ\)](#)
- [設定変更の展開 \(9 ページ\)](#)

Snort 2 から Snort 3 への移行

Snort は、バージョン 2 からバージョン 3 に大幅な変更が加えられた侵入検知および防御システムです。Snort 3 の拡張機能を活用するには、Snort 2 から既存のルールセットを移行することが重要になります。この移行プロセスでは、Snort 2 ルールを変換して Snort 3 ルール構文への適応を行い、検出とパフォーマンスを向上させるためにルールを最適化します。

組織によっては、脅威防御デバイスを Cisco Secure Firewall Management Center で管理することができます。組織では、Snort 2 から Snort 3 への移行時にハイブリッド展開アプローチを選択できます。このアプローチにより、段階的な移行が可能になり、中断の可能性が最小限に抑えられます。

Snort 3 への移行の利点

- **プロトコルサポートの強化**：Snort 3 ではプロトコルサポートが改善されており、暗号化されたトラフィックを含む幅広い最新のプロトコルで脅威をモニターおよび検出できます。
- **ルール管理の合理化**：Snort 3 は、より使いやすいルール言語とルール管理システムを提供し、ルールの作成、変更、および効果的な管理を容易にします。

- **パフォーマンスの向上**：Snort 3 は、大量のトラフィックをより効率的に処理するように最適化されているため、パフォーマンスのボトルネックのリスクが軽減され、タイムリーな脅威検出が可能になります。

ビジネスシナリオの例

Alice は、ネットワーク インフラストラクチャのモニターと保護を Snort インスペクションエンジンに大きく依存している大規模な組織でセキュリティアナリストとして働いています。この組織は数年間 Snort バージョン 2 を使用していますが、いくつかの制限と課題に直面しています。

ネットワーク管理者の Bob は、これらの問題を克服し、組織のネットワークセキュリティ機能を強化するために、Snort 2 から Snort 3 に移行しようとしています。

この移行により、ネットワークセキュリティのモニタリングが改善され、パフォーマンスが向上し、ルール管理が合理化されます。

Snort 2 から Snort 3 への移行のベストプラクティス

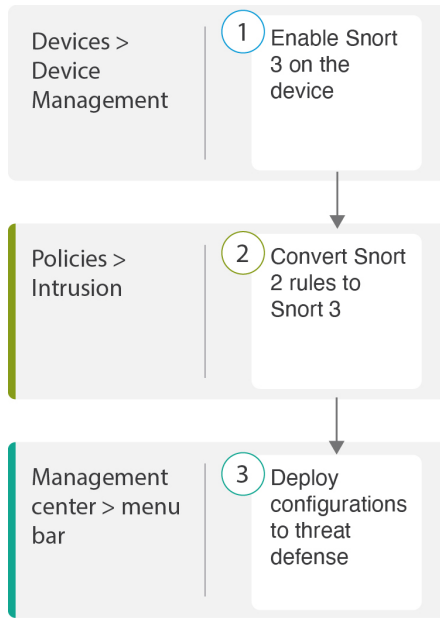
- 移行を実行する前に、侵入ポリシーをバックアップします。『[Cisco Secure Firewall Management Center Administration Guide](#)』の「Export Configurations」タスクを参照してください。
- デバイスを Snort 3 にアップグレードする前に、Snort 2 で変更が行われた場合は、同期ユーティリティを使用して Snort 2 から Snort 3 に最新の同期を追加すると、同様の対象範囲で開始できます。[Snort 2 のルールと Snort 3 の同期](#) を参照してください。
- Snort 2 カスタムルールは Snort 3 に自動的に変換されないため、手動で移行する必要があります。[Snort 2 のカスタム IPS ルールの Snort 3 への変換](#) を参照してください。
- 同期では、しきい値または抑制を含む Snort 2 ルールは移行されません。これらのルールは、Snort 3 で再度作成する必要があります。

前提条件

- Snort の実用的な知識を持っている。Snort 3 アーキテクチャの詳細については、[Snort 3 Adoption](#) を参照してください。
- Management Center をバックアップする。「[Backup the Management Center](#)」を参照してください。
- 侵入ポリシーをバックアップする。「[Exporting Configurations](#)」を参照してください。

エンドツーエンドの移行ワークフロー

次のフローチャートは、Cisco Secure Firewall Management Center で Snort 2 を Snort 3 に移行するためのワークフローを示しています。



ステップ	説明
①	デバイスで Snort 3 を有効にします。 Threat Defense で Snort 3 を有効にする (3 ページ) を参照してください。
②	Snort 2 ルールを Snort 3 に変換します。 単一の侵入ポリシーの Snort 2 ルールの Snort 3 への変換 (4 ページ) を参照してください。
③	設定を展開します。 設定変更の展開 を参照してください。

Threat Defense で Snort 3 を有効にする



注目 展開プロセス中に現在の検査エンジンをシャットダウンする必要があるため、一時的なトラフィック損失が発生します。

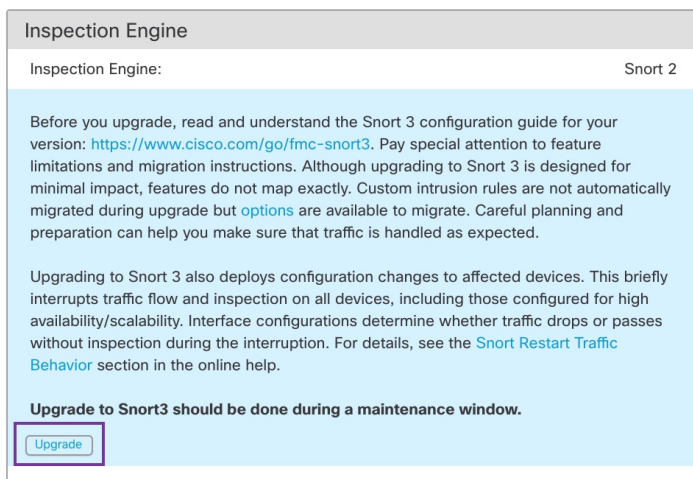
ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。

ステップ 2 対応するデバイスをクリックして、デバイスのホームページに移動します。

単一の侵入ポリシーの Snort 2 ルールの Snort 3 への変換

ステップ 3 [デバイス (Device)] タブをクリックします。

ステップ 4 [検査エンジン (Inspection Engine)] セクションで、[アップグレード (Upgrade)] をクリックします。



ステップ 5 [はい (Yes)] をクリックします。

次のタスク

デバイスに変更を展開します。 [設定変更の展開](#) を参照してください。

選択した Snort バージョンとの互換性を得るため、システムは展開プロセス中にポリシー設定を変換します。

単一の侵入ポリシーの Snort 2 ルールの Snort 3 への変換

ステップ 1 [ポリシー (Policies)] > [侵入 (Intrusion)] を選択します。

ステップ 2 [侵入ポリシー (Intrusion Policies)] タブで、[Snort 3 同期ステータスの表示 (Show Snort 3 Sync status)] をクリックします。

Firewall Management Center
Policies / Access Control / Intrusion / Intrusion Policies Overview

Intrusion Policies Network Analysis Policies

Show Snort 3 Sync status ⓘ

Search by Intrusion Policy, Description, or Bas

Intrusion Policy	Description
_Intrusion_Policy_1	

ポリシーにオレンジ色の矢印が表示されている場合は、侵入ポリシーの Snort 2 バージョンと Snort 3 バージョンが同期されていないことを示しています。

Intrusion Policies Network Analysis Policies

Hide Snort 3 Sync status ⓘ

Search by Intrusion Policy, Description, or Base P

Intrusion Policy	Description
_Intrusion_Policy_1 → Snort 3 is out of sync with Snort 2. 2023-07-	

ステップ 3 オレンジ色の矢印をクリックします。

[Snort 2 から Snort 3 への同期の概要 (Snort 2 to Snort 3 Sync Summary)] ページに、Snort 2 から Snort 3 への同期が保留中であることが表示されます。

Snort 2 to Snort 3 Sync Summary ⓘ

This is a utility to synchronize Snort 2 policy configuration with Snort 3 version to start with a similar coverage.

- Snort 3 policy configuration is synched from Snort 2 version by the system when Firewall Management Center is upgraded from pre-7.0 version.
- Before upgrading a device to Snort 3, If changes are made in Snort 2 version, you can use this utility to have the latest synchronization from Snort 2 version to Snort 3 version so that you start with similar coverage.

Note: After moving to Snort 3, it is recommended that you manage the Snort 3 version of the policy independently and do not use this utility as a regular operation.

[Click here](#) to learn more.

Policy Name: _Intrusion_Policy_1

→ Snort 3 and Snort 2 Sync Pending 2023-07-09 21:16:51 EDT

Used by: 1 Access Control Policy | 1 Device

Re-Sync Close

ステップ 4 [再同期 (Re-Sync)] をクリックして同期を開始します。

(注) [再同期 (Re-Sync)] をクリックすると、snort2Lua ツールはルールを Snort 2 から Snort 3 に変換します。

[概要の詳細 (Summary Details)] セクションには、移行またはスキップされたルールが一覧表示されます。この使用例では、76 個のカスタム Snort 2 ルール、しきい値がある 17 個のルール、および同期プロセス中にスキップされた抑制付きの 15 個のルールがあります。カスタムルールを移行するには、次のステップに進みます。

Policy Name: **_Intrusion_Policy_1**

→ Snort 3 is partially in sync with Snort 2. 2023-08-01 05:42:52 EDT
Used by: 1 Access Control Policy | 0 Devices (Snort 2), 1 Devices (Snort 3)

Summary Details

Rule Overrides

- Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules.
- Rules migration skipped for 17 rules with threshold, 15 rules with suppression, as sync of Suppression and Threshold setting(s) are not supported.
- Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported. You can manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.

Download Summary Details

Overridden Advanced **Custom Rules**

The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. Use one of the following options to convert the custom rules manually:

しきい値と抑制を含むルールを移行するには、[ステップ 6](#)に進みます。

Policy Name: **_Intrusion_Policy_1**

→ Snort 3 is partially in sync with Snort 2. 2023-08-01 05:42:52 EDT
Used by: 1 Access Control Policy | 0 Devices (Snort 2), 1 Devices (Snort 3)

Summary Details

Rule Overrides

- Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules.
- Rules migration skipped for 17 rules with threshold, 15 rules with suppression, as sync of Suppression and Threshold setting(s) are not supported.
- Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported. You can manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.

Download Summary Details


Overridden Advanced **Custom Rules**

The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. Use one of the following options to convert the custom rules manually:



ステップ 5 76 個のカスタムルールを移行するには、次のいずれかの手順を実行します。

- [カスタムルール (Custom Rules)] タブで、[インポート (Import)] アイコンをクリックして、ローカルルールをポリシーの Snort 3 バージョンに変換して自動インポートします。

Overridden Advanced **Custom Rules**

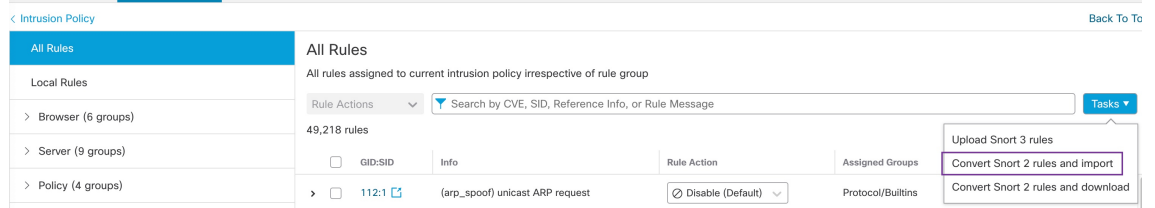
Convert the rules and auto-import them to the Snort 3 version of the policy 

OR

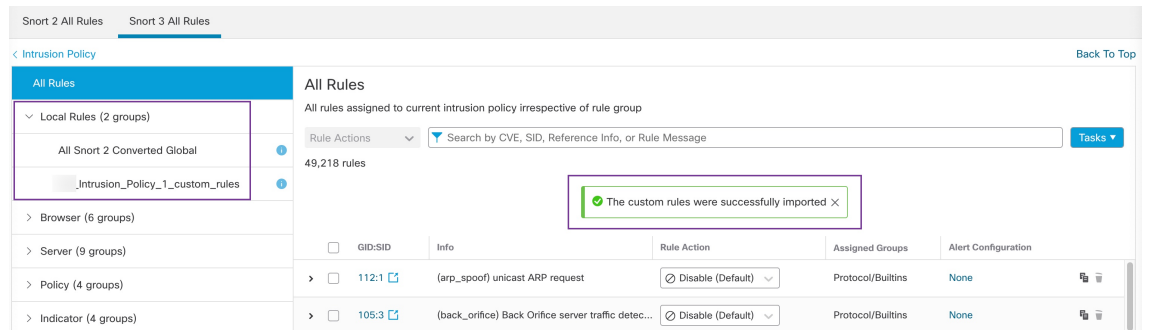
Download converted rules  You can upload the file after you have reviewed the converted rules 

ルールが正常にインポートされると、確認メッセージが表示されます。

- [オブジェクト (Objects)] > [侵入ルール (Intrusion Rules)] を選択し、[Snort 3のすべてのルール (Snort 3 All Rules)] をクリックします。
1. 左側のパネルで[ローカルルール (Local Rules)] をクリックして、ルールが移行されているかどうかを確認します。Snort 2 のカスタムルールは移行されていないことに注意してください。
 2. [タスク (Tasks)] ドロップダウンリストから、[Snort 2ルールの変換とインポート (Convert Snort 2 rules and import)] を選択します。

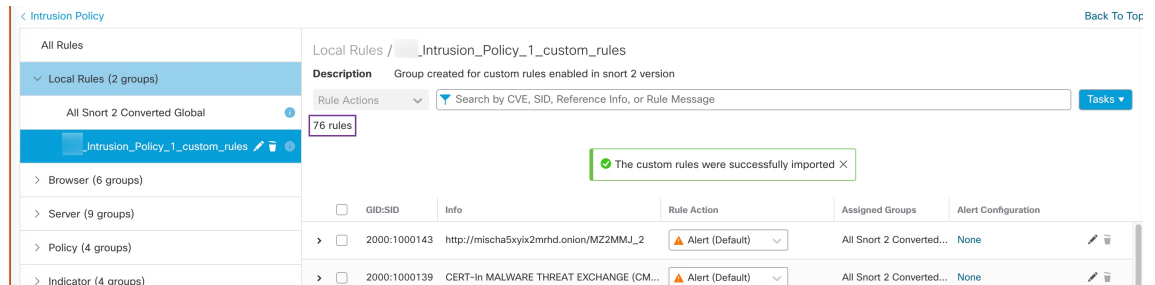


3. [OK] をクリック



新しく作成されたルールグループ ([すべてのSnort 2変換済みグローバル (All Snort 2 Converted Global)]) が、左側のパネルの [ローカルルール (Local Rules)] の下に作成されます。

次の図に示すように、76 個のカスタムルールがすべて移行されています。



または、前の手順で [Snort 2ルールの変換とダウンロード (Convert Snort 2 rules and download)] を選択して、ルールファイルをローカルに保存します。ダウンロードしたファイル内の変換後のルールを確認し、後で [Snort 3ルールのアップロード (Upload Snort 3 rules)] オプションを使用してファイルをアップロードできます。

ステップ 6 [サマリーの詳細のダウンロード (Download Summary Details)] リンクをクリックして、.txt 形式でルールをダウンロードします。

次に、表示されるサマリーの例を示します。

```
"id": "00505691-15DC-0ed3-0000-004294988561",
"name": "_Intrusion_Policy_1",
"type": "IntrusionPolicy",
"syncStatus": {
  "source": {
    "id": "bdce2d6a-1ebe-11ee-8e88-220032eb1fb5",
    "type": "IntrusionPolicy"
  },
  "status": "WARN",
  "description": "Migration is partially successful. Some of the rules are not copied to Snort3.",

  "timestamp": 1690883954814,
  "lastUser": {
    "name": "admin"
  },
  "details": [
    {
      "type": "Summary",
      "status": "INFO",
      "description": "Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules."
    },
    {
      "id":
"1:1000156=alert,1:1000114=alert,1:1000160=alert,1:1000135=alert,1:1000115=alert,1:1000118=alert,
1:1000092=alert,1:1000139=alert,1:1000123=alert,1:1000159=alert,1:1000149=disabled,1:1000167=alert,
1:1000133=alert,1:1000095=alert,1:1000143=alert,1:1000106=alert,1:1000153=alert,1:1000097=alert,1:1000141=alert,
1:1000148=alert,1:1000090=alert,1:1000119=alert,1:1000112=alert,1:1000138=alert,1:1000128=alert,1:1000132=alert,
1:1000134=alert,1:1000145=disabled,1:1000110=disabled,1:1000107=alert,1:1000163=alert,1:1000124=alert,1:1000125=alert,
1:1000094=alert,1:1000113=disabled,1:1000147=alert,1:1000161=alert,1:1000105=disabled,1:1000140=alert,1:1000111=alert,
1:1000102=alert,1:1000129=disabled,1:1000108=alert,1:1000144=disabled,1:1000088=alert,1:1000091=alert,1:1000131=alert,
1:1000157=alert,1:1000120=alert,1:1000126=alert,1:1000165=alert,1:1000146=alert,1:1000162=alert,1:1000116=alert,1:1000142=alert,
1:1000170=disabled,1:1000169=alert,1:1000104=alert,1:1000099=disabled,1:1000171=alert,1:1000093=alert,1:1000087=alert,1:1000100=alert,
1:1000137=alert,1:1000158=alert,1:1000103=alert,1:1000098=alert,1:1000127=disabled,1:1000130=alert,1:1000164=alert,1:1000089=alert,
1:1000109=alert,1:1000136=alert,1:1000117=alert,1:1000166=alert,1:1000168=alert",
      "type": "PolicyInfo",
      "description": "Corresponding Snort 2 policy overridden custom (local) rules."
    },
    {
      "type": "AssignedDevices",
```



```
"status": "INFO",
"description": "Snort3:0 , Snort2:0"
},
{
  "id": "122:6",
  "type": "Threshold",
  "status": "ERROR",
  "description": "PSNG_TCP_FILTERED_DECOY_PORTSCAN"
},
{
  "id": "122:15",
  "type": "Threshold",
  "status": "ERROR",
  "description": "PSNG_IP_PORTSWEEP_FILTERED"
},
{
  "id": "122:1",
  "type": "Threshold",
  "status": "ERROR",
  "description": "PSNG_TCP_PORTSCAN"
},
},
```

- ステップ 7** [閉じる (Close)] をクリックして、[同期の概要 (Sync Summary)] ダイアログボックスを閉じます。
- ステップ 8** ステータスが **ERROR** のルールを確認するには、[ポリシー (Policies)] > [侵入 (Intrusion)] を選択し、侵入ポリシーの [Snort 2] バージョンをクリックします。
- ステップ 9** [ポリシー情報 (Policy Information)] で、[ルール (Rules)] をクリックし、ルールをフィルタ処理します。たとえば、[フィルタ (Filter)] フィールドに **PSNG_TCP_PORTSCAN** と入力してルールを検索します。
- ステップ 10** ルールの詳細バージョンを表示するには、[詳細の表示 (Show Details)] をクリックします。
- ステップ 11** Snort 3 ルールガイドラインを使用して Snort 3 でルールを再度作成し、ファイルを .txt または .rules ファイルとして保存します。詳細については、www.snort3.org を参照してください。
- ステップ 12** ローカルで作成したカスタムルールがすべての Snort 3 ルールのリストにアップロードされます。「[Add Custom Rules to Rule Groups](#)」を参照してください。

次のタスク

設定変更を展開します。[設定変更の展開](#) を参照してください。

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。



- (注) このトピックでは、設定変更を展開する基本的な手順について説明します。手順を進める前に、最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Deploy Configuration Changes*」トピックを参照し、変更を展開する上での前提条件と影響を理解しておくことを強く推奨します。



注意 展開する際にリソースを要求すると、いくつかの packets 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。

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

[GUI] ページには、期限切れの設定を持ち、ステータスが [保留中 (Pending)] のデバイスのリストが表示されます。

- [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。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ーが表示されます。

(注) 削除されたポリシーおよびオブジェクトのユーザー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を示されます。


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。

- [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示します。
- [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。

ステップ 2 設定変更を展開するデバイスを特定して選択します。

- [検索 (Search)] : [検索 (Search)] ボックスのデバイス名、タイプ、ドメイン、グループ、またはステータスを検索します。
- [展開 (Expand)] : 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** ([展開矢印 (expand arrow)] アイコン [展開矢印 (expand arrow)] アイコン) をクリックします。

デバイスの横にあるチェックボックスをオンにすると、デバイスに加えられ、デバイスの下にリストされているすべての変更が展開のためにプッシュされます。ただし、**ポリシーの選択** ([ポリシーの選択 (policy selection)] アイコン [ポリシーの選択 (policy selection)] アイコン) を使用して展開する個々のポリシーや特定の設定を選択し、残りの変更は展開せずに保持することができます。

- (注)
- [インスペクションの中断 (Inspect Interruption)] 列のステータスに [あり (Yes)] と表示され、展開によって脅威に対する防御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る場合は、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 **インスペクションの中断** ([インスペクションの中断 (inspect interruption)] アイコン [インスペクションの中断 (inspect interruption)]  アイコン) で示されます。
 - インターフェイスグループ、セキュリティゾーン、またはオブジェクトに変更がある場合、影響を受けるデバイスは、Management Center で失効として表示されます。これらの変更が有効になるようにするには、これらのインターフェイスグループ、セキュリティゾーン、またはオブジェクトを含むポリシーも、これらの変更とともに展開する必要があります。影響を受けるポリシーは、Management Center の [プレビュー (Preview)] ページに失効として表示されます。

ステップ 3 [展開 (Deploy)] をクリックします。

ステップ 4 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。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

展開中に展開が失敗した場合、その障害がトラフィックに影響を与える可能性があります。ただし、特定の条件によって異なります。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。詳細については、最新バージョンの『Cisco Secure Firewall Management Center Configuration Guide』の「Deploy Configuration Changes」のトピックを参照してください。

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。