



Firewall Threat Defense のアップグレード

- [Firewall Threat Defense のアップグレード \(1 ページ\)](#)
- [無人モードでの Firewall Threat Defense のアップグレード \(5 ページ\)](#)
- [Firewall Threat Defense アップグレードのモニタリング \(7 ページ\)](#)
- [Firewall Threat Defense のアップグレードオプション \(8 ページ\)](#)
- [Firewall Threat Defense のアップグレードのトラブルシューティング \(10 ページ\)](#)
- [無応答および失敗した Firewall Threat Defense のアップグレード \(11 ページ\)](#)

Firewall Threat Defense のアップグレード

アップグレードウィザードで Firewall Threat Defense をアップグレードするには、次の手順を実行します。

続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。

アップグレードウィザードから移動しても進行状況は保持されます。他のユーザーは、すでに選択されているデバイスの新しいアップグレードワークフローを開始できません。ワークフローに戻るには、**[デバイス (Devices)]** > **[+さらに表示 (+ Show more)]** > **[アップグレード (Upgrade)]** > **[Threat Defense のアップグレード (Threat Defense Upgrade)]** を選択します。

アップグレードは、ウィザードを完了して **[アップグレードの開始 (Start Upgrade)]** をクリックするまで開始されません。準備状況の確認、アップグレードパッケージのコピー、アップグレードオプションの選択など、その時点までのすべての手順は、メンテナンスウィンドウ外で実行できます。



注意 アップグレード中は、設定の変更を展開しないでください。デバイスが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アップグレード中にデバイスが複数回再起動する場合があります。これは想定されている動作です。アップグレードに失敗する、デバイスが応答しないなど、アップグレードで問題が発生した場合には [無応答および失敗した Firewall Threat Defense のアップグレード \(11 ページ\)](#) を参照してください。

始める前に

アップグレードの準備が整っていることを確認します。

- ターゲットバージョンを実行できるかどうかを確認します：[互換性](#)
- アップグレードパスを計画します：[アップグレードパス](#)
- アップグレードのガイドラインを確認します：[アップグレードのガイドライン](#)
- インフラストラクチャとネットワークを確認します：[インフラストラクチャとネットワークの確認](#)
- 設定、タスク、および展開全体の正常性を確認します：[設定と展開の確認](#)
- バックアップを実行します：[バックアップ](#)
- 必要に応じてシャーシをアップグレードします：[Firewall Threat Defense 3100、4100、4200、9300 のアップグレード](#)

手順

- ステップ 1** クラウド提供型 Firewall Management Center で、**[管理 (Administration)] > [アップグレードと更新 (Upgrades & updates)] > [製品アップグレード (Product Upgrades)]** を選択します。
- [製品のアップグレード (Product Upgrades)] ページには、アップグレードを中心とした展開の概要（デバイスの数、それらが最後にアップグレードされた日時、進行中のアップグレードの有無など）が表示されます。利用可能なアップグレードが一覧表示されます（推奨リリースには特別なマークが付いています）。
- ステップ 2** （オプション）アップグレードパッケージを取得してクラウド提供型 Firewall Management Center に配置するか、内部サーバーに配置します。
- デバイスがインターネットから直接アップグレードパッケージを取得できる場合は、この手順をスキップします。他のオプションについては、[クラウド提供型 Firewall Management Center によるアップグレードパッケージの管理](#) を参照してください。
- ステップ 3** アップグレードウィザードを起動します。

ターゲットバージョンの横にある [アップグレード (Upgrade)] をクリックします。ドロップダウンメニューが表示されたら、[Threat Defense] を選択します。

ステップ 4 アップグレードするデバイスを選択します。

アップグレードするデバイスを選択しやすくするために、アップグレードウィザードではさまざまな便利な条件に基づいて検索やフィルタ処理を行うことができます。[続行準備完了 (Ready to proceed)] フィルタには、現在アップグレードの対象となっているすべての選択済みデバイスが表示されます。アップグレード手順を続行する前に、選択した番号が続行準備完了番号と一致している必要があります。一致しない場合は、[非候補 (Not candidates)] フィルタを使用して理由を確認します。不適格なデバイスを削除する必要はありません。自動的にアップグレードの対象から除外されます。デバイスクラスとハイアベイラビリティペアのメンバーは、同時にアップグレードする必要があります。



(注) デバイスを選択したら、無人モードを使用してアップグレードを自動的に準備および開始できます。アップグレードが完了したら、検証とアップグレード後のタスクを開始します。詳細については、「[無人モードでの Firewall Threat Defense のアップグレード \(5 ページ\)](#)」を参照してください。

ステップ 5 [アップグレードの準備 (Prepare for Upgrade)] をクリックすると、アップグレードパッケージのデバイスへのコピーと準備状況のチェックがすぐに開始されます。

アップグレードパッケージの入手先は、展開や以前の構成によって異なります。詳細については、「[デバイスへのアップグレードパッケージのコピー](#)」を参照してください。

準備状況チェックの多くは現在のデバイスヘルスに基づいて行われますが、現在バージョン 7.6.x 以前を実行しているデバイスでのチェックには時間がかかる場合があります。すべてのチェックに合格すると、アップグレードが失敗する可能性が大幅に減少します。チェックの結果、解決できない問題が見つかった場合は、アップグレードを開始しないでください。Cisco TAC の指示がある場合にのみ、チェックを無効にします。詳細については、「[設定と展開の確認](#)」を参照してください。



(注) このプロセスでは、無人モードの準備専用オプションを利用します。つまり、ウィザードがパッケージのコピーと準備状況の確認をしている間、明示的に開始していない場合でも、無人モードの実行に関するメッセージが表示されることがあります。

ステップ 6 (オプション) [詳細設定 (Advanced settings)] をクリックして、アップグレードオプションを選択します。

これらのオプションを無効にできる理由については、[Firewall Threat Defense のアップグレードオプション \(8 ページ\)](#) を参照してください。

ステップ 7 [アップグレードの開始 (Start upgrade)] をクリックして、選択を確定します。

アップグレード中、デバイスはメンテナンス モードで稼働します。アップグレード時のトラフィック処理の詳細については、「[トラフィック フローとインスペクション](#)」を参照してください。

ステップ 8 アップグレードをモニターします。

ウィザードには、全体的なアップグレードの進行状況が表示されます。その他のアップグレード モニタリング オプション（高可用性アップグレードの監視に関する特別な留意事項を含む）については、「[Firewall Threat Defense アップグレードのモニタリング（7 ページ）](#)」を参照してください。

ステップ 9 成功したことを確認します。

アップグレードが完了したら、**[デバイス (Devices)] > [デバイス管理 (Device Management)]** で成功を確認します。

ステップ 10 （オプション）高可用性展開またはクラスタ化された展開では、デバイスのロールを調べます。

アップグレードプロセスは、常にスタンバイユニットまたはデータノードをアップグレードするようにデバイスのロールを切り替えます。デバイスをアップグレード前のロールに戻すことはありません。特定のデバイスに優先するロールがある場合は、それらの変更を今すぐ行ってください。

ステップ 11 侵入ルールおよび脆弱性データベース (VDB) を更新します。

[管理 (Administration)] > [アップグレードと更新 (Upgrades & updates)] > [コンテンツの更新 (Content Updates)] を選択して現在インストールされているバージョンを確認し、すべての更新を実行します。

アップグレードによってこれらのコンポーネントが更新されることがよくありますが、より新しいコンポーネントが利用できる可能性があります。シスコ サポートおよびダウンロードサイトに新しいバージョンがある場合は、それをインストールします。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 12 アップグレード後に必要な構成変更があれば、実行します。**ステップ 13** アップグレードしたデバイスに構成を再度展開します。

Snort は、通常、アップグレード後の最初の展開時に再起動されます。Snort プロセスを再起動すると、高可用性またはクラスタリングの構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。詳細については、[設定展開時のトラフィックフローとインスペクション](#) を参照してください。

展開する前に、アップグレードによって加えられた変更（およびアップグレード後に加えた変更）を確認できます。

- ワークフローをクリアしていない場合は、ウィザードに戻ることができます。**[デバイス (Devices)] > [+さらに表示 (+ Show more)] > [アップグレード (Upgrade)] > [Threat Defenseのアップグレード (Threat Defense Upgrade)]** を選択し、各デバイスの横にある **[構成変更 (Configuration Changes)]** をクリックします。
- ワークフローをクリアした場合、または複数のデバイスの変更レポートをすばやく生成する場合は、**[高度な展開 (Advanced Deploy)]** ページを使用します。**[展開 (Deploy)] > [高度な展開 (Advanced Deploy)]** を選択し、アップグレードしたデバイスを選択して、**[保留中の変更レポート (Pending Changes Reports)]** をクリックします。レポートの生成が完了したら、メッセージセンターの **[タスク (Tasks)]** タブからレポートをダウンロードできます。

次のタスク

- (オプション) **[アップグレード情報のクリア (Clear Upgrade Information)]** をクリックして、ウィザードをクリアします。これを行うまで、ページには、実行したばかりのアップグレードに関する詳細が引き続き表示されます。ウィザードをクリアしたら、**[デバイス管理 (Device Management)]** ページの **[アップグレード (Upgrade)]** タブを使用して、前回のアップグレード情報を確認します。また、**[高度な展開 (Advanced Deploy)]** 画面で設定の変更を確認します。
- Firepower 4100/9300 の場合、アップグレードした論理デバイスごとに新しい Firewall Threat Defense スタートアップバージョンを設定します。Cisco Secure Firewall Chassis Manager の **[論理デバイス (Logical Devices)]** タブ、または `set startup-version FXOS` コマンドを使用できます。これにより、アップグレード後のバックアップから論理デバイスを復元する必要がある場合に、バックアップとスタートアップのバージョンが一致します。詳細については、『[Cisco Firepower 4100/9300 FXOS Secure Firewall Chassis Manager 設定ガイド](#)』または『[Cisco Firepower 4100/9300 FXOS Command Reference](#)』の「*Image Management*」の章を参照してください。
- 再度バックアップします：[バックアップ](#)

無人モードでの Firewall Threat Defense のアップグレード

Firewall Threat Defense アップグレードウィザードには、オプションの無人モードがあります。ウィザードを開始して、アップグレードするターゲットバージョンとデバイスを選択し、アップグレードオプションを選択したら、その場を離れます。ログアウトしたり、ブラウザを閉じたりすることもできます。システムが自動的にアップグレードパッケージをデバイスにコピーし、準備状況をチェックし、指定されている場合はアップグレードを開始します。アップグレードが完了したら、検証とアップグレード後のタスクを開始します。



- (注) 通常 (有人) アップグレードにおいて、**[アップグレードの準備 (Prepare for upgrade)]** をクリックすると、無人モードに関するメッセージが表示される場合があります。これは、ウィザードがパッケージをコピーして準備状況を確認する際に、無人モードの準備専用機能を使用するためです。

表 1: 無人モードでの Firewall Threat Defense のアップグレード

目的	ウィザードで実行
無人アップグレードを開始します。	アップグレードするターゲットバージョンとデバイスを選択したら、 [無人モード (Unattended mode)] > [開始 (Start)] を選択します。 無人モードのオプションについては、次の表を参照してください。

目的	ウィザードで実行
コピーフェーズとチェックフェーズの間に無人アップグレードを一時停止します。	[無人モード (Unattended mode)] > [停止 (Stop)] を選択します。 コピーフェーズとチェックフェーズの間に無人モードを一時停止して再開できます。ただし、無人モードを一時停止しても、進行中のタスクは停止しません。開始されたコピーとチェックは完了するまで実行されます。手動アップグレードアクションを実行するには、無人モードを一時停止する必要があります。 実際のデバイスのアップグレードが開始されると、無人モードを停止してキャンセルすることはできません。代わりに、[デバイス管理 (Device Management)] ページの [アップグレード (Upgrade)] タブからアクセスできる [アップグレードステータス (Upgrade Status)] ポップアップを使用します。
コピーフェーズとチェックフェーズの間に無人アップグレードを監視します。	[無人モード (Unattended mode)] > [ステータスの表示 (View status)] を選択します。 実際のデバイスのアップグレードが開始されたら、「Firewall Threat Defense アップグレードのモニタリング (7 ページ)」を参照してください。

無人モードのオプション

これらのオプションは無人アップグレードに適用され、デフォルトでは無効になっています。

表 2: 無人モードのオプション

オプション	有効にするタイミング	詳細
デバイスの準備が完了したら、アップグレードを開始します。	アップグレードの時期を慎重に判断する必要がない場合。	アップグレードを開始するとメンテナンスウィンドウが必要になりますが、ステージングには必要ありません。システムはアップグレードパッケージをデバイスにコピーし、準備状況をチェックしますが、実際のアップグレードは実行しません。 このオプションを無効にして無人アップグレードを実行することは、メインのアップグレードウィザードで [アップグレードの準備 (Prepare for Upgrade)] をクリックするのと同じであることに注意してください。このため、明示的に開始していない場合でも、無人モードに関するメッセージが表示されることがあります。

オプション	有効にするタイミング	詳細
すでに合格したデバイスの準備状況チェックを再実行します。	デバイスの準備状況が不明な場合。	合格してから24時間を過ぎたデバイスや、デバイスが最後に合格した後に変更を加えた場合は、チェックを再実行することを推奨します。 一部のデバイスで準備状況チェックを最近実行したため、再度実行する必要がない場合があります。

Firewall Threat Defense アップグレードのモニタリング



注意 アップグレード中は、設定の変更を展開しないでください。デバイスが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。アップグレード中にデバイスが複数回再起動する場合があります。これは想定されている動作です。アップグレードに失敗する、デバイスが応答しないなど、アップグレードで問題が発生した場合には [無応答および失敗した Firewall Threat Defense のアップグレード \(11 ページ\)](#) を参照してください。

デバイスおよびシャーシアップグレードのモニタリング

Firewall Threat Defense およびシャーシアップグレードのモニタリングに使用できる機能は次のとおりです。

- ワークフローをクリアしていない場合、または新しいワークフローを開始していない場合は、アップグレードウィザードの [アップグレードステータス (Upgrade Status)] 画面 ([**デバイス (Devices)**] > [**Threat Defense アップグレード/シャーシのアップグレード (Threat Defense Upgrade/Chassis Upgrade)**])。詳細なステータスについては、確認するデバイスの横にある [詳細ステータス (Detailed Status)] をクリックしてください。
- [デバイス管理 (Device Management)] ページ ([**デバイス (Devices)**] > [**デバイス管理 (Device Management)**]) の [アップグレード (Upgrade)] タブ。詳細なステータスについては、確認するデバイスの横にある [詳細の表示 (View Details)] をクリックしてください。
- メッセージセンターの [アップグレード (Upgrades)] タブ。

アップグレード中の高可用性状態

Firewall Threat Defense 高可用性ペアの場合、最初にスタンバイデバイスがアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレード中に、システムは次の不整合状態をレポートできます。

- [アップグレードの開始 (Start Upgrade)] をクリックすると、メッセージセンターとアップグレードウィザードはユニットをその状態に関連付けます。つまり、フェールオーバーが発生し、スタンバイのみをアップグレードしている場合でも、「スタンバイ」、次に「アクティブ」のアップグレードがレポートされます。
- デバイス管理ページには、ユニットの現在の正しい状態が常に表示されます。この状態は、メッセージセンターまたはウィザードで表示される元の状態とは異なる場合があります。

高可用性アップグレードの成功

Firewall Threat Defense 高可用性ペアの場合、メッセージセンターは、個別のタスクで各ユニットのアップグレードの成功をレポートします。



重要 メッセージセンターの表示に関係なく、両方のデバイスのアップグレードが完了するまで、高可用性ペアに設定を再展開しないでください。

Firewall Threat Defense のアップグレードオプション

アップグレードオプションを選択するには、アップグレードウィザードで [詳細設定 (Advanced settings)] をクリックするか、無人モードを開始します。

一般的なアップグレードオプション

これらのオプションはすべてのアップグレードに適用され、デフォルトで有効になっています。

表 3: 一般的な アップグレードオプション

オプション	無効にする場合	詳細
互換性と準備状況のチェック 互換性と準備状況のチェックに合格する必要があります。	Cisco TAC の指示があった場合。	このオプションを無効にすると、互換性と準備状況のチェックに合格せずにアップグレードを開始できます。ただし、推奨されません。すべてのチェックに合格すると、アップグレードが失敗する可能性が大幅に減少します。チェックの結果、解決できない問題が見つかった場合は、アップグレードを開始しないでください。

オプション	無効にする場合	詳細
アップグレードの失敗 アップグレードに失敗すると自動的にキャンセルされ、1つ前のバージョンにロールバックされます。	失敗したアップグレードを手動で（自動ではなく）キャンセルし、再試行する場合。	オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。高可用性またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。 パッチまたはホットフィックスではサポートされていません。
復元の有効化 アップグレード成功後の復元を可能にします。	時間とディスク容量を節約する場合。	ほとんどの Firewall Threat Defense のアップグレードは、30 日間は元に戻すことができます。 復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなくアップグレードも元に戻されます。 コンテナインスタンス、パッチ、またはホットフィックスではサポートされていません。
Snortのアップグレード 対象デバイスを Snort 2からSnort 3に変換します。	Snort 3 のアップグレードを防ぐ場合。	バージョン 7.2 ～ 7.6 へのアップグレードでは、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。 バージョン 7.3 以降へのアップグレードでは、このオプションを無効にすることはできません。個々のデバイスを元に戻すことはできますが、Snort 2 はバージョン 7.7 で非推奨になったため、Firewall Threat Defense はアップグレードできなくなります。 カスタム侵入またはネットワーク分析ポリシーを使用しているために不適格なデバイスの場合、手動で Snort 3 にアップグレードします。移行のサポートについては、お使いのバージョンの Custom Snort 3 Intrusion Policies for Access Control を参照してください。

無人モードのオプション

これらのオプションは無人アップグレードにのみ適用され、デフォルトでは無効になっています。「[無人モードでの Firewall Threat Defense のアップグレード（5 ページ）](#)」を参照してください。

表 4: 無人モードのオプション

オプション	有効にするタイミング	詳細
デバイスの準備が完了したら、アップグレードを開始します。	アップグレードの時期を慎重に判断する必要がない場合。	アップグレードを開始するとメンテナンスウィンドウが必要になりますが、ステージングには必要ありません。システムはアップグレードパッケージをデバイスにコピーし、準備状況をチェックしますが、実際のアップグレードは実行しません。 このオプションを無効にして無人アップグレードを実行することは、メインのアップグレードウィザードで[アップグレードの準備 (Prepare for Upgrade)]をクリックするのと同じであることに注意してください。このため、明示的に開始していない場合でも、無人モードに関するメッセージが表示されることがあります。
すでに合格したデバイスの準備状況チェックを再実行します。	デバイスの準備状況が不明な場合。	合格してから24時間を過ぎたデバイスや、デバイスが最後に合格した後に変更を加えた場合は、チェックを再実行することを推奨します。 一部のデバイスで準備状況チェックを最近実行したため、再度実行する必要がない場合があります。

Firewall Threat Defense のアップグレードのトラブルシューティング

表 5: Threat Defense のアップグレードのトラブルシューティング

Issue	解決方法
ターゲットバージョンの [アップグレード (Upgrade)] ボタンがない。	次のいずれかを行います。 • 現在、そのバージョンにアップグレードできるものはありません。 • インターネットにアクセスできる対象デバイスがありません。パッケージをクラウド提供型 Firewall Management Center にアップロードするか、内部サーバーを設定します。「クラウド提供型 Firewall Management Center によるアップグレードパッケージの管理」を参照してください。

Issue	解決方法
アップグレードウィザードにデバイスが一覧表示されない。	[デバイス (Devices)] > [+さらに表示 (+ Show more)] > [アップグレード (Upgrade)] > [Threat Defenseのアップグレード (Threat Defense Upgrade)] から直接ウィザードにアクセスした場合は、ターゲットバージョンが選択されていないため、ワークフローが空白になることがあります。開始するには、[アップグレード先 (Upgrade to)] メニューからターゲットバージョンを選択します。そのバージョンにアップグレードできるデバイスが表示されます。
ターゲットバージョンが [アップグレード先 (Upgrade to)] メニューに表示されていません。	[アップグレード先 (Upgrade to)] メニューの選択肢は、クラウド提供型 Firewall Management Center のデバイス アップグレード パッケージに対応しているほか、サポートサイトで利用可能なアップグレードも含まれています。必要なアップグレードが表示されない場合は、対象となるデバイスがない可能性があります。または、パッケージの自動アップロード (ホットフィックスなど) が必要な場合があります。アップグレードパッケージをアップロードするには、[アップグレードパッケージの管理 (Manage Upgrade Packages)] をクリックしてください。「 クラウド提供型 Firewall Management Center によるアップグレードパッケージの管理 」を参照してください。
ターゲットバージョンが選択されているのに、アップグレードウィザードにデバイスが一覧表示されません。	そのバージョンにアップグレードできるデバイスがありません。それでもデバイスがここに表示される必要があると思われる場合は、ユーザーロールによって、デバイスの管理が（そのため、アップグレードも）禁止されている可能性があります。
メッセージセンターでのブルーニングデーモンエラー。	主に、バージョン 7.6.x 以前を実行しているデバイスで、準備状況チェックの完了後 10 分以内にアップグレードを開始しなかった場合に発生します。その場合でも、これらのメッセージを無視してアップグレードを続行できます。 エラーの詳細は次のとおりです。Process Status - device_name. The pruning daemon exited n time(s).

無応答および失敗した Firewall Threat Defense のアップグレード

次の表に、応答せずに失敗した Firewall Threat Defense アップグレードの障害対応情報を示します。シャーシのアップグレードの問題については、Cisco TAC にお問い合わせください。



注意 システムが非アクティブに見えても、アップグレード中のどの時点でも再起動またはシャットダウンしないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。

表 6: 無応答および失敗した Firewall Threat Defense のアップグレード

Issue	解決方法
デバイスに到達できない。	デバイスは、アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。アップグレードする前に、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。 デバイスを経由せずに クラウド提供型 Firewall Management Center の管理インターフェイスにアクセスできる必要もあります。
アップグレードまたはパッチがハングアップしているように見える/デバイスが非アクティブになっているように見える。	クラウド提供型 Firewall Management Center でのデバイス アップグレード ステータスの更新が停止しているものの、アップグレードの失敗のレポートがない場合は、アップグレードのキャンセルを試みることができます。以下を参照してください。キャンセルできない場合やキャンセルが機能しない場合は、Cisco TAC にお問い合わせください。 ヒント： エキスパートモードおよび <code>tail</code> または <code>tailf</code> (<code>tail /ngfw/var/log/sf/update.status</code>) を使用して、デバイス自体のアップグレードログをモニターできます。
アップグレードが失敗する。	アップグレードが失敗する場合は、次の手順を実行してください。 • デバイスがアップグレード前の状態に戻っている（自動キャンセルが有効になっている）場合は、問題を修正して最初から再試行します。 • デバイスが引き続きメンテナンスモードである場合は、問題を修正してアップグレードを再開します。または、キャンセルし、後で再試行します。 再試行またはキャンセルできない場合、または問題が解消されない場合は、Cisco TAC にお問い合わせください。
パッチが失敗する。	進行中のパッチまたは失敗したパッチはキャンセルできません。ただし、パッチが早い段階（検証段階など）で失敗した場合は、デバイスが正常に稼働しつづける可能性があります。単純に、問題を修正し、再試行してください。 デバイスがメンテナンスモードになった後にパッチが失敗した場合は、アンインストールが存在するか確認します。アンインストールが存在する場合は、それを実行して失敗したパッチを削除できます。「Firewall Threat Defense のパッチのアンインストール」を参照してください。アンインストールが完了したら、問題を修正して再試行できます。 アンインストールが存在しない場合、アンインストールが失敗する場合、または問題が解決しない場合は、Cisco TAC にお問い合わせください。

Issue	解決方法
クラスター化されたデバイスのアップグレードが失敗し、アップグレードを再試行する代わりに再イメージ化する必要があります。	クラスターノードのアップグレードが失敗し、ノードの再イメージ化を選択した場合は、クラスターに追加する前に、現在のバージョンの制御ノードに再イメージ化します。アップグレードが失敗した時期と方法に応じて、制御ノードの現在のバージョンは古いバージョンまたはターゲットバージョンになります。 アップグレード中の一時的な場合を除き、バージョンが混在するクラスターはサポートされていません。バージョンが混在するクラスターを意図的に作成すると、停止が発生する可能性があります。 ヒント 障害が発生したノードをクラスターから削除し、ターゲットバージョンに再イメージ化します。クラスターの残りの部分をターゲットバージョンにアップグレードしてから、再イメージ化されたノードを追加します。
アップグレードをキャンセルしたい。	キャンセルすると、デバイスはアップグレード前の状態に戻ります。失敗したアップグレードや進行中のアップグレードは、[デバイス管理 (Device Management)] ページの [アップグレード (Upgrade)] タブからアクセスできる [アップグレードステータス (Upgrade Status)] ポップアップでキャンセルできます。パッチはキャンセルできません。 キャンセルできない場合やキャンセルが機能しない場合は、Cisco TAC にお問い合わせください。
失敗したアップグレードを再試行 (再開) したい。	[デバイス管理 (Device Management)] ページの [アップグレード (Upgrade)] タブからアクセスできる [アップグレードステータス (Upgrade Status)] ポップアップでアップグレードを再開できます。 問題が解消されない場合は、Cisco TAC にお問い合わせください。
アップグレードが失敗した場合の動作を変更したい。	アップグレードプロセスの一部は、失敗した場合の動作の選択です。これは、[アップグレードに失敗すると自動的にキャンセルされる... (Automatically cancel on upgrade failure...)] (自動キャンセル) オプションで実行されます。 • [自動キャンセルが有効 (Auto-cancel enabled)] (デフォルト) : アップグレードが失敗すると、アップグレードがキャンセルされ、デバイスは自動的にアップグレード前の状態に復元されます。これにより、再グループ化して再試行しながら、可能な限り迅速に通常の操作に戻ります。 • [自動キャンセルが無効 (Auto-cancel disabled)] : アップグレードが失敗した場合、デバイスはそのままになります。これにより、問題を修正し、アップグレードを再開することができます。 高可用性およびクラスターデバイスでは、自動キャンセルは各デバイスに個別に適用されます。つまり、1つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

無応答および失敗した Firewall Threat Defense のアップグレード

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。