Threat Defense のアップグレード

Threat Defense のアップグレード

Threat Defense をアップグレードするには、次の手順を使用します。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。あるデバイスが 1 つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。

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。（例外：CAC でログインしている場合、ログアウトしてから 24 時間後に進行状況がクリアされます）。ワークフローに戻るには、**[デバイス（Devices）] > [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、アップグレード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。アップグレードパッケージのダウンロード、それらのデバイスへのコピー、準備状況チェックの実行、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。アップグレード中およびアップグレード後の最初の展開時におけるトラフィック処理については（通常は Snort が再起動されます）、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。

Caution 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。システム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 Threat Defense のアップグレードを参照してください。

Before you begin

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：Secure Firewall 3100 または Firepower 4100/9300 シャーシのアップグレード

Procedure

ステップ 1 Management Center で、**システム**（⚙）> **[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。

ステップ 2 デバイス アップグレード パッケージを Management Center に取得します。

アップグレードパッケージを管理対象デバイスにコピーする前に、パッケージを Management Center またはデバイスがアクセスできる内部サーバーにアップロードする必要があります。

[製品のアップグレード（Product Upgrades）]ページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。ほとんどの場合、必要なアップグレードパッケージまたはバージョンの横にある [ダウンロード（Download）] をクリックするだけで取得できます。

詳細については、Management Center でのアップグレードパッケージの管理およびアップグレードパッケージのトラブルシューティング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。

Threat Defense アップグレードウィザードが表示されます。これには、左側の [デバイスの選択（Device Selection）] と右側の [デバイスの詳細（Device Details）] の 2 つのペインがあります。[デバイスの選択（Device Selection）] ペインでデバイスリンク（「`4 つのデバイス（4 devices）`」 など）をクリックして、[デバイスの詳細（Device Details）] を表示します。ターゲットバージョンは、[アップグレード先

（Upgrade to）] メニューで事前に選択されています。システムは、どのデバイスをそのバージョンにアップグレードできるかを判断し、[デバイスの詳細（Device Details）] ペインに表示します。

ステップ 4 アップグレードするデバイスを選択します。

[デバイスの詳細（Device Details）] ペインで、アップグレードするデバイスを選択し、[選択に追加（Add to Selection）] をクリックします。

[デバイスの選択（Device Selection）] ペインのデバイスリンクを使用すると、選択したデバイス、残りのアップグレード候補、不適格なデバイス（理由付き）、アップグレードパッケージが必要なデバイスなどの間で [デバイスの詳細（Device Details）] ペインを切り替えることができます。選択からデバイスを削除したり、[リセット（Reset）] をクリックしてデバイスの選択をクリアし、最初からやり直すことができます。不適格なデバイスを削除する必要はありません。それらはアップグレードから自動的に除外されます。デバイスクラスタ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。

Tip
アップグレードするデバイスを選択したら、無人モード（**[無人モード（Unattended Mode）]** > **[開始（Start）]**）でアップグレードを開始できます。いくつかのオプションを指定すると、システムは自動的に必要なアップグレードパッケージをデバイスにコピーし、互換性チェックと準備状況チェックを実行して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。詳細については、「無人モードでの Threat Defense のアップグレード, on page 7」を参照してください。

ステップ 5 アップグレードパッケージをデバイスにコピーします。

[アップグレードパッケージのコピー（Copy Upgrade Package）] をクリックし、転送が完了するまで待ちます。 の場合、シャーシをアップグレードしていると、アップグレードパッケージは、通常、すでにデバイス上に存在しています（削除していない場合）。

ステップ 6 [次へ（Next）] をクリックして互換性および準備状況チェックを実行します。

互換性やその他のクイック事前チェックは自動的に実行されます。たとえば、設定を展開する必要がある場合、すぐにアラートが表示されます。他のチェックには、より長い時間がかかります。これらを開始するには、[準備状況チェックの実行（Run Readiness Check）] をクリックします。

準備状況チェックの実行中は、デバイスに変更を展開したり、手動で再起動またはシャットダウンしたりしないでください。[互換性と準備状況のチェックに合格することを必須にする（Require passing compatibility and readiness checks option）] オプションを無効にするとチェックをスキップできますが、推奨しません。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。

ステップ 7 [次へ（Next）] 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使用すると、成功したアップグレードと失敗したアップグレードの両方から元に戻し、トラブルシューティングファイルを生成し、Snort をアップグレードすることができます。これらのオプションを無効にできる理由については、Threat Defense のアップグレードオプション, on page 5を参照してください。

ステップ 8 アップグレードの準備ができていることを再確認します。

以前に実行した設定と展開の正常性チェックを再確認することをお勧めします（設定と展開の確認）。

ステップ 9 [Start Upgrade] をクリックし、アップグレードして、デバイスを再起動することを確認します。

ウィザードにアップグレードの全体的な進行状況が表示されます。メッセージセンターでもアップグレードの進行状況をモニターできます。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）][詳細ステータス（Detailed Status）]** をクリックしてください。この詳細なステータスは、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブでも確認できます。

高可用性デバイスの場合、[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によってユニットが高可用性状態と関連付けられることに注意してください。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（Device Management）] ページには、ユニットの現在の正しい高可用性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。

Caution
高可用性デバイスの場合、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報告します。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。

Tip
失敗したアップグレードまたは進行中のアップグレードをキャンセルする必要がある場合や、失敗したアップグレードを再試行する必要がある場合は、詳細なステータスのポップアップから実行します。ワークフローをクリアしていない場合は、ウィザードに戻って詳細なステータスを表示できます。クリア済みの場合は、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブを使用してください。Threat Defense CLI を使用することもできます。

ステップ 10 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）]** を選択し、アップグレードしたデバイスのソフトウェアバージョンが正しいことを確認します。

ステップ 11 （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 12 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

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で利用可能なコンポーネントが現在実行中のバージョンより新しい場合は、新しいバージョン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 13 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 14 アップグレードしたデバイスに構成を再度展開します。

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）]**>**[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。

What to do next

- （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、管理対象デバイスに関する最後のアップグレードの情報を確認し、[高度な展開（Advanced Deploy）] 画面で設定の変更を確認します。
- 再度バックアップします：バックアップ

Threat Defense のアップグレードオプション

表 *1 : Threat Defense* の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。
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。

オプション	無効にする場合	詳細
アップグレードを開始する前にトラブルシューティング ファイルを生成します。	時間とディスク容量を節約する場合。	バージョン 7.3 以降へのアップグレードでは、アップグレード前のトラブルシューティング ファイルの自動生成をスキップできます。 脅威防御デバイスのトラブルシューティング ファイルを手動で生成するには、**システム**（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択し、左側のパネルでデバイスをクリックし、[システムおよびトラブルシューティングの詳細を表示（View System & Troubleshoot Details）]、[トラブルシューティング ファイルの生成（Generate Troubleshooting Files）] をクリックします。
Snort 2 を Snort 3 にアップグレードします。	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 は将来のリリースで非推奨になるため、今すぐ使用を停止することを強く推奨します。 カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスがアップグレード対象外になる場合は、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。
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。	7.1 以降へのアップグレードでは、Threat Defense のアップグレードを元に戻す期間が 30 日間あります。 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。

無人モードでの Threat Defense のアップグレード

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。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、いくつかのアップグレードオプションを指定して、その場から離れるだけです。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。

無人アップグレードを使用すると、システムは自動的に必要なアップグレードパッケージをデバイスにコピーし、互換性チェックと準備状況チェックを実行してアップグレードを開始します。ウィザードを手動でステップ実行する場合と同様に、アップグレードのステージに「合格」しなかったデバイス（たとえば、チェックの失敗）は、次のステージに含まれません。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。

表 *2:*

目的	操作手順
無人アップグレードを開始します。	Threat Defense アップグレードウィザードで、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ます。**[無人モード（Unattended Mode）] > [開始（Start）]** を選択し、アップグレードオプションを選択して、もう一度 [開始（Start）] をクリックします。
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一時停止します。	Threat Defense アップグレードウィザードで、**[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。
無人アップグレードをモニターします。	無人アップグレードをモニターする方法は、次のとおりです。 • コピーおよび確認ステータス：**[無人モード（Unattended Mode）] > [ステータスの表示（View Status）]** • 全体的なアップグレードステータス：メッセージセンター • 詳細なアップグレードステータス：[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

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。