復元またはアンインストール

アップグレードまたはパッチに成功したにもかかわらず、システムが期待どおりに機能しない場合は、復元またはアンインストールが可能な場合があります。

- 復元とアンインストール （1 ページ）
- Threat Defense アップグレードの復元 （2 ページ）
- Threat Defense パッチのアンインストール （7 ページ）

復元とアンインストール

復元するかアンインストールするかは、リリースタイプによって異なります。

表 *1*：復元とアンインストール

	[元に戻す（Revert）]	アンインストール
リリース	バージョン 7.2 以降へのメジャーおよびメンテナンスアップグレード。	パッチ。
詳細	ソフトウェアは、最後のメジャーアップグレードまたはメンテナンスアップグレード（スナップショット）の直前の状態に戻ります。詳細については、元に戻る設定 （4 ページ）を参照してください。	ソフトウェアをパッチを適用したバージョンに戻します。設定は変更されません。
制約事項	コンテナインスタンスではサポートされていません。復元を妨げるその他のシナリオについては、「復元ガイドライン （2 ページ）」を参照してください。	アンインストールがサポートされていない、または推奨されていないシナリオについては、「アンインストールのガイドライン （7 ページ）」を参照してください。

	[元に戻す（Revert）]	アンインストール
復元/アンインストール元	**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を使用して Threat Defense アップグレードを元に戻します。	デバイスでエキスパートモード（CLI）を使用して Threat Defense パッチをアンインストールします。

例：復元とアンインストール

パッチ適用後に元に戻すと、パッチも削除されます。次に例を示します。

1. Threat Defense をバージョン 7.2.0 から 7.2.5 にアップグレードします。
2. バージョン 7.2.5 → 7.2.5.2 にパッチを適用します。
3. 次のいずれかを実行できます。
   - パッチをアンインストールして、バージョン 7.2.5 に戻します。

     これにより、パッチのみが削除されます。
   - アップグレードを元に戻して、バージョン 7.2.0 に戻します。

     これにより、パッチとメンテナンスリリースが削除されます。

Threat Defense アップグレードの復元

復元ガイドライン

このセクションでは、復元の一般的なガイドラインについて説明します。バージョン固有の復元の問題を確認するには、リリースノート「https://cisco.com/go/fmc-ftd-release-notes-74」のアップグレードガイドラインを参照してください。

高可用性またはクラスタ化デバイスの復元

Management Center Web インターフェイスを使用して Threat Defense を復元する場合、個々の高可用性ユニットまたはクラスタ化されたノードを選択することはできません。

すべてのユニットやノードを同時に復元させたほうが、復元が成功する可能性が高くなります。Management Center から復元を開始すると、システムは自動的にこれを実行します。デバイス CLI を使用する必要がある場合は、これを手動で行います。すべてのユニットとノードでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。同時復元とは、すべてのデバイスがスタンドアロンであるかのように、トラフィックフローと検査の中断がインターフェイスの設定のみに依存することを意味します。

完全または部分的にアップグレードされたグループで復元がサポートされていることに注意してください。部分的にアップグレードされたグループの場合、システムはアップグレードされ

たユニットとノードからのみアップグレードを削除します。元に戻しても高可用性やクラスタが壊れることはありませんが、グループを分解してその新しいスタンドアロンデバイスを復元することができます。

Firepower 4100/9300 の復元

復元しても FXOS はダウングレードされません。

Firepower 4100/9300 の場合、Threat Defense のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。Threat Defense の以前のバージョンに戻った後、推奨されていないバージョンの FXOS（新しすぎる）を実行している可能性があります。

新しいバージョンの FXOS は旧バージョンの Threat Defense と下位互換性がありますが、シスコでは推奨の組み合わせについて拡張テストを実施しています。FXOS を手動ではダウングレードできないため、このような状況下で推奨の組み合わせを稼働するには、完全な再イメージ化が必要になります。

復元を妨げるシナリオ

次のいずれかの状況で復元を試みると、システムはエラーを表示します。

表 *2*：復元を妨げるシナリオ

シナリオ	解決方法
次の理由により、スナップショットを復元することはできません。 • デバイスをアップグレードしたときに、復元を有効にしていませんでした。 • Management Center またはデバイスからスナップショットを削除したか、スナップショットの期限が切れました。 • 別の Management Center でデバイスをアップグレードしました。 • 現在実行しているバージョンに戻しました（連続して複数の復元を実行しようとしています）。	なし。 復元スナップショットは、Management Center とデバイスに 30 日間保存され、その後自動的に削除され、復元できなくなります。ディスク容量を節約するためにどのアプライアンスからでもスナップショットを手動で削除できますが、復元の機能が失われます。 システムは1つのスナップショットのみを保存します。複数回復元することはできません。つまり、次のとおりです。 • サポート対象：A → B → C → B • サポート対象外：A → B → C → B → A

シナリオ	解決方法
最後のアップグレードに失敗しました。	アップグレードをキャンセルして、デバイスをアップグレード前の状態に戻します。または、問題を修正して再試行してください。 復元は、アップグレードは成功したものの、アップグレードされたデバイスが期待どおりに機能しない場合に使用します。復元は、失敗または進行中のアップグレードをキャンセルすることとは異なります。元に戻すこともキャンセルすることもできない場合は、イメージを再作成する必要があります。
アップグレード以降に、管理アクセスインターフェイスが変更されています。	元に戻して、もう一度お試しください。
クラスタのユニットが異なるバージョンからアップグレードされました。	すべて一致するまでユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。
クラスタでのアップグレード後に 1 つ以上のユニットがクラスタに追加されました。	新しいユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。
クラスタで Management Center と FXOS が異なる数のクラスタユニットを識別しています。	クラスタメンバーを調整して再試行しますが、すべてのユニットを復元することはできない場合があります。

元に戻る設定

元に戻る設定

次の設定が元に戻ります。

- Snort バージョン。
- デバイス固有の設定。

  一般的なデバイス設定、ルーティング、インターフェース、インラインセット、DHCP、SNMPなど、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**ページで設定するものすべて。
- デバイス固有の設定で使用されるオブジェクト。

  アクセスリスト、AS パス、キーチェーン、インターフェイス、ネットワーク、ポート、ルートマップ、SLA モニターオブジェクトなどが含まれます。デバイスのアップグレード後にこれらのオブジェクトを編集した場合、システムは新しいオブジェクトを作成する

か、元に戻されたデバイスが使用するオブジェクトのオーバーライドを設定します。これにより、他のデバイスは現在の設定に従ってトラフィックを処理し続けることができます。

復元に成功したら、復元したデバイスで使用されているオブジェクトを調べ、必要な調整を行うことをお勧めします。

元に戻されない設定

次の設定は元に戻りません。

- 複数のデバイスで使用できる共有ポリシー。たとえば、プラットフォーム設定やアクセスコントロール ポリシーなどです。

  正常に元に戻されたデバイスは期限切れとしてマークされているため、設定を再展開する必要があります。

- Firepower 4100/9300 の場合、Secure Firewall Chassis Manager または FXOS CLI を使用して行ったインターフェイスの変更。

  復元に成功した後にインターフェイスの変更を同期します。

- Firepower 4100/9300 の場合、FXOS およびファームウェア。

  推奨される FXOS と Threat Defense の組み合わせを実行する必要がある場合は、完全な再イメージ化が必要になる場合があります。復元ガイドライン （2 ページ）を参照してください。

Threat Defense アップグレードの復元

Management Center とデバイス間の通信が中断されない限り、Management Center を使用してデバイスを復元する必要があります。通信が中断された場合は、デバイスで **upgrade revert** CLI コマンドを使用できます。システムがどのバージョンに戻るのかを確認するには、**show upgrade revert-info** コマンドを使用します。

⚠

Caution CLI から復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。

Before you begin

- 復元がサポートされていることを確認してください。ガイドラインを読んで理解してください。
- 「アップグレードの計画」の章に戻ります。一般に、インストールの準備をしたのと同じ方法で、アップグレードを元に戻す準備をします。安全な外部の場所にバックアップする

ことが特に重要です。復元に失敗した場合、再イメージ化が必要になることがあります。再イメージ化を行うと、ほとんどの設定が工場出荷時の状態に戻ります。

Procedure

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 復元するデバイスの横にある **その他**（⋮） をクリックして、[アップグレードの復元（Revert Upgrade）] を選択します。

ハイ アベイラビリティペアとクラスタを除き、複数のデバイスを選択して復元することはできません。

ステップ 3 復元して再起動することを確認します。

復元中のトラフィックフローとインスペクションの中断は、すべてのデバイスがスタンドアロンであるかのように、インターフェイス設定に依存します。 これは、高可用性/クラスタ展開であっても、システムがすべてのユニットを同時に復元するためです。

ステップ 4 復元の進行状況を監視します。

高可用性/クラスタ展開では、最初のユニットがオンラインに戻ると、トラフィックフローとインスペクションが再開されます。数分間にわたり進展がない場合、または復元が失敗したことを示している場合は、Cisco TAC にお問い合わせください。

ステップ 5 復元が成功したことを確認します。

復元が完了したら、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、復元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 6 （Firepower 4100/9300）Chassis Manager または FXOS CLI を使用して、Threat Defense 論理デバイスに加えたインターフェイスの変更を同期します。

Management Center で **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスを編集して [同期（Sync）] をクリックします。

ステップ 7 その他に必要となる復元後の構成変更を完了します。

たとえば、デバイスのアップグレード後にデバイス固有の設定で使用されるオブジェクトを編集した場合、システムは新しいオブジェクトを作成するか、復元されたデバイスが使用するオブジェクトのオーバーライドを設定します。復元したデバイスで使用されるオブジェクトを調べ、必要な調整を行うことをお勧めします。

ステップ 8 復元したデバイスに構成を再度展開します。

正常に復元されたデバイスは期限切れとしてマークされます。デバイスは古いバージョンを実行することになるため、展開が成功した後でも、新しい構成がサポートされない場合があります。

Threat Defense パッチのアンインストール

アンインストールのガイドライン

このトピックでは、アンインストールの一般的なガイドラインについて説明します。バージョン固有のアンインストールの問題を確認するには、リリースノート「https://cisco.com/go/fmc-ftd-release-notes-74」のアップグレードガイドラインを参照してください。

高可用性またはクラスタ化デバイスからのアンインストール

一度に1つのデバイスからアンインストールすることで、中断を最小限に抑えます。アップグレードとは異なり、システムはこの操作を行いません。次に移る前に、パッチが1つのユニットから完全にアンインストールされるまで待ちます。

高可用性：高可用性用に設定されたデバイスからパッチをアンインストールすることはできません。先にハイ アベイラビリティを解除する必要があります。

1. ハイ アベイラビリティを解除します。
2. 以前のスタンバイからアンインストールします。
3. 以前のアクティブからアンインストールします。
4. ハイ アベイラビリティを再確立します。

クラスタ：一度に1つのユニットからアンインストールし、制御ユニットを最後に残します。クラスタ化されたユニットは、パッチのアンインストール中はメンテナンス モードで動作します。

1. データモジュールから一度に 1 つずつアンインストールします。
2. データモジュールの 1 つを新しい制御モジュールに設定します。
3. 以前のコントロールからアンインストールします。

アンインストールの防止または制限のシナリオ

これらの状況のいずれかでアンインストールしようとすると、重大な問題が発生する可能性があります。

表 *3:* アンインストールの防止または制限のシナリオ

シナリオ	解決方法
リリースノートには、特定のパッチがアンインストールをサポートしていない、または推奨していないと記載されています。	パッチのアンインストールは、ソフトウェアにのみ適用されます。オペレーティングシステムを更新するパッチや、アンインストールによって元に戻されないその他のコンポーネントをアンインストールすると、設定の変更を展開できなかったり、新しいコンポーネントと古いソフトウェアの間でその他の非互換性が発生する可能性があります。このような場合は、アンインストールしないことをお勧めします。 パッチは累積的であり、パッチをアンインストールするとソフトウェアが開始時のバージョンに戻るため、影響を受けるパッチよりも前のバージョンに戻る場合は、それ以降のパッチをアンインストールしないことを推奨します。たとえば、パッチ5でオペレーティングシステムを更新する場合は、パッチ 5 をアンインストールしないでください。また、パッチ 4 以前（基本バージョンを含む）で起動した場合は、パッチ 6 以降もアンインストールしないでください。 これまたはその他の理由によりインストールすべきではない特定のパッチは、リリースノートに記載されています。これらのパッチのいずれかをアンインストールする必要がある場合は、Cisco TAC にお問い合わせください。
セキュリティ認定コンプライアンス（CC/UCAPL）モードになっています。	パッチによってオペレーティングシステムが更新され、セキュリティ認定コンプライアンスが有効になっている場合、アプライアンスのリブート時にFSIC（ファイルシステム完全性チェック）が失敗します。ソフトウェアは起動せず、リモートSSHアクセスが無効になり、ローカルコンソールを介してのみアプライアンスにアクセスできます。アンインストールは、セキュリティ認定コンプライアンスモードでは推奨されません。これを行う必要がある場合は、Cisco TAC にお問い合わせください。

シナリオ	解決方法
ホットフィックスまたはホットフィックスパッチをアンインストールする必要があります。	ホットフィックスとパッチは、インストールとまったく逆の順序（最後にインストールしたものを最初に削除）でアンインストールする必要があります。次に例を示します。 • インストール：パッチ A → ホットフィックス B → ホットフィックス C → パッチ D → ホットフィックス E • アンインストール：ホットフィックス E → パッチ D → ホットフィックス C → ホットフィックス B → パッチ A 更新履歴を表示するには、エキスパートモードを使用します（**cat /etc/sf/patch_history**）。 ホットフィックスおよびホットフィックスパッチのアンインストールは推奨されません。これを行う必要がある場合は、Cisco TAC にお問い合わせください。
現在実行中のバージョンに戻りました。	なし。 メジャーリリースまたはメンテナンスリリースにアップグレードすると、新しいバージョンに適用されないアップグレードパッケージとアンインストーラが削除されます。

Threat Defense のパッチのアンインストール

Linux シェル（エキスパートモード）を使用してパッチをアンインストールします。デバイスの admin ユーザーとして、または CLI 設定アクセス権を持つ別のローカルユーザーとして、デバイス シェルにアクセスできる必要があります。Management Center ユーザーアカウントは使用できません。シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

Caution アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、シャットダウン、または再起動しないでください。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。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストールで問題が発生した場合には、Cisco TAC にお問い合わせください。

Before you begin

- アンインストールがサポートされていることを確認します。ガイドラインを読んで理解してください。
- 「アップグレードの計画」の章に戻ります。一般に、パッチのアンインストールは、インストールの準備と同じ方法で準備する必要があります。

- 高可用性ペアを解除します。

Procedure

ステップ 1 デバイスの設定が古い場合は、この時点で Management Center から展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。展開とその他の必須のタスクが完了していることを確認してください。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 2 デバイスの Threat Defense CLI にアクセスします。`admin` として、または設定アクセス権を持つ別の CLI ユーザーとしてログインします。

デバイスの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用できます。コンソールを使用する場合、一部のデバイスではデフォルトでオペレーティング システムの CLI に設定されており、次のように Threat Defense CLI にアクセスする場合は追加の手順が必要になります。

Firepower 1000 Firepower 2100 Cisco Secure Firewall 3100 Cisco Secure Firewall 4200	`connect ftd`
Firepower 4100/9300	`connect module` *slot_number* `console`、次に `connect ftd`（最初のログインのみ）
ASA 5500-X シリーズ ISA 3000	—
Threat Defense Virtual	—

ステップ 3 `expert` コマンドを使用して Linux シェルにアクセスします。

ステップ 4 アップグレードディレクトリにアンインストールパッケージがあることを確認します。

```
ls /var/sf/updates
```

パッチのアンインストーラには、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には `Patch` ではなく `Patch_Uninstaller` が含まれています。デバイスにパッチを適用すると、そのパッチ用のアンインストーラがアップグレードディレクトリに自動的に作成されます。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

ステップ 5 uninstall コマンドを実行し、プロンプトが表示されたらパスワードを入力します。

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

Caution
確認を求められることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック フローとインスペクションの中断は、アップグ

レード時に発生する中断と同じです。準備が整っていることを確認してください。`--detach` オプションを使用すると、SSH セッションがタイムアウトした場合にアンインストールプロセスが強制終了されなくなり、デバイスが不安定な状態になる可能性があることに注意してください。

ステップ 6 ログアウトするまでアンインストールを監視します。

個別のアンインストールの場合は、`tail` か `tailf` を使用してログを表示します。

```
tail /ngfw/var/log/sf/update.status
```

それ以外の場合は、コンソールか端末で進行状況を監視します。

ステップ 7 アンインストールが成功したことを確認します。

アンインストールが完了したら、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。Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

ステップ 8 高可用性でクラスタ化されている展開では、ユニットごとに手順 2 から 7 を繰り返します。

クラスタの場合、制御ユニットからアンインストールしないでください。すべてのデータユニットからアンインストールしたら、そのうちの 1 つを新しい制御ユニットに設定し、以前の制御ユニットからアンインストールします。

ステップ 9 構成を再展開します。

例外：複数のバージョンが構成されている高可用性ペアまたはデバイスクラスタには展開しないでください。展開は最初のデバイスからアンインストールする前に行いますが、すべてのグループメンバーからパッチのアンインストールを終えるまでは再度展開しないでください。

What to do next

- 高可用性については、高可用性を再確立します。
- クラスタについては、特定のデバイスに優先するロールがある場合は、それらの変更をすぐに行います。

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。