ソフトウェアのインストール

バージョン 7.4 にアップグレードできない場合、またはアップグレードしたくない場合は、ソフトウェアを新しくインストールできます。これは再イメージ化とも呼ばれます。

設置に関するガイドライン

以下のガイドラインにより再イメージ化の一般的な問題を防ぐことができますが、包括的な解決策ではありません。詳細なチェックリストと手順については、該当するインストールガイドを参照してください。

Cisco Secure Firewall 3100 バージョン 7.3 以降への再イメージ化

再イメージ化の影響。

バージョン 7.3 では、次のように、Secure Firewall 3100 の Threat Defense のインストールおよびアップグレードパッケージを組み合わせました。

- バージョン 7.1 ～ 7.2 インストールパッケージ：isco-ftd-fp3k.*version*.SPA
- バージョン 7.1 ～ 7.2 アップグレードパッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar
- バージョン 7.3 以降の統合パッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar

Threat Defense は問題なくアップグレードできますが、古い Threat Defense および ASA バージョンから Threat Defense バージョン 7.3 以上に直接再イメージ化することはできません。これは、新しいイメージタイプに必要な ROMMON アップデートが原因です。これらの古いバージョンから再イメージ化するには、古い ROMMON でサポートされているだけでなく新しい ROMMON への更新も行う、ASA 9.19 以上を「通過」する必要があります。個別の ROMMON アップデータはありません。

Threat Defense バージョン 7.3 以上にするには、次のオプションがあります。

- Threat Defense バージョン 7.1 または 7.2 からのアップグレード — 通常のアップグレードプロセスを使用します。

  該当するアップグレードガイドを参照してください。

- Threat Defense バージョン 7.1 または 7.2 からの再イメージ化 — 最初に ASA 9.19 以上に再イメージ化してから、Threat Defense バージョン 7.3 以上に再イメージ化します。

  『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「*Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100*」、次に「*ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100*」を参照してください。

- ASA 9.17 または 9.18 からの再イメージ化 — 最初に ASA 9.19 以上にアップグレードしてから、Threat Defense バージョン 7.3 以上に再イメージ化します。

  『Cisco Secure Firewall ASA アップグレードガイド』を参照し、次に『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「*ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100*」を参照してください。

- Threat Defense バージョン 7.3 以上からの再イメージ化 — 通常の再イメージ化プロセスを使用します。

  『Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）』の「*Reimage the System with a New Software Version*」を参照してください。

バックアップ

再イメージ化の前に、安全なリモートロケーションにバックアップし、正常に転送されたことを確認することを強く推奨します。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。アプライアンスに残っているすべてのバックアップが削除されます。

（注） アップグレードを不要にするため再イメージ化したい場合、バージョンの制約によっては、バックアップを使用して古い設定をインポートすることはできません。設定は手動で再作成する必要があります。

アプライアンス アクセス

アプライアンスに物理的にアクセスできない場合、現在のメジャーリリースまたはメンテナンスリリースへの再イメージ化によって管理ネットワークの設定を維持できます。これにより、再イメージ化した後、アプライアンスに接続して、初期設定を実行できます。ネットワーク設定を削除する場合や以前のリリースに再イメージ化する場合は、アプライアンスに物理的にアクセスできる必要があります。Lights-Out 管理（LOM）を使用することはできません。

デバイスに関して、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。Management

Center の展開では、デバイスを経由せずに Management Center 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。

Smart Software Manager からの登録解除

アプライアンスまたはスイッチデバイス管理のイメージを再作成する前に、Cisco Smart Software Manager（CSSM） での登録解除が必要になる場合があります。これは、再登録を妨げる可能性のある孤立した権限付与の発生を避けるためです。

登録を解除すると、仮想アカウントからアプライアンスが削除され、クラウドおよびクラウドサービスからアプライアンスが登録解除され、関連付けられたライセンスが解放されるため、ライセンスを再割り当てできるようになります。アプライアンスを登録解除すると、適用モードになります。アプライアンスの現在の設定とポリシーはそのまま機能しますが、変更を加えたり展開したりすることはできません。

バックアップから復元する予定がある場合は、再イメージ化の前に登録を解除しないでください。また、Management Center からデバイスを削除しないでください。代わりに、バックアップを実行した後に行われたライセンス変更を手動で元に戻します。復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。

表 *1 : CSSM* からの登録解除シナリオ（バックアップから復元しない）

シナリオ	アクション
Management Center を再イメージ化します。	手動で登録解除します。
Management Center のモデルを移行します。	ソースの Management Center をシャットダウンする前に、手動で登録を解除します。
Management Center で Threat Defense を再イメージ化します。	Management Center からデバイスを削除すると、自動的に登録が解除されます。
Device Manager で Threat Defense を再イメージ化します。	手動で登録解除します。
Threat Defense を Management Center から Device Manager へ切り替えます。	Management Center からデバイスを削除すると、自動的に登録が解除されます。
デバイスマネージャーから Management Center に Threat Defense を切り替えます。	手動で登録解除します。

Management Center からのデバイスの削除

Management Center の展開で再イメージ化されたアプライアンスを手動で設定する予定がある場合は、再イメージ化する前に、Management Center からデバイスを削除します。バックアップからの復元を予定している場合は、これを行う必要はありません。

表 *2: Management Center* からデバイスを削除するシナリオ（バックアップから復元しない）

シナリオ	アクション
Management Center を再イメージ化します。	管理からデバイスを削除します。
Threat Defense を再イメージ化します。	管理から任意のデバイスを削除します。
Threat Defense を Management Center から Device Manager へ切り替えます。	管理から任意のデバイスを削除します。

FXOS をダウングレードするための Threat Defense ハードウェアの完全な再イメージ化

FXOS オペレーティングシステムを使用する Threat Defense ハードウェアモデルの場合、以前のソフトウェアバージョンに再イメージ化するには、FXOSがソフトウェアにバンドルされているか、個別にアップグレードされているかに関係なく、完全な再イメージ化が必要になる場合があります。

表 *3:* 完全な再イメージ化のシナリオ

モデル	詳細
Firepower 1000 シリーズ Firepower 2100 シリーズ Secure Firewall 3100 シリーズ Cisco Secure Firewall 4200 シリーズ	**erase configuration** メソッドを使用してイメージを再作成すると、FXOS がソフトウェアとともにダウングレードされない場合があります。この場合、特にハイ アベイラビリティ展開では、障害が発生する可能性があります。これらのデバイスの完全な再イメージ化を実行することを推奨します。 Secure Firewall 3100/4200 の場合は、再イメージ化によってデバイスがアプライアンスモードになります。マルチインスタンスモードを使用していた場合は、再度有効にする必要があります。
Firepower 4100/9300	Threat Defense を復元しても 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。

設置ガイド

表 *4*:設置ガイド

プラットフォーム	ガイド
Management Center	
Cisco Secure Firewall Management Center 1700、2700、4700	Cisco Secure Firewall Management Center 1700、2700、および 4700 スタートアップガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide ド
Management Center Virtual	Cisco Secure Firewall Management Center Virtual 入門ガイド
Threat Defense	
Firepower 1000/2100 シリーズ Secure Firewall 3100/4200 シリーズ	Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）
Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Configuration Guides：イメージ管理に関する章 Cisco Firepower 4100 Getting Started Guide Cisco Firepower 9300 Getting Started Guide
ISA 3000	Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド
Threat Defense Virtual	Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

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。