Cisco Secure Firewall 移行ツール 10.0.4 リリースノート

最終更新：2026 年 11 月 5 日

Cisco Secure Firewall 移行ツール

Secure Firewall Migration ツールを使用すると、Management Center で管理されるサポート対象の Cisco Secure Firewall Threat Defense にファイアウォール設定を移行できます。この移行ツールでは、Cisco Secure Firewall ASA、ASA with FirePOWER Services（FPS）、FDM 管理対象デバイス、および Microsoft Azure、Check Point、Palo Alto Networks、Fortinet のサードパーティ製ファイアウォールからの移行をサポートします。

このドキュメントでは、Secure Firewall Migration ツールに関する重要かつリリース固有の情報を示します。Cisco Secure Firewall のリリースに精通していて、移行プロセスを以前に経験したことがある場合でも、このドキュメントを読み、十分に理解しておくことをお勧めします。

新機能

このリリースに含まれる機能について説明します。

リリースバージョン	機能	説明
10.0.4	パッチリリース	このパッチリリースにはバグ修正が含まれています。詳細については、「未解決および解決済みの問題」を参照してください。

未解決および解決済みの問題

次の表に、Firewall Migration Manager バージョン 10.0.4 の解決済みの移行バグを示します。

表 *1*：解決済みの問題

不具合 ID	説明
CSCwu62168	ASA から Firewall Threat Defense への移行中に、ループバック インターフェイスでセキュリティゾーンを設定することはできません。

不具合 ID	説明
CSCwu62166	ASA から Firewall Threat Defense への移行が失敗し、次のエラーメッセージが表示されます。 `s2s vpn のプッシュ中にエラーが発生しました：トンネル送信元 IP アドレスを設定してください。（Error while pushing s2s vpn: Configure a tunnel source IP address.）仮想トンネル intarana の有効なトンネル送信元 IP アドレスを設定してください。（Configure a valid tunnel source IP address for the virtual tunnel intarana.）DYNAMIC-VTI`
CSCwu37642	PAN から Firewall Threat Defense への設定の移行中に、一括プッシュが失敗したか、分割されました。この障害により、ACL バッチが分割され、ACL エントリが 1 つずつプッシュされました。
CSCwu37618	PAN から Firewall Threat Defense への移行では、ネットワークオブジェクトがサポートされていないため、関連する ACL とオブジェクトグループはサポートされません。
CSCwu13544	ASA の移行中、送信元 ASA 設定の RAVPN 接続プロファイル内で複数のグループ URL が参照されています。ただし、これらの接続プロファイルとそのグループ URL は移行されません。代わりに、この情報は移行前レポートに記録されます。
CSCws98076	ASA から Firewall Threat Defense への移行で、インターフェイスのプッシュ中にエラーが発生しました：`ループバック ID の無効な値、許可された範囲：1 ～ 1024。（Invalid Value for Loopback Id, Allowed range: 1 to 1024.）`
CSCwu51895	ASA から Firewall Threat Defense への移行で、サイト間 VPN ハブおよびスポークトポロジの作成中にエラーが発生しました。

未解決および解決済みの警告

このリリースで未解決の警告には、Cisco バグ検索ツールを使用してアクセスできます。この Web ベースツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコバグトラッキングシステムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントを持っていない場合は、Cisco.com でアカウントに登録できます。バグ検索ツールの詳細については、「Bug Search Tool（BST）ヘルプおよび FAQ」を参照してください。

Secure Firewall Migration ツールの未解決および解決済みの警告に関する最新リストについては、未解決および解決済みの警告ダイナミッククエリを使用してください。

リリース機能概要（基礎編）ビデオ

Cisco Secure Firewall Migration ツールリリース概要ビデオでは、このリリースの次のような包括的な概要が示されます。

- 更新で導入された主な機能
- 新機能と改善点
- 最新の機能拡張によってもたらされる利点の明確な説明

このビデオは、「Cisco Secure Firewall Migration Tool – Release Overview」でご覧いただけます。

今回のリリースについて十分に理解し、更新された製品でエクスペリエンスを最適化するために、このビデオをご覧になることをお勧めします。

移行でサポートされる設定要素

Secure Firewall Migration ツールのサポート対象の設定については、以下のリンクを参照してください。

- サポートされている Azure 構成
- サポートされている ASA の設定
- サポートされている ASA with FirePOWER Services の構成
- サポートされているチェックポイントの設定
- サポートされている PAN 構成
- サポートされている FortiNet の設定
- サポートされている FDM 管理対象デバイス構成

インフラストラクチャとプラットフォームの要件

Secure Firewall Migration ツールには、次のインフラストラクチャとプラットフォームが必要です。

- Windows 10 64 ビット オペレーティング システムまたは MacOS バージョン 10.13 以降
- Google Chrome がシステムのデフォルト ブラウザ

ヒント　移行ツールを使用するときは、ブラウザで全画面表示モードを使用することをお勧めします。

- システムごとの Secure Firewall Migration ツールのシングルインスタンス
- Management Center と Threat Defense がバージョン 6.2.3.3 以降であること

（注）　新しいバージョンをダウンロードする前に、以前のビルドを削除する。

関連資料

Cisco Secure Firewall 移行ツールの履歴情報については、次を参照してください。

- History of the ASA Firewall Migration Tool
- History of the ASA with FirePOWER Services Firewall to Threat Defense with the Firewall Migration Tool
- History of the Check Point Firewall Migration Tool
- History of the Palo Alto Networks Firewall Migration Tool
- History of the Fortinet Firewall Migration Tool
- History of the FDM-Managed Device Migration Tool

移行ワークフロー

Secure Firewall Migration ツールの移行ワークフローについては、以下を参照してください。

- ASA 構成ファイルのエクスポート
- ASA with FirePOWER Services 構成ファイルのエクスポート
- Microsoft Azure ネイティブファイアウォール構成ファイルのエクスポート
- Check Point 構成ファイルのエクスポート
- Palo Alto Networks ファイアウォールからの構成のエクスポート
- Fortinet ファイアウォールからの構成のエクスポート
- FDM 管理対象デバイス構成ファイルのエクスポート

移行レポート

Secure Firewall Migration ツールは、以下のレポートを移行の詳細とともに HTML 形式で提供します。

- 移行前のレポート
- 移行後のレポート

Secure Firewall Migration ツールの機能

Secure Firewall Migration ツールには、次のような機能があります。

- 分析およびプッシュ操作を含む移行全体の検証
- オブジェクト再利用機能
- オブジェクト競合の解決
- インターフェイス マッピング
- インターフェイス オブジェクトの自動作成または再利用（セキュリティゾーンとインターフェイス グループ マッピングに対する ASA name if）
- インターフェイス オブジェクトの自動作成または再利用
- 自動ゾーンマッピング
- ユーザー定義のセキュリティゾーンとインターフェイスグループの作成
- ユーザー定義のセキュリティゾーンの作成
- 送信先 Threat Defense デバイスのサブインターフェイス制限チェック
- サポートされるプラットフォーム：
  - ASA Virtual から Threat Defense Virtual へ
  - FDM Virtual から Threat Defense Virtual へ
  - 同じハードウェアでの移行（X から X デバイスへの移行）
  - X から Y デバイスへの移行（Y に多数のインターフェイスが存在）
- ACP ルールアクションに対する送信元 ASA、FDM 管理対象デバイス、Fortinet、および Checkpoint の ACL 最適化。

ファイアウォール移行ツールのドキュメントへのリンク

- Navigating the Cisco Secure Firewall Migration Tool Documentation
- Migrating ASA Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating ASA Firewall with FirePOWER Services to Firewall Threat Defense with the Secure Firewall Migration Tool

- Cisco Secure Firewall ASA から Threat Defense への機能マッピング
- 移行ツールを使用した Cisco Secure Firewall Threat Defense への FDM 管理対象デバイスの移行
- Cisco Secure Firewall 移行ツールを使用した Microsoft Azure ネイティブファイアウォールから Cisco Secure Firewall Threat Defense への移行
- Migrating Check Point Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Fortinet Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Migration Tool
- Palo Alto Networks to Cisco Secure Firewall Threat Defense Migration Prerequisites Guide
- Migrating Palo Alto Networks Firewall to Firewall Threat Defense with the Secure Firewall Migration Tool
- Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool
- Cisco Secure Firewall Migration Tool Compatibility Guide
- Secure Firewall Migration Tool Best Practices Guide

© 2026 Cisco Systems, Inc. All rights reserved.

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。