



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

最終更新：2025 年 8 月 29 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ www.cisco.com/jp/go/safety_warning/ ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025– Cisco Systems, Inc. All rights reserved.



目次

第 1 章

Cisco Secure Firewall 移行ツールのスタートアップガイド 1

- Cisco Secure Firewall 移行ツールについて 1
- Cisco Secure Firewall 移行ツールの最新情報 5
- Cisco Secure Firewall 移行ツールのライセンス 20
- Cisco Secure Firewall 移行ツールのプラットフォーム要件 20
- Threat Defense デバイスの要件および前提条件 20
- 注意事項と制約事項 21
- サポートされる移行先の管理センター 22
- 移行でサポートされるソフトウェアのバージョン 24

第 2 章

Microsoft Azure ネイティブファイアウォールから Threat Defense への移行ワークフロー 25

- エンドツーエンドの手順 25
- 移行の前提条件 27
 - Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード 27
 - Microsoft Azure ネイティブファイアウォールからの構成のエクスポート 28
 - Azure ファイアウォール GUI からのポリシー構成のエクスポート 28
 - IP グループ構成のエクスポート 29
- 移行の実行 29
 - Cisco Secure Firewall 移行ツールの起動 29
 - Cisco Secure Firewall 移行ツールでのデモモードの使用 31
 - Microsoft Azure 構成ファイルのアップロード 32
 - Cisco Secure Firewall 移行ツールの接続先パラメータの指定 33
 - 移行前レポートの確認 36
 - 最適化、構成の確認と検証 37

移行された構成の以下へのプッシュ : Firewall Management Center 41

移行後レポートの確認と移行の完了 42

解析のサマリー 44

移行の失敗 45

Cisco Secure Firewall 移行ツールのアンインストール 46

移行例 : Azure から Threat Defense 2100 46

メンテナンス期間前のタスク 47

メンテナンス期間のタスク 48

第 3 章 Cisco Success Network : テレメトリデータ 49

Cisco Success Network - テレメトリデータ 49

第 4 章 移行の問題のトラブルシューティング 53

Cisco Secure Firewall 移行ツールのトラブルシューティング 53

トラブルシューティングに使用されるログおよびその他のファイル 54



第 1 章

Cisco Secure Firewall 移行ツールのスタートアップガイド

- [Cisco Secure Firewall 移行ツールについて \(1 ページ\)](#)
- [Cisco Secure Firewall 移行ツールの最新情報 \(5 ページ\)](#)
- [Cisco Secure Firewall 移行ツールのライセンス \(20 ページ\)](#)
- [Cisco Secure Firewall 移行ツールのプラットフォーム要件 \(20 ページ\)](#)
- [Threat Defense デバイスの要件および前提条件 \(20 ページ\)](#)
- [注意事項と制約事項 \(21 ページ\)](#)
- [サポートされる移行先の管理センター \(22 ページ\)](#)
- [移行でサポートされるソフトウェアのバージョン \(24 ページ\)](#)

Cisco Secure Firewall 移行ツールについて

このガイドでは、Cisco Secure Firewall 移行ツールをダウンロードして移行を完了する方法について説明します。さらに、発生する可能性のある移行の問題を解決するのに役立つトラブルシューティングのヒントも提供します。

本書に記載されているサンプルの移行手順（「[移行例：Azure から Threat defense 2100](#)」）は、移行プロセスに関する理解を促進するのに役立ちます。

Cisco Secure Firewall 移行ツールは、サポートされている Azure 構成をサポートされている Secure Firewall Threat Defense プラットフォームに変換します。Cisco Secure Firewall 移行ツールを使用すると、サポートされている Azure 機能とポリシーを自動的に Firewall Threat Defense に移行できます。移行前レポートで無視された構成について確認し、移行後にそれらを手動で構成する必要があります。

Cisco Secure Firewall 移行ツールは、Azure 情報を収集し、解析して、最終的に Secure Firewall Management Center にプッシュします。解析フェーズ中に、Cisco Secure Firewall 移行ツールは、以下を特定する **移行前レポート** を生成します。

- 正常に移行できるサポートされている Microsoft Azure 構成要素の概要。
- エラーがある Azure 構成行

- 移行で無視される Azure 構成項目

解析エラーがある場合は、問題を修正し、新しい構成を再アップロードし、接続先デバイスに接続し、構成の見直しと確認を実行します。その後、構成を接続先デバイスに移行できます。

コンソール

Cisco Secure Firewall 移行ツールを起動すると、コンソールが開きます。コンソールには、Cisco Secure Firewall 移行ツールの各ステップの進行状況に関する詳細情報が表示されます。コンソールの内容は、Cisco Secure Firewall 移行ツールのログファイルにも書き込まれます。

Cisco Secure Firewall 移行ツールが開いていて実行中の間は、コンソールを開いたままにする必要があります。



重要 Cisco Secure Firewall 移行ツールを終了するために Web インターフェイスが実行されているブラウザを閉じると、コンソールはバックグラウンドで実行され続けます。Cisco Secure Firewall 移行ツールを完全に終了するには、キーボードの **Command キー + C** を押してコンソールを終了します。

ログ

Cisco Secure Firewall 移行ツールは、各移行のログを作成します。ログには、移行の各ステップで発生した内容の詳細が含まれるため、移行が失敗した場合の原因の特定に役立ちます。

Cisco Secure Firewall 移行ツールのログファイルは、`<migration_tool_folder>\logs`にあります。

リソース

Cisco Secure Firewall 移行ツールは、**移行前レポートのコピー**、**移行後レポートのコピー**、Azure 構成、および **Resources** フォルダ内のログを保存します。

Resources フォルダは、`<migration_tool_folder>\resources` にあります

未解析ファイル

Cisco Secure Firewall 移行ツールは、未解析ファイルで無視した構成行に関する情報をログに記録します。この Cisco Secure Firewall 移行ツールは、Azure 構成ファイルを解析する際に、このファイルを作成します。

未解析ファイルは、次の場所にあります。

`<migration_tool_folder>\resources`

Cisco Secure Firewall 移行ツールでの検索

[最適化、確認および検証 (Optimize, Review and Validate)] ウィンドウの項目など、Cisco Secure Firewall 移行ツールに表示されるテーブル内の項目を検索できます。

テーブルの任意の列または行の項目を検索するには、テーブルの上の **検索** (🔍) をクリックし、フィールドに検索語を入力します。Cisco Secure Firewall 移行ツールはテーブル行をフィルタ処理し、その検索語を含む行のみを表示します。

単一の列で項目を検索するには、列見出しにある [検索 (Search)] フィールドに検索語を入力します。Cisco Secure Firewall 移行ツールはテーブル行をフィルタ処理し、検索語に一致する行のみを表示します。

ポート

Cisco Secure Firewall 移行ツールは、ポート 8321 ~ 8331 およびポート 8888 の 12 ポートのうちいずれかのポートで実行されるテレメトリをサポートします。デフォルトでは、Cisco Secure Firewall 移行ツールはポート 8888 を使用します。ポートを変更するには、`app_config` ファイルのポート情報を更新します。更新後、ポートの変更を有効にするために、Cisco Secure Firewall 移行ツールを再起動します。`app_config` ファイルは、`<migration_tool_folder>\app_config.txt` にあります。



- (注) テレメトリはこれらのポートでのみサポートされているため、ポート 8321 ~ 8331 およびポート 8888 を使用することを推奨します。Cisco Success Network を有効にすると、Cisco Secure Firewall 移行ツールに他のポートを使用できなくなります。

通知センター

移行中にポップアップ表示される成功メッセージ、エラーメッセージ、警告を含むすべての通知は、通知センターでキャプチャされ、[成功 (Successes)]、[警告 (Warnings)]、および [エ

ラー (Errors)] に分類されます。移行中はいつでも右上隅にある  アイコンをクリックして、ポップアップしたさまざまな通知と、それらがツールにポップアップ表示された時刻を確認できます。

Cisco Success Network

Cisco Success Network はユーザ対応のクラウドサービスです。Cisco Success Network を有効にすると、Cisco Secure Firewall 移行ツールと Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、Cisco Secure Firewall 移行ツールからの対象のデータを選択して、それを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- ネットワーク内の製品の有効性を向上させるために、利用可能な未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカルサポートサービスとモニタリングについて通知します。
- シスコ製品の改善に役立ちます。

Cisco Secure Firewall 移行ツールはセキュアな接続を確立および維持し、Cisco Success Network に登録できるようにします。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。

Cisco Secure Firewall 移行ツールの最新情報

バージョン	サポートされる機能
7.7.10	

バージョン	サポートされる機能
	<p>このリリースには、次の新機能が含まれています。</p> <ul style="list-style-type: none"> • Cisco Secure Firewall 移行ツールを使用して、Microsoft Azure ネイティブファイアウォールから Firewall Threat Defense に設定を移行できるようになりました。詳細と移行手順については、『Migrating Microsoft Azure Native Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool』を参照してください。 • Cisco Secure Firewall 移行ツールを使用して、Check Point ファイアウォールから Multicloud Defense に設定を移行できるようになりました。詳細と移行手順については、『Migrating Check Point Firewall to Cisco Multicloud Defense with the Migration Tool』を参照してください。 • Cisco Secure Firewall 移行ツールを使用して、Fortinet ファイアウォールから Multicloud Defense に設定を移行できるようになりました。詳細と移行手順については、『Migrating Fortinet Firewall to Cisco Multicloud Defense with the Migration Tool』を参照してください。 • Cisco Secure Firewall 移行ツールが、既存のセキュリティグループタグオブジェクトの設定を検出できるようになりました。この検出機能は、特定のタグをユーザー、デバイス、またはシステムに関連付けることでセキュリティポリシーの管理を簡素化し、動的でスケーラブルなアクセス制御を可能にします。 「構成の最適化、確認および検証」を参照してください サポートされる移行：Cisco Secure Firewall ASA • [設定の最適化、確認、検証 (Optimize, Review and Validate Configurations)] ページで、オブジェクトまたはオブジェクトグループを追加、削除、または変更してアクセスルールを編集できるようになりました。 「構成の最適化、確認および検証」を参照してください サポートされる移行：すべて • 移行前レポートと移行後レポートが強化され、ユーザー体験が向上しました。 各セクションの CSV ファイルをダウンロードして、詳細な分析を行えるようになりました。移行後レポートに比較チャートが導入され、移行前レポートと移行後レポートでカテゴリごとに設定数を比較できます。 「構成の最適化、確認および検証」を参照してください サポートされる移行：すべて

バージョン	サポートされる機能
7.7	<p data-bbox="678 298 1273 327">このリリースには、次の新機能が含まれています。</p> <ul data-bbox="711 352 1523 722" style="list-style-type: none"><li data-bbox="711 352 1523 525">• Cisco Secure Firewall 移行ツールを使用して、Secure Firewall ASA から Multicloud Defense に構成を移行できるようになりました。詳細と移行手順については、『Migrating Cisco Secure Firewall ASA to Cisco Multicloud Defense with the Migration Tool』を参照してください。<li data-bbox="711 550 1523 722">• Cisco Secure Firewall 移行ツールを使用して、Palo Alto Networks ファイアウォールから Multicloud Defense に構成を移行できるようになりました。詳細と移行手順については、『Migrating Palo Alto Networks Firewall to Cisco Multicloud Defense with the Migration Tool』を参照してください。

バージョン	サポートされる機能
7.0.1	

バージョン	サポートされる機能
	<p>このリリースには、次の新機能と機能拡張が含まれています。</p> <ul style="list-style-type: none"> • ASA および FDM 管理対象デバイスやサードパーティ製ファイアウォールなどのシスコファイアウォールから Cisco Secure Firewall 1200 シリーズ デバイスに設定を移行できるようになりました。 「Cisco Secure Firewall 1200 Series」を参照してください • 複数のサイト間 VPN トンネル設定の事前共有キーを一度に更新できるようになりました。[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページのサイト間 VPN テーブルを Excel シートにエクスポートし、それぞれのセルに事前共有キーを指定して、シートをアップロードします。移行ツールは、Excel から事前共有キーを読み取り、テーブルを更新します。 「構成の最適化、確認および検証」を参照してください サポートされる移行：すべて • 移行を妨げる誤った設定を無視し、移行の最終プッシュを続行することを選択できるようになりました。以前は、単一のオブジェクトのプッシュがエラーのために失敗した場合でも、移行全体が失敗していました。また、移行を手動で中止してエラーを修正し、移行を再試行することもできるようになりました。 「移行された構成の Management Center へのプッシュ」を参照してください サポートされる移行：すべて • Secure Firewall 移行ツールは、ターゲットの Threat Defense デバイスの既存のサイト間 VPN 設定を検出し、Management Center にログインせずに削除するかどうかを選択するように求めます。[いいえ (No)] を選択し、Management Center から手動で削除して移行を続行できます。 「構成の最適化、確認および検証」を参照してください サポートされる移行：すべて • 移行先の Management Center によって管理される Threat Defense デバイスのいずれかに既存のハブアンドスポークトポロジが設定されている場合は、移行ツールから、ターゲットの Threat Defense デバイスをスポークの 1 つとして既存のトポロジに追加できます。 Management Center で手動で行う必要はありません。 「構成の最適化、確認および検証」を参照してください サポートされる移行：Cisco Secure Firewall ASA • サードパーティ製ファイアウォールを移行するときに、高可用性ペ

バージョン	サポートされる機能
	<p>アの一部である Threat Defense デバイスをターゲットとして選択できるようになりました。以前は、スタンドアロンの Threat Defense デバイスのみをターゲットデバイスとして選択できました。</p> <p>サポートされる移行：Palo Alto Networks、Check Point、および Fortinet ファイアウォールの移行</p> <ul style="list-style-type: none">• Cisco Secure Firewall 移行ツールは、より強化された直感的なデモモードを提供し、すべてのステップでガイド付きの移行手順が提供されるようになりました。さらに、要件に基づいて選択してテストするターゲット Threat Defense デバイスのバージョンを確認することもできます。 <p>サポートされる移行：すべて</p>

バージョン	サポートされる機能
7.0	<p>このリリースには、次の新機能と機能拡張が含まれています。</p> <p>Cisco Secure Firewall Threat Defense への Cisco Secure Firewall ASA の移行</p> <ul style="list-style-type: none"> 移行先の Management Center に Threat Defense の高可用性（HA）ペアを設定し、Cisco Secure Firewall ASA HA ペアから Management Center に設定を移行できるようになりました。[ターゲットの選択（Select Target）] ページで [HAペア設定を続行（Proceed with HA Pair Configuration）] を選択し、アクティブデバイスとスタンバイデバイスを選択します。アクティブな Threat Defense デバイスを選択する場合は、HA ペア設定を成功させるために、Management Center に同一のデバイスがあることを確認してください。詳細については、『Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool』の「Specify Destination Parameters for the Secure Firewall Migration Tool」を参照してください。 ASA デバイスからサイト間 VPN 設定を移行するときに、Threat Defense デバイスを使用してサイト間ハブアンドスポーク VPN トポロジを設定できるようになりました。[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] ページの [サイト間VPNトンネル（Site-to-Site VPN Tunnels）] の下にある [ハブアンドスポークトポロジの追加（Add Hub & Spoke Topology）] をクリックします。詳細については、『Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool』の「構成の最適化、確認および検証」を参照してください。 <p>Cisco Secure Firewall Threat Defense への Fortinet ファイアウォールの移行</p> <ul style="list-style-type: none"> Fortinet ファイアウォールから Threat Defense デバイスに、SSL VPN および中央 SNAT 設定の IPv6 および複数のインターフェイスとインターフェイスゾーンを移行できるようになりました。詳細については、『Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool』の「Fortinet Configuration Support」を参照してください。

バージョン	サポートされる機能
6.0.1	

バージョン	サポートされる機能
	<p>このリリースには、次の新機能と機能拡張が含まれています。</p> <p>Cisco Secure Firewall Threat Defense への Cisco Secure Firewall ASA の移行</p> <ul style="list-style-type: none"> • Cisco Secure Firewall ASA から Threat Defense に設定を移行する際に、ネットワークとポートのオブジェクトを最適化できるようになりました。[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページの該当するタブでこれらのオブジェクトを確認し、[オブジェクトとグループの最適化 (Optimize Objects and Groups)] をクリックして、移行先の Management Center に移行する前にオブジェクトのリストを最適化します。移行ツールは、同じ値を持つオブジェクトとグループを識別し、どちらを保持するかを選択するように求めます。詳細については、「構成の最適化、確認および検証」を参照してください。 <p>Cisco Secure Firewall Threat Defense への FDM 管理対象デバイスの移行</p> <ul style="list-style-type: none"> • FDM 管理対象デバイスから Threat Defense デバイスに DHCP、DDNS、および SNMPv3 の設定を移行できるようになりました。[機能の選択 (Select Features)] ページで、[DHCP] チェックボックスと [サーバー (Server)]、[リレー (Relay)]、および [DDNS] チェックボックスがオンになっていることを確認します。詳細については、「構成の最適化、確認および検証」を参照してください。 <p>Cisco Secure Firewall Threat Defense への Fortinet ファイアウォールの移行</p> <ul style="list-style-type: none"> • Fortinet ファイアウォールから Threat Defense デバイスに URL オブジェクトを他のオブジェクトタイプに加えて移行できるようになりました。移行中に、[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページの [オブジェクト (Objects)] ウィンドウの [URL オブジェクト (URL Objects)] タブを確認します。詳細については、「構成の最適化、確認および検証」を参照してください。 <p>Palo Alto Networks ファイアウォールの Cisco Secure Firewall Threat Defense への移行</p> <ul style="list-style-type: none"> • Palo Alto Networks ファイアウォールから Threat Defense デバイスに URL オブジェクトを他のオブジェクトタイプに加えて移行できるようになりました。移行中に、[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページの [オブジェクト (Objects)] ウィンドウの [URL オブジェクト (URL Objects)] タブを必ず確認します。詳細については、「構成の最適化、確認および検証」を参照してください。

バージョン	サポートされる機能
	<p data-bbox="641 296 1481 359">Cisco Secure Firewall Threat Defense への Check Point ファイアウォールの移行</p> <ul data-bbox="673 380 1481 590" style="list-style-type: none"><li data-bbox="673 380 1481 590">• Check Point ファイアウォールから Threat Defense デバイスにポートオブジェクト、FQDN オブジェクト、およびオブジェクトグループを移行できるようになりました。移行中に、[構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] ページの [オブジェクト (Objects)] ウィンドウを確認します。詳細については、「構成の最適化、確認および検証」を参照してください。

バージョン	サポートされる機能
6.0	

バージョン	サポートされる機能
	<p>このリリースには、次の新機能と機能拡張が含まれています。</p> <p>Cisco Secure Firewall Threat Defense への Cisco Secure Firewall ASA の移行</p> <ul style="list-style-type: none"> Secure Firewall ASA の WebVPN 設定を、Threat Defense デバイスの Zero Trust Access Policy 設定に移行できるようになりました。[機能の選択 (Select Features)] ページで [WebVPN] チェックボックスがオンになっていることを確認し、[設定の最適化、確認、検証 (Optimize, Review and Validate Configuration)] ページで新しい [WebVPN] タブを確認します。Threat Defense デバイスとターゲット管理センターは、バージョン 7.4 以降で実行され、検出エンジンとして Snort3 を実行している必要があります。 Simple Network Management Protocol (SNMP) および Dynamic Host Configuration Protocol (DHCP) の設定を Threat Defense デバイスに移行できるようになりました。[機能の選択 (Select Features)] ページで、[SNMP] および [DHCP] チェックボックスがオンになっていることを確認します。Secure Firewall ASA で DHCP を設定している場合は、DHCP サーバーまたはリレーエージェントと DDNS の設定も移行対象として選択できることに注意してください。 マルチコンテキスト ASA デバイスを実行するときに、等コストマルチパス (ECMP) ルーティング設定を単一インスタンスの脅威防御のマージされたコンテキスト移行に移行できるようになりました。解析されたサマリーの [ルート (Routes)] タイルに ECMP ゾーンも含まれるようになりました。[設定の最適化、レビュー、検証 (Optimize, Review and Validate Configuration)] ページの [ルート (Routes)] タブで同じことを検証できます。 ダイナミック仮想トンネルインターフェイス (DVTI) 設定のダイナミックトンネルを Secure Firewall ASA から Threat Defense デバイスに移行できるようになりました。これらは、[セキュリティゾーン、インターフェイスグループ、および VRF への ASA インターフェイスのマッピング (Map ASA Interfaces to Security Zones, Interface Groups, and VRFs)] ページでマッピングできます。この機能を適用するには、ASA のバージョンが 9.19(x) 以降であることを確認します。 <p>Cisco Secure Firewall Threat Defense への FDM 管理対象デバイスの移行</p> <ul style="list-style-type: none"> SNMP や HTTP を含むレイヤ 7 セキュリティポリシー、マルウェアおよびファイルポリシー設定を FDM 管理対象デバイスから Threat Defense デバイスに移行できるようになりました。ターゲット管理センターのバージョンが 7.4 以降であること、および [機能の選択 (Select Features)] ページの [プラットフォーム設定 (Platform

バージョン	サポートされる機能
	<p>Settings)]および[ファイルとマルウェアポリシー (File and Malware Policy)]チェックボックスがオンになっていることを確認します。</p> <p>Cisco Secure Firewall Threat Defense への Check Point ファイアウォールの移行</p> <ul style="list-style-type: none">• Check Point ファイアウォールのサイト間 VPN (ポリシーベース) 設定を Threat Defense デバイスに移行できるようになりました。この機能は、Check Point R80 以降のバージョン、および Management Center および Threat Defense バージョン 6.7 以降に適用されることに注意してください。[機能の選択 (Select Features)]ページで、[サイト間VPNトンネル (Site-to-Site VPN Tunnels)]チェックボックスがオンになっていることを確認します。これはデバイス固有の設定であるため、[FTDなしで続行 (Proceed without FTD)]を選択した場合、移行ツールにこれらの設定は表示されないことに注意してください。 <p>Cisco Secure Firewall Threat Defense への Fortinet ファイアウォールの移行</p> <ul style="list-style-type: none">• Fortinet ファイアウォールから Threat Defense デバイスに設定を移行するときに、アプリケーションアクセスコントロールリスト (ACL) を最適化できるようになりました。[設定の最適化、レビュー、検証 (Optimize, Review and Validate Configuration)]ページの [ACLの最適化 (Optimize ACL)]ボタンを使用して、冗長 ACL とシャドウ ACL のリストを表示し、最適化レポートをダウンロードして詳細な ACL 情報を表示します。

バージョン	サポートされる機能
5.0.1	<p>このリリースには、次の新機能と機能拡張が含まれています。</p> <ul style="list-style-type: none"> • Cisco Secure Firewall 移行ツールは、Cisco Secure Firewall ASA デバイスから Threat Defense デバイスへの複数のトランスペアレントファイアウォールモードのセキュリティコンテキストの移行をサポートするようになりました。Cisco Secure Firewall ASA デバイス内の2つ以上のトランスペアレントファイアウォールモードのコンテキストをトランスペアレントモードのインスタンスにマージし、それらを移行できます。 <p>1つ以上のコンテキストにVPN設定がある場合のVPN設定のASA展開では、VPN設定をターゲットのThreat Defense デバイスに移行するコンテキストを1つのみ選択できます。選択しなかったコンテキストからは、VPN設定以外のすべての設定が移行されます。</p> <p>詳細については、「ASA セキュリティコンテキストの選択」を参照してください。</p> <ul style="list-style-type: none"> • Cisco Secure Firewall 移行ツールを使用して、サイト間およびリモートアクセスVPN設定をFortinet および Palo Alto Networks ファイアウォールから Threat Defense に移行できるようになりました。[機能の選択 (Select Features)] ペインから、移行するVPN機能を選択します。『Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool』および『Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool』の「Specify Destination Parameters for the Secure Firewall Migration Tool」セクションを参照してください。 • Cisco Secure Firewall ASA デバイスから1つ以上のルーテッドまたはトランスペアレントファイアウォールモードのセキュリティコンテキストを選択し、Cisco Secure Firewall 移行ツールを使用してシングルコンテキストまたはマルチコンテキストを移行できるようになりました。

バージョン	サポートされる機能
5.0	<ul style="list-style-type: none"> • Cisco Secure Firewall 移行ツールは、Cisco Secure Firewall ASA から Threat Defense デバイスへの複数のセキュリティコンテキストの移行をサポートするようになりました。いずれかのコンテキストから設定を移行するか、すべてのルーテッドファイアウォールモードのコンテキストから設定をマージして移行するかを選択できます。複数のトランスペアレントファイアウォールモードコンテキストからの設定のマージのサポートは、まもなく利用可能になります。詳細については、「ASA プライマリ セキュリティ コンテキストの選択」を参照してください。 • 移行ツールは、仮想ルーティングおよび転送（VRF）機能を活用して、マルチコンテキストの ASA 環境で観察される分離されたトラフィックフローを複製します。これは、新たにマージされた設定の一部になります。移行ツールが検出したコンテキストの数は、新しい [コンテキスト (Contexts)] タイルで確認でき、解析後は [解析の概要 (Parsed Summary)] ページの新しい [VRF] タイルで確認できます。また移行ツールは、[セキュリティゾーンとインターフェイスグループへのインターフェイスのマッピング (Map Interfaces to Security Zones and Interface Groups)] ページに、これらの VRF がマッピングされているインターフェイスを表示します。 • Cisco Secure Firewall 移行ツールの新しいデモモードを使用して移行ワークフロー全体を試し、実際の移行がどのようになるかを可視化できるようになりました。詳細については、「ファイアウォール移行ツールでのデモモードの使用」を参照してください。 • 新しい機能拡張とバグの修正により、Cisco Secure Firewall 移行ツールは、Palo Alto Networks ファイアウォールの Threat Defense への移行に関して、改善された迅速な移行エクスペリエンスをご提供します。
4.0.3	<p>Cisco Secure Firewall 移行ツール 4.0.3 には、バグの修正と、次の新たな拡張機能が含まれています。</p> <ul style="list-style-type: none"> • 移行ツールで、PAN 設定を Threat Defense に移行するための強化された [アプリケーションマッピング (Application Mapping)] 画面が提供されるようになりました。詳細については、『移行ツールを使用した Palo Alto Networks ファイアウォールから Cisco Secure Firewall Threat Defense への移行』ガイドの「構成とアプリケーションのマッピング」を参照してください。

バージョン	サポートされる機能
4.0.2	<p>Cisco Secure Firewall 移行ツール 4.0.2 には、次の新機能と拡張機能が含まれています。</p> <ul style="list-style-type: none"> 移行ツールに常時接続のテレメトリが追加されました。ただし、限定的なテレメトリデータまたは広範なテレメトリデータの送信を選択できるようになっています。限定的なテレメトリデータにデータポイントはほとんど含まれませんが、広範なテレメトリデータは、より詳細なテレメトリデータのリストを送信します。この設定は、[設定 (Settings)] > [テレメトリデータをシスコに送信しますか (Send Telemetry Data to Cisco?)] から変更できます。

Cisco Secure Firewall 移行ツールのライセンス

Cisco Secure Firewall 移行ツールアプリケーションは無料であり、ライセンスは必要ありません。

Cisco Secure Firewall 移行ツールのプラットフォーム要件

Cisco Secure Firewall 移行ツールには、次のインフラストラクチャとプラットフォームの要件があります。

- Microsoft 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 以降で実行している
- Google Chrome がシステムのデフォルトブラウザである
- (Windows) [Power & Sleep] で [Sleep] 設定が [Never put the PC to Sleep] に設定されているため、大規模な移行プッシュ中にシステムがスリープ状態にならない
- (macOS) 大規模な移行プッシュ中にコンピュータとハードディスクがスリープ状態にならないように [Energy Saver] 設定が構成されている

Threat Defense デバイスの要件および前提条件

Management Center に移行する際は、対象 Threat Defense デバイスを追加することは必須ではありません。ポリシーは、Threat Defense デバイスの今後のデプロイに向けて Management Center に移行できます。

Threat Defense デバイスが Management Center に追加されている場合、Azure 構成を Threat Defense に移行するには、次の要件と前提条件を考慮します。

- ターゲット Threat Defense デバイスは、管理センターに登録されている必要があります。

- ターゲットの Threat Defense デバイスは、高可用性構成にすることができます。
- Threat Defense デバイスは、スタンドアロンデバイスまたはコンテナインスタンスにすることができます。クラスタの一部になることは**できません**。
 - ターゲット Threat Defense デバイスがコンテナインスタンスである場合、最低でも、Azure と同数の物理インターフェイス、物理サブインターフェイス、ポートチャンネルインターフェイス、およびポートチャンネルサブインターフェイス（「管理専用」を除く）が使用されている必要があります。使用されていない場合、ターゲット Threat Defense デバイスに必要な種類のインターフェイスを追加する必要があります。



- (注)
- サブインターフェイスは、Cisco Secure Firewall 移行ツールでは作成されません。インターフェイスマッピングのみが許可されます。
 - 異なるインターフェイスタイプ間のマッピングは許可されません。たとえば、物理インターフェイスをポートチャンネルインターフェイスにマップできます。

注意事項と制約事項

Cisco Secure Firewall 移行ツールは、変換中にルールまたはポリシーで使用されるかどうかにかかわらず、サポートされているすべてのオブジェクトおよびルールに対して 1 対 1 のマッピングを作成します。Cisco Secure Firewall 移行ツールには、未使用のオブジェクト（ACL および NAT で参照されていないオブジェクト）の移行を除外できる最適化機能があります。

Cisco Secure Firewall 移行ツールは、サポートされていないオブジェクト、NAT ルール、およびルートに移行しません。

Azure 構成の制限

送信元 Azure 構成の移行には、次の制限があります。

- インターフェイスとルートの構成を手動で Firewall Threat Defense に移行する必要があります

Azure 移行のガイドライン

ソース構成ファイルは、次のファイルで構成される zip 形式にする必要があります。

- Azure ポータルからエクスポートされた、`template.json` ファイル
- PowerShell を使用してエクスポートされた、IP グループデータで構成された `IPGroup.txt` ファイル

サポートされている Azure 構成

Cisco Secure Firewall 移行ツールは、次の Azure 構成を完全に移行できます。

- アクセス コントロール リスト
- ネットワーク オブジェクト
- サービス オブジェクト
- ネットワーク オブジェクト グループ (IPGroup)
- 宛先 NAT (D-NAT)
- FQDN
- IP グループ
- URL



(注) Firewall Threat Defense で上記の構成を移行するには、Firewall Management Center および Firewall Threat Defense のバージョンが 6.6 以降である必要があります。サービスオブジェクトの構成を移行する場合、Firewall Threat Defense のバージョンは 6.4 以降である必要があります。

Threat Defense デバイスに関する注意事項と制約事項

Azure 構成を Firewall Threat Defense に移行する予定で、ルート、インターフェイスなど、Threat Defense に既存のデバイス固有の構成がある場合、プッシュ移行中に Cisco Secure Firewall 移行ツールは自動的にデバイスを消去し、Azure 構成から上書きします。



(注) デバイス (ターゲット Threat Defense) 構成データの望ましくない損失を防ぐために、移行前にデバイスを手動で消去することを推奨します。

サポートされる移行先の管理センター

Cisco Secure Firewall 移行ツールは、管理センターおよびクラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスへの移行をサポートします。

Management Center

管理センターは強力な Web ベースのマルチデバイスマネージャです。独自のサーバーハードウェア上で、またはハイパーバイザ上の仮想デバイスとして稼働します。移行のためのターゲット管理センターとして、オンプレミス管理センターと仮想管理センターの両方を使用できます。

管理センターは、移行に関する次のガイドラインを満たす必要があります。

- 移行でサポートされる Management Center ソフトウェアバージョン ([移行でサポートされるソフトウェアのバージョン \(24 ページ\)](#)) を参照)。
- Azure の移行でサポートされるクラウド提供型またはオンプレミス Firewall Management Center ソフトウェアのバージョンは 6.6 以降です。
- Azure インターフェイスから移行する予定の以下に記載されているすべての機能を含む Firewall Threat Defense のスマートライセンスを取得済みおよびインストール済みであること。
 - Cisco.com の「[Cisco Smart Accounts](#)」の「Getting Started」セクション。
 - [Register the Firepower Management Center with the Cisco Smart Software Manager](#) [英語]
 - [Licensing the Firewall System](#) [英語]
 - REST API の Firewall Management Center が有効になっています。

Firewall Management Center Web インターフェイスで、[システム (System)] > [設定 (Configuration)] > [Rest API設定 (Rest API Preferences)] > [Rest APIを有効にする (Enable Rest API)] に移動し、[Rest APIを有効にする (Enable Rest API)] チェックボックスをオンにします。



重要 REST API を有効にするには、Firewall Management Center の管理者ユーザーロールが必要です。管理センターのユーザーロールの詳細については、「[ユーザーロール](#)」を参照してください。

クラウド提供型 Firewall Management Center

クラウド提供型 Firewall Management Center は、Threat Defense デバイスの管理プラットフォームであり、Cisco Defense Orchestrator (旧 Cisco Defense Orchestrator) を介して提供されます。クラウド提供型 Firewall Management Center は、管理センターと同じ機能を多数提供します。

CDO からクラウド提供型 Firewall Management Center にアクセスできます。CDO は、Secure Device Connector (SDC) を介してクラウド提供型 Firewall Management Center に接続します。クラウド提供型 Firewall Management Center の詳細については、「[クラウド提供型 Firewall Management Center による Cisco Secure Firewall Threat Defense デバイスの管理](#)」を参照してください。

Cisco Secure Firewall 移行ツールは、移行先の管理センターとしてクラウド提供型 Firewall Management Center をサポートしています。クラウド提供型 Firewall Management Center を移行先の管理センターとして選択するには、CDO の地域を追加し、CDO ポータルから API トークンを生成する必要があります。

CDO の地域

CDO は 3 つの異なる地域で利用でき、地域は URL 拡張子で識別できます。

表 1: CDO の地域と URL

地域	CDO URL
欧州	https://eu.manage.security.cisco.com/
US	https://us.manage.security.cisco.com/
APJC	https://apj.manage.security.cisco.com/
オーストラリア	https://au.manage.security.cisco.com/
インド	https://in.manage.security.cisco.com/

移行でサポートされるソフトウェアのバージョン

以下は、移行でサポートされている Cisco Secure Firewall 移行ツール、 Azure および Firewall Threat Defense バージョンです。

サポートされている Cisco Secure Firewall 移行ツールのバージョン

software.cisco.com に掲載されているバージョンは、当社のエンジニアリングおよびサポート組織によって正式にサポートされているバージョンです。 software.cisco.com から最新バージョンの Cisco Secure Firewall 移行ツールをダウンロードすることを強くお勧めします。

送信元の Microsoft Azure ファイアウォール構成でサポートされている Management Center

Azure ファイアウォールの場合、Cisco Secure Firewall 移行ツールは、バージョン 6.6 以降が実行されている Management Center が管理する Management Center デバイスへの移行をサポートします。

サポートされる Firewall Threat Defense のバージョン

Cisco Secure Firewall 移行ツールでは、Threat defense 6.6 以降または FTD virtual 7.0 以降が実行されているデバイスへの移行が推奨されています。

Firewall Threat Defense のオペレーティングシステムとホスティング環境の要件を含めた Cisco Firewall のソフトウェアとハードウェアの互換性の詳細については、『[Cisco Firepower Compatibility Guide](#)』 [英語] を参照してください。



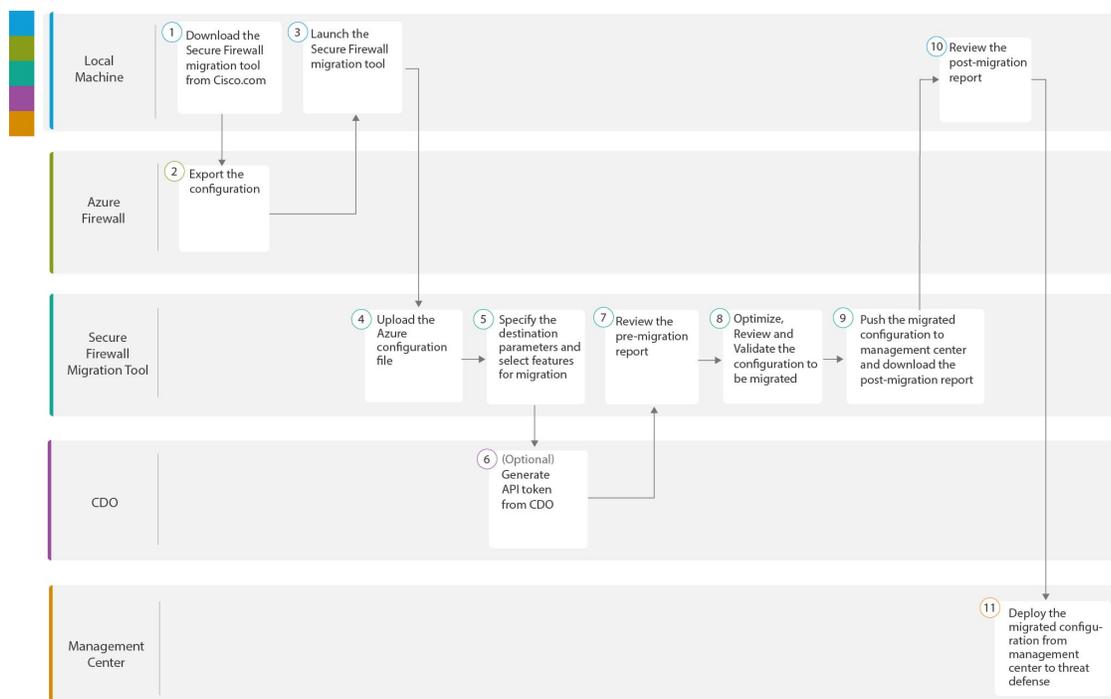
第 2 章

Microsoft Azure ネイティブファイアウォールから Threat Defense への移行ワークフロー

- [エンドツーエンドの手順 \(25 ページ\)](#)
- [移行の前提条件 \(27 ページ\)](#)
- [移行の実行 \(29 ページ\)](#)
- [Cisco Secure Firewall 移行ツールのアンインストール \(46 ページ\)](#)
- [移行例 : Azure から Threat Defense 2100 \(46 ページ\)](#)

エンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall 移行ツールを使用して、Microsoft Azure ネイティブファイアウォールを Threat Defense に移行するワークフローを示しています。



	ワークスペース	手順
①	Local Machine	Cisco.com から Cisco Secure Firewall 移行ツールをダウンロードします。詳細な手順については、「 Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード 」を参照してください。
②	Azure ファイアウォール	構成ファイルのエクスポート：Azure ファイアウォールから構成をエクスポートするには、 Microsoft Azure ネイティブファイアウォールからの構成のエクスポート (28 ページ) を参照してください。
③	Local Machine	ローカルマシンで Cisco Secure Firewall 移行ツールを起動します。「 Cisco Secure Firewall 移行ツールの起動 」を参照してください。
④	Cisco Secure Firewall 移行ツール	Azure ファイアウォールからエクスポートされた Azure 構成ファイルをアップロードします。 Microsoft Azure 構成ファイルのアップロード (32 ページ) を参照してください。
⑤	Cisco Secure Firewall 移行ツール	このステップでは、移行の接続先パラメータを指定できます。詳細な手順については、「 Cisco Secure Firewall 移行ツールの接続先パラメータの指定 」を参照してください。
⑥	CDO	(オプション) この手順はオプションであり、クラウドで提供される Firewall Management Center を移行先管理センターとして選択した場合にのみ必要です。詳細な手順については、「 Cisco Secure Firewall 移行ツールの接続先パラメータの指定、ステップ 1 」を参照してください。

	ワークスペース	手順
7	Cisco Secure Firewall 移行ツール	移行前レポートをダウンロードした場所に移動し、レポートを確認します。詳細な手順については、「 移行前レポートの確認 」を参照してください。
8	Cisco Secure Firewall 移行ツール	構成を慎重に確認し、それが適切で Threat Defense デバイスの構成内容と一致することを確認します。詳細な手順については、「 移行する構成の最適化、確認および検証 」を参照してください。
9	Cisco Secure Firewall 移行ツール	移行プロセスのこのステップでは、移行された構成を管理センターに送信し、移行後レポートをダウンロードできるようにします。詳細な手順については、「 移行された構成の Management Center へのプッシュ 」を参照してください。
10	Local Machine	移行後レポートをダウンロードした場所に移動し、レポートを確認します。詳細な手順については、「 移行後レポートの確認と移行の完了 」を参照してください。
11	Management Center	移行した構成を管理センターから Threat Defense に展開します。詳細な手順については、「 移行後レポートの確認と移行の完了 」を参照してください。

移行の前提条件

Microsoft Azure 構成を移行する前に、次のアクティビティを実行します。

Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード

始める前に

Cisco.com へのインターネット接続が可能な Windows 10 64 ビットまたは macOS バージョン 10.13 以降のマシンが必要です。

CDO でホストされている Cisco Secure Firewall 移行ツールのクラウドバージョンを使用する場合は、手順 4 に進みます。

手順

ステップ 1 コンピュータで、Cisco Secure Firewall 移行ツール用のフォルダを作成します。

このフォルダには、他のファイルを保存しないことをお勧めします。Cisco Secure Firewall 移行ツールを起動すると、ログ、リソース、およびその他すべてのファイルがこのフォルダに配置されます。

(注)

Cisco Secure Firewall 移行ツールの最新バージョンをダウンロードする場合は、必ず新しいフォルダを作成し、既存のフォルダは使用しないでください。

ステップ 2 <https://software.cisco.com/download/home/286306503/type> を参照し、[Firewall移行ツール (Firewall Migration Tool)] をクリックします。

上記のリンクをクリックすると、[Firewall NGFWバーチャル (Firewall NGFW Virtual)] の [Cisco Secure Firewall移行ツール (Firewall Migration Tool)] に移動します。Firewall Threat Defense デバイスのダウンロード領域から Cisco Secure Firewall 移行ツールをダウンロードすることもできます。

ステップ 3 Cisco Secure Firewall 移行ツールの最新バージョンを、作成したフォルダにダウンロードします。

Windows 用または macOS マシン用の Cisco Secure Firewall 移行ツールの適切な実行可能ファイルをダウンロードしていることを確認してください。

ステップ 4 CDO ユーザーでそこにホストされている移行ツールを使用する場合は、CDO テナントにログインして、左側のペインで、[管理 (Administration)]>[移行 (Migration)]>[ファイアウォール移行ツール (Firewall Migration Tool)] に移動して、移行インスタンスを作成します。

Microsoft Azure ネイティブファイアウォールからの構成のエクスポート

次の手順を実行して、Microsoft Azure の構成をエクスポートします。

- [Azure ファイアウォール GUI からのポリシー構成のエクスポート \(28 ページ\)](#)
- [IP グループ構成のエクスポート \(29 ページ\)](#)

Azure ファイアウォール GUI からのポリシー構成のエクスポート

この手順を使用して、Microsoft Azure ファイアウォール GUI からポリシー構成をエクスポートします。

手順

ステップ 1 Microsoft Azure ファイアウォール GUI で、[ポリシー (Policy)] を選択します。

ステップ 2 [自動化 (Automation)] セクションで、[テンプレートをエクスポート (Export Template)] を選択します。

ステップ 3 [ダウンロード (Download)] ボタンをクリックして、構成をダウンロードします。

ポリシー構成は、zip 形式でダウンロードされます。template.json ファイルを抽出します。

次のタスク

- [IP グループ構成のエクスポート \(29 ページ\)](#)

IP グループ構成のエクスポート

この手順を使用して、Microsoft Azure PowerShell から IP アドレスグループ構成を抽出します

手順

ステップ 1 PowerShell を開き、次のコマンドを実行します。

```
Get-AzIpGroup -ResourceGroupName "your_ResourceGrp_name" | Select Name, IPAddresses
```

(注)

your_ResourceGrp_name をリソースグループ名に置き換えます。

ステップ 2 出力結果をテキストファイルにコピーし、“IPGroup.txt”として保存します。

次のタスク

[Microsoft Azure 構成ファイルのアップロード \(32 ページ\)](#)

移行の実行

Cisco Secure Firewall 移行ツールの起動

このタスクは、デスクトップバージョンの Cisco Secure Firewall 移行ツールを使用している場合にのみ適用されます。CDO でホストされている移行ツールのクラウドバージョンを使用している場合は、[Microsoft Azure 構成ファイルのアップロード \(32 ページ\)](#)に進みます。



(注) 移行ツールのデスクトップバージョンを起動すると、別のウィンドウでコンソールが開きます。移行が進むのに合わせて、Cisco Secure Firewall 移行ツールの現在のステップの進行状況がコンソールに表示されます。画面にコンソールが表示されない場合は、Cisco Secure Firewall 移行ツールの背後にある可能性があります。

始める前に

- [Cisco.com](#) からの Cisco Secure Firewall 移行ツールのダウンロード
- Cisco Secure Firewall 移行ツールを実行するために、最新バージョンの Google Chrome ブラウザがコンピュータにインストールされていることを確認します。Google Chrome をデフォルトのブラウザとして設定する方法については、「[Set Chrome as your default web browser](#)」を参照してください。

- 大規模な構成ファイルを移行する場合は、移行プッシュ中にシステムがスリープ状態にならないようにスリープ設定を構成します。

手順

ステップ 1 コンピュータで、Cisco Secure Firewall 移行ツールをダウンロードしたフォルダに移動します。

ステップ 2 次のいずれかを実行します。

- Windows マシンで、Cisco Secure Firewall 移行ツールの実行可能ファイルをダブルクリックして、Google Chrome ブラウザで起動します。

プロンプトが表示されたら、[はい (Yes)] をクリックして、Cisco Secure Firewall 移行ツールがシステムに変更を加えることができるようにします。

(注)

ログインポップアップの表示を妨げる可能性があるため、ブラウザのポップアップブロッカーを必ず無効にします。

Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 移行ツールの存在するフォルダに保存します (ログおよびリソースのフォルダを含む)。

- Mac では、Cisco Secure Firewall 移行ツールの *.command ファイルを目的のフォルダに移動し、ターミナルアプリケーションを起動して、Cisco Secure Firewall 移行ツールがインストールされているフォルダを参照し、次のコマンドを実行します。

```
# chmod 750 Firewall_Migration_Tool-version_number.command
# ./Firewall_Migration_Tool-version_number.command
```

Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 移行ツールの存在するフォルダに保存します (ログおよびリソースのフォルダを含む)。

ヒント

Cisco Secure Firewall 移行ツールを開こうとすると、警告ダイアログが表示されます。これは、身元が明らかな開発者によって Cisco Secure Firewall 移行ツールが Apple に登録されていないためです。身元不明の開発者によるアプリケーションを開く方法については、「[開発元が不明な Mac アプリを開く](#)」を参照してください。

(注)

MAC のターミナルの zip メソッドを使用します。

ステップ 3 [エンドユーザライセンス契約 (End User License Agreement)] ページで、テレメトリ情報をシスコと共有する場合は、[Cisco Success Network と情報を共有することに同意 (I agree to share data with Cisco Success Network)] をクリックし、それ以外の場合は [後で行う (I'll do later)] をクリックします。

Cisco Success Network に統計を送信することに同意すると、Cisco.com アカウントを使用してログインするように求められます。Cisco Success Network に統計を送信しないことを選択した場合は、ローカルログイン情報を使用して Cisco Secure Firewall 移行ツールにログインします。

ステップ 4 Cisco Secure Firewall 移行ツールのログインページで、次のいずれかを実行します。

- Cisco Success Network と統計を共有するには、[CCOでログイン (Login with CCO)] リンクをクリックし、シングルサインオンログイン情報を使用してCisco.comアカウントにログインします。Cisco.comアカウントがない場合は、Cisco.com のログインページで作成します。

Cisco.com アカウントを使用してログインしている場合は、[ステップ 8](#)に進みます。

- インターネットにアクセスできないエアギャップネットワークにファイアウォールを展開した場合は、Cisco TACに連絡して、管理者のログイン情報で動作するビルドを入手してください。このビルドでは使用状況の統計がシスコに送信されず、TACがログイン情報を提供できることに注意してください。

ステップ 5 [パスワードのリセット (Reset Password)] ページで、古いパスワードと新しいパスワードを入力し、新しいパスワードを確認します。

新しいパスワードは 8 文字以上で、大文字と小文字、数字、および特殊文字を含める必要があります。

ステップ 6 [リセット (Reset)] をクリックします。

ステップ 7 新しいパスワードでログインします。

(注)

パスワードを忘れた場合は、既存のすべてのデータを <migration_tool_folder> から削除し、Cisco Secure Firewall 移行ツールを再インストールします。

ステップ 8 移行前チェックリストを確認し、記載されているすべての項目を完了していることを確認します。

チェックリストの項目を 1 つ以上完了していない場合は、完了するまで続行しないでください。

ステップ 9 [新規移行 (New Migration)] をクリックします。

ステップ 10 [ソフトウェアアップデートを確認 (Software Update Check)] 画面で、Cisco Secure Firewall 移行ツールの最新バージョンを実行しているかどうか不明な場合は、Cisco.com でバージョンを確認します。

ステップ 11 [続行 (Proceed)] をクリックします。

次のタスク

次のステップに進むことができます。

- お使いのコンピュータにFDM管理対象デバイス構成をエクスポートした場合は、[Microsoft Azure 構成ファイルのアップロード \(32 ページ\)](#)に進みます。

Cisco Secure Firewall 移行ツールでのデモモードの使用

Cisco Secure Firewall 移行ツールを起動し、[送信元設定の選択 (Select Source Configuration)] ページで、[移行の開始 (Start Migration)] を使用して移行を開始するか、[デモモード (Demo Mode)] に入るかを選択できます。

デモモードでは、ダミーデバイスを使用してデモ移行を実行し、実際の移行フローがどのようになるかを可視化できます。移行ツールは、[送信元ファイアウォールベンダー (Source Firewall

Vendor)] ドロップダウンでの選択に基づいてデモモードをトリガーします。構成ファイルをアップロードするか、ライブデバイスに接続して移行を続行することもできます。デモ FMC やデモ FTD デバイスなどの送信元デバイスや対象デバイスを選択すると、デモの移行を実行できます。



注意 [デモモード (Demo Mode)] を選択すると、既存の移行ワークフローがあれば消去されます。[移行の再開 (Resume Migration)] にアクティブな移行があるときにデモモードを使用すると、アクティブな移行は失われ、デモモードを使用した後に最初から再開する必要があります。

移行前レポートをダウンロードして確認し、実際の移行ワークフローで実行するその他のアクションを実行することもできます。ただし、デモ移行は設定の検証までしか実行できません。これはデモモードにすぎないため、選択したデモターゲットデバイスに設定をプッシュすることはできません。検証ステータスと概要を確認し、[デモモードの終了 (Exit Demo Mode)] をクリックして [送信元設定の選択 (Select Source Configuration)] ページに再度移動し、実際の移行を開始できます。



(注) デモモードでは、設定のプッシュを除く Cisco Secure Firewall 移行ツールのすべての機能セットを活用して、実際の移行を行う前にエンドツーエンドの移行手順のトライアルを実行できます。

Microsoft Azure 構成ファイルのアップロード

次の手順を実行して、Microsoft Azure 構成ファイルを Firewall 移行ツールにアップロードします。

始める前に

- 送信元 Azure デバイスからポリシーと IP グループ構成ファイルをエクスポートします。詳細については、「[Microsoft Azure ネイティブファイアウォールからの構成のエクスポート \(28 ページ\)](#)」を参照してください。
- 抽出した IPGroup.txt ファイルと template.json ファイルを含む zip ファイルを作成します。



(注) Azure 環境で IPGroup が構成されていない場合は、移行に template.json ファイルのみを使用します。

手順

ステップ 1 Cisco Secure Firewall 移行ツールを起動します。

ステップ 2 [ソース構成を選択 (Select Source Configuration)] ウィンドウのドロップダウンリストで、[Microsoft Azure] を選択し、[移行を開始 (Start Migration)] をクリックします。

The screenshot shows the 'Select Source Configuration' interface. The 'Source Firewall Vendor' dropdown is set to 'Microsoft Azure'. Below it are 'Start Migration' and 'Demo Mode' buttons. To the right is a 'Microsoft Azure Pre-Migration Instructions' panel. The panel contains a warning: 'This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) when migration is in progress.' Below this is a 'Session Telemetry' section explaining data collection. An 'Acronyms used' section lists: FMT: Firewall Migration Tool, FMC: Firewall Management Center, and FTD: Firewall Threat Defense. A final section lists prerequisites: 'Stable IP Connection', 'FMC Version' (7.2 or later), and 'FMC Account' (dedicated user account).

ステップ 3 [構成情報を抽出 (Extract Config Information)] ウィンドウで [アップロード (Upload)] をクリックし、ローカルマシンで zip ファイルを選択します。

[解析サマリー (Parsed Summary)] セクションに解析ステータスが表示されます。

ステップ 4 アップロードされた構成ファイルで、Cisco Secure Firewall 移行ツールが検出して解析した要素の概要を確認します。

Cisco Secure Firewall 移行ツールの接続先パラメータの指定

始める前に

CDOでホストされるクラウドバージョンの移行ツールを使用している場合は、[手順3](#)に進んでください。

- オンプレミス Firewall Management Center の Firewall Management Center の IP アドレスを取得します。
- Cisco Secure Firewall 移行ツール 3.0 以降では、オンプレミスの Firewall Management Center またはクラウド提供型 Firewall Management Center を選択できます。
- クラウド提供型 Firewall Management Center の場合、リージョンと API トークンを指定する必要があります。詳細については、「[サポートされる移行先の管理センター](#)」を参照してください。
- (任意) Firewall Management Center に追加します。「[Adding Devices to the Firewall Management Center](#)」を参照してください。

手順

ステップ 1 [ターゲットの選択 (Select Target)] 画面の [ファイアウォール管理 (Firewall Management)] セクションで、次の手順を実行します。オンプレミスのファイアウォール管理センターまたはクラウド提供型ファイアウォール管理センターへの移行を選択できます。

- オンプレミスのファイアウォール管理センターに移行するには、次の手順を実行します。

- a) [オンプレミス FMC (On-Prem FMC)] オプションボタンをクリックします。
- b) 管理センターの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
- c) [接続 (Connect)] をクリックして、**手順 2** に進みます。

- クラウド提供型 Firewall Management Center に移行するには、次の手順を実行します。

- a) [クラウド提供型 FMC (Cloud-delivered FMC)] オプションボタンをクリックします。
- b) リージョンを選択し、CDO API トークンを貼り付けます。CDO から API トークンを生成するため、以下の手順に従います。
 1. CDO にログインします。
 2. 右上隅から、[設定 (Preferences)] > [一般設定 (General Preferences)] に移動し、[マイトークン (My Tokens)] セクションから API トークンをコピーします。

- c) [接続 (Connect)] をクリックして、**手順 2** に進みます。

ステップ 2 [Firewall Management Centerへのログイン (Firewall Management Center Login)] ダイアログボックスで、Cisco Secure Firewall 移行ツール専用アカウントのユーザー名とパスワードを入力し、[ログイン (Login)] をクリックします。

Cisco Secure Firewall 移行ツールは Firewall Management Center にログインし、その Firewall Management Center による管理対象 Firewall Threat Defense デバイスのリストを取得します。この手順の進行状況はコンソールで確認できます。

ステップ 3 [ターゲットを選択 (Select Target)] 画面の [Threat Defenseを選択 (Choose Threat Defense)] セクションで、移行する Firewall Threat Defense デバイスを選択するか、Firewall Threat Defense デバイスが無い場合は、Azure構成の共有ポリシー (アクセス制御リスト、NAT、およびオブジェクト) を Firewall Management Center に移行します。

ステップ 4 [FTDの選択 (Choose FTD)] セクションで、次のいずれかを実行します。

- [FTDデバイスを選択 (Select FTD Device)] ドロップダウンリストをクリックし、Azure 構成を移行するデバイスをオンにします。

(注)

このリストには、スタンドアロンの Threat Defense デバイスと、ターゲット Firewall Management Center の高可用性 (HA) ペアの一部であるデバイスの両方が含まれます。

選択した Firewall Management Center ドメイン内のデバイスが、[IPアドレス (IP Address)]、[名前 (Name)]、[デバイスモデル (Device Model)]、および[モード (Mode)] (ルーテッドまたはトランスペアレント) 別に表示されます。

- [FTD を使用せず続行 (Proceed without FTD)] をクリックして、構成を Firewall Management Center に移行します。

Firewall Threat Defense なしで続行すると、Cisco Secure Firewall 移行ツールは Firewall Threat Defense に構成またはポリシーをプッシュしません。したがって、Firewall Threat Defense のデバイス固有の校正であるインターフェイスとルート、およびサイト間 VPN は移行されず、Firewall Management Center で手動で構成する必要があります。ただし、NAT、ACL、ポートオブジェクトなど、サポートされている他のすべての構成 (共有ポリシーとオブジェクト) は移行されます。リモートアクセス VPN は共有ポリシーであり、Threat Defense なしでも移行できます。

ステップ 5 [続行 (Proceed)] をクリックします。

移行先に応じて、Cisco Secure Firewall 移行ツールを使用して移行する機能を選択できます。

ステップ 6 [機能の選択 (Select Features)] セクションをクリックして、移行先に移行する機能を確認して選択します。

- 接続先 Firewall Threat Defense デバイスを移行する場合、Cisco Secure Firewall 移行ツールは、[デバイス構成 (Device Configuration)] および [共有構成 (Shared Configuration)] セクションの Azure 構成からの移行で利用可能な機能を自動で選択します。要件に応じて、デフォルトの選択をさらに変更できます。
- Firewall Management Center に移行する場合、Cisco Secure Firewall 移行ツールは、[デバイス構成 (Device Configuration)]、[共有構成 (Shared Configuration)] および [最適化 (Optimization)] セクションの Azure 構成からの移行で利用可能な機能を自動で選択します。要件に応じて、デフォルトの選択をさらに変更できます。

(注)

[デバイス構成 (Device Configuration)] セクションは、Azure 移行には適用されません。インターフェイスとルートの移行は、手動で実行する必要があります。

- (任意) [Optimization] セクションで、[Migrate only referenced objects] を選択して、アクセス コントロール ポリシーと NAT ポリシーで参照されているオブジェクトのみを移行します。

(注)

このオプションを選択すると、Azure 構成の参照されていないオブジェクトは、移行されません。これにより、移行時間が最適化され、未使用のオブジェクトが構成から消去されます。

ステップ 7 [続行 (Proceed)] をクリックします。

ステップ 8 [Rule Conversion/ Process Config] セクションで、[Start Conversion] をクリックして変換を開始します。

ステップ 9 Cisco Secure Firewall 移行ツールによって変換された要素の概要を確認します。

構成ファイルが正常にアップロードおよび解析されたかどうかを確認するには、移行を続行する前に**移行前レポート**をダウンロードして確認します。

ステップ 10 [レポートのダウンロード (Download Report)] をクリックし、**移行前レポート**を保存します。

移行前レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある Resources フォルダに保存されます。

次のタスク

[移行前レポートの確認 \(36 ページ\)](#)

移行前レポートの確認



(注) 移行前レポートのすべての内容をよく確認してください。サポートされていないルールは完全に移行されないため、元の構成が変更されたり、トラフィックが制限されたり、不要なトラフィックが許可されたりする場合があります。構成が正常に移行されたら、Firewall Management Center で関連するルールとポリシーを更新して、トラフィックが適切に処理されているか確認することをお勧めします。

移行中に移行前レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行前レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/pre_migration_summary_html_format



(注) レポートは、Cisco Secure Firewall 移行ツールの実行中にのみダウンロードできます。

手順

ステップ 1 移行前レポートをダウンロードした場所に移動します。

移行前レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある Resources フォルダに保存されます。

ステップ 2 移行前レポートを開き、その内容を慎重に確認して、移行が失敗する原因となる問題を特定します。

移行前レポートには、次の情報が含まれています。

- Firewall Threat Defense への移行に成功したサポートされている Azure 構成要素と移行用に選択された特定の Azure 機能のサマリー。
- エラーがある構成行：Cisco Secure Firewall 移行ツールが解析できなかったために正常に移行できない Azure 構成要素の詳細。Azure 構成でこれらのエラーを修正し、新しい構成ファイルをエクスポートしたら、新しい構成ファイルを Cisco Secure Firewall 移行ツールにアップロードして、続行します。

- **無視された構成** : Firewall Management Center または Cisco Secure Firewall 移行ツールがサポートしていないために無視された Azure 構成要素の詳細。Cisco Secure Firewall 移行ツールはこれらの行を解析しません。これらの行を確認し、各機能が Firewall Management Center でサポートされているかどうかを確認します。サポートされている場合は、機能を手動で構成することを計画します。

Firewall Management Center と Firewall Threat Defense でサポートされる機能の詳細については、『[Management Center Configuration Guide](#)』 [英語] を参照してください。

- ステップ 3** 移行前レポートで修正措置が推奨されている場合は、Azure インターフェイスで、これらの修正を完了し、再度 構成ファイルをエクスポートし、更新された構成ファイルをアップロードして、続行します。
- ステップ 4** Azure 構成ファイルを正常にアップロードし、解析したら、Cisco Secure Firewall 移行ツールに戻り、[次へ (Next)] をクリックして移行を続行します。

最適化、構成の確認と検証

移行した Azure 構成を Firewall Management Center にプッシュする前に、構成を慎重に最適化および見直して、構成が正確で Firewall Threat Defense デバイスの構成内容と一致しているかを確認します。点滅しているタブは、次の一連のアクションを実行する必要があることを示しています。

タブで特定の構成項目を検索するには、列の上部にあるフィールドに項目名を入力します。テーブルの行はフィルタ処理され、検索語に一致する項目のみが表示されます。



- (注) デフォルトでは、[インライングループ化 (Inline Grouping)] オプションが有効になっていません。

Cisco Secure Firewall 移行ツールの ACL 最適化の概要

Cisco Secure Firewall 移行ツールは、ネットワーク機能に影響を与えることなく、ファイアウォールルールベースから最適化（無効化または削除）できる ACL を識別および分離するサポートを提供します。

ACL 最適化は、次の ACL タイプをサポートします。

- **冗長 ACL** : 2つの ACL の構成とルールのセットが同じ場合、基本以外の ACL を削除してもネットワークに影響はありません。たとえば、2つのルールが同じネットワーク上で FTP および IP トラフィックを許可し、アクセスを拒否するルールが定義されていない場合、最初のルールを削除できます。
- **シャドウ ACL** : 最初の ACL は、2番目の ACL の設定を完全にシャドウイングします。2つのルールに同様のトラフィックがある場合、2番目のルールはアクセスリストの後半に表示されるため、どのトラフィックにも適用されません。2つのルールがトラフィックに対して異なるアクションを指定している場合、シャドウイングされたルールを移動するか、いずれかのルールを編集して必要なポリシーを実装できます。たとえば、特定の送信

元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイングされたルールで FTP トラフィックを許可できます。

Cisco Secure Firewall 移行ツールは、ACL 最適化のルールを比較する際に次のパラメータを使用します。



(注) Azure では、ACP ルールアクションに対してのみ最適化を使用できます。

- 無効化された ACL は、最適化プロセス中に考慮されません。
- 送信元の ACL は、対応する ACE（インライン値）に展開された後、次のパラメータについて比較されます。
 - 送信元と宛先のゾーン
 - 送信元と宛先のネットワーク
 - 送信元/宛先ポート

ACL を選択し、[設定の最適化、確認、検証 (Optimize, Review and Validate Configuration)] ウィンドウの右上にある [ダウンロード (Download)] アイコンをクリックして、ACL 名と、対応する冗長 ACL およびシャドウ ACL を Excel ファイルで表形式にして見直します。

オブジェクトの最適化

次のオブジェクトは、移行プロセス中にオブジェクトの最適化について考慮されます。

- [ネットワーク オブジェクト (Network Object)]
- ポート オブジェクト
- URL オブジェクト

手順

ステップ 1 (オプション) [構成の最適化、確認および検証 (Optimize, Review and Validate Configuration)] 画面で、[アクセス制御 (Access Control)] > [ACP] の [ACL の最適化 (Optimize ACL)] をクリックして最適化コードを実行し、以下の操作を実行します。

- a) ルールを選択し、[アクション (Actions)] > [無効として移行 (Migrate as disabled)] または [移行しない (Do not migrate)] を選択して、いずれかのアクションを適用します。

(注)

[アクション (Actions)] > [編集 (Edit)] の順に選択すると、任意のルールを編集できます。

- b) [保存 (Save)] をクリックします。
移行操作が [移行しない (Do not migrate)] から [無効として移行 (Migrate as disabled)] またはその逆になります。

次のオプションを使用して、ルールの一括選択を実行できます。

- [移行 (Migrate)] : デフォルトの状態に移行します。
- [移行しない (Do not migrate)] : ACL の移行を無視します。
- [無効として移行 (Migrate as disabled)] : [状態 (State)] フィールドが [無効 (Disable)] に設定されている ACL を移行します。
- [有効として移行 (Migrate as enabled)] : [状態 (State)] フィールドが [有効 (Enable)] に設定されている ACL を移行します。

ステップ 2 [設定の最適化、確認、および検証 (Optimize, Review and Validate Configuration)] 画面で、[アクセス制御ルール (Access Control Rules)] をクリックし、次の手順を実行します。

- a) テーブル内の各エントリについて、マッピングを確認し、それらが正しいことを確認します。
- b) 1つ以上のアクセス制御リストポリシーを移行しない場合は、ポリシーのボックスをオンにして行を選択し、[アクション (Actions)] > [移行しない (Do not migrate)] を選択して、[保存 (Save)] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

- c) アクセス制御リストポリシーを編集するには、ポリシーのチェックボックスをオンにして行を選択し、[アクション (Actions)] > [編集 (Edit)] の順に選択します。

[ルールを編集 (Edit Rule)] ダイアログボックスが表示されます。選択したポリシーで、既存のデータを更新したり、新しいデータを追加したりできます。

オブジェクトを送信元または接続先に追加するには、次の手順を実行します。

1. オブジェクトのチェックボックスをオンにして、左側のペインからオブジェクトを選択します。
2. [選択した送信元 (Selected Sources)] または [選択した接続先およびアプリケーション (Selected Destination and Applications)] 列で、[送信元を追加 (Add Source)] または [宛先を追加 (Add Destination)] ボタンをクリックし、オブジェクトをそれぞれの場所に移動します。

[削除 (Delete)] アイコンをクリックすると、送信元または接続先から既存のオブジェクトを削除することもできます。

該当しないすべてのルールは、テーブルでグレーアウトされます。

- d) ロギングが有効になっているアクセスコントロールルールのロギングオプションを変更する場合は、該当する行のボックスをオンにし、[アクション (Actions)] > [ログ (Log)] を選択します。

[ログ (Log)] ダイアログでは、接続の開始時または終了時、またはその両方でイベントのロギングを有効にできます。ロギングを有効にする場合は、接続イベントを **イベントビューア** または **Syslog** のいずれか、または両方に送信することを選択する必要があります。接続イベントを **syslog** サーバに送信することを選択した場合、**Firewall Management Center** ですでに構成されている **syslog** ポリシーを [Syslog] ドロップダウンメニューから選択できます。

- e) [アクセスコントロール (Access Control)] テーブル内の移行されたアクセスコントロールルールのアクションを変更する場合は、該当する行のボックスをオンにし、[アクション (Actions)] > [ルールアクション (Rule Action)] を選択します。

ACE カウントは、昇順、降順、等しい、大なり、および小なりのフィルタリング順序シーケンスでフィルタ処理できます。

フィルタリング条件をクリアするには、[フィルタのクリア (Clear Filter)] をクリックします。

(注)

ACE に基づいた ACL のソート順序は、表示のみを目的としています。ACL は、発生した時間順に基づいてプッシュされます。

ステップ 3 次のタブをクリックし、構成項目を確認します。

- アクセス制御 (Access Control)
- オブジェクト (Objects) (ネットワークオブジェクト (Network Objects)、ポートオブジェクト (Port Objects)、URL オブジェクト (URL Objects))
- NAT

1 つ以上の NAT ルールまたはルートインターフェイスを移行しない場合は、該当する行のボックスをオンにし、[アクション (Actions)] > [移行しない (Do not migrate)] を選択して、[保存 (Save)] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

ステップ 4 (任意) グリッド内の各構成項目の詳細をダウンロードするには、[ダウンロード (Download)] をクリックします。

ステップ 5 確認が完了したら、[検証 (Validate)] をクリックします。注意が必要な必須フィールドは、値を入力するまで点滅し続けることに注意してください。[検証 (Validate)] ボタンは、すべての必須フィールドに入力した後にのみ有効になります。

検証中、Cisco Secure Firewall 移行ツールは Firewall Management Center に接続し、既存のオブジェクトを確認し、それらのオブジェクトを移行対象オブジェクトのリストと比較します。オブジェクトがすでに Firewall Management Center に存在する場合、Cisco Secure Firewall 移行ツールは次の処理を実行します。

- オブジェクトの名前と構成が同じ場合、Cisco Secure Firewall 移行ツールは既存のオブジェクトを再利用し、Firewall Management Center に新しいオブジェクトを作成しません。
- オブジェクトの名前が同じで構成が異なる場合、Cisco Secure Firewall 移行ツールはオブジェクトの競合を報告します。

検証の進行状況はコンソールで確認できます。

ステップ 6 検証が完了し、[検証ステータス (Validation Status)] ダイアログボックスに 1 つ以上のオブジェクトの競合が表示された場合は、次の手順を実行します。

a) [競合の解決 (Resolve Conflicts)] をクリックします。

Cisco Secure Firewall 移行ツールは、オブジェクトの競合が報告された場所に応じて、[ネットワークオブジェクト (Network Objects)] タブまたは [ポートオブジェクト (Port Objects)] タブのいずれかまたは両方に警告アイコンを表示します。

b) タブをクリックし、オブジェクトを確認します。

- c) 競合がある各オブジェクトのエントリを確認し、[アクション (Actions)] > [競合の解決 (Resolve Conflicts)] を選択します。
- d) [競合の解決 (Resolve Conflicts)] ウィンドウで、推奨アクションを実行します。
たとえば、既存の Firewall Management Center オブジェクトとの競合を避けるために、オブジェクト名にサフィックスを追加するように求められる場合があります。デフォルトのサフィックスを受け入れるか、独自のサフィックスに置き換えることができます。
- e) [解決 (Resolve)] をクリックします。
- f) タブ上のすべてのオブジェクトの競合を解決したら、[保存 (Save)] をクリックします。
- g) [検証 (Validate)] をクリックして構成を再検証し、すべてのオブジェクトの競合を解決したことを確認します。

ステップ 7 検証が完了し、[検証ステータス (Validation Status)] ダイアログボックスに「Successfully Validated」というメッセージが表示されたら、[移行された構成の以下へのプッシュ : Firewall Management Center \(41 ページ\)](#)に進みます。

移行された構成の以下へのプッシュ : Firewall Management Center

構成を正常に検証しておらず、すべてのオブジェクト競合を解決していない場合、移行済み Azure 構成を、Firewall Management Center にプッシュできません。

移行プロセスのこのステップでは、移行された構成を Firewall Management Center に送信します。Firewall Threat Defense デバイスに構成を展開しません。ただし、Firewall Threat Defense 上の既存の構成はこのステップで消去されます。



- (注) Cisco Secure Firewall 移行ツールが移行された構成を Firewall Management Center に送信している間は、構成を変更したり、デバイスに展開したりしないでください。

手順

ステップ 1 [検証ステータス (Validation Status)] ダイアログボックスで、検証の概要を確認します。

ステップ 2 [構成をプッシュ (Push Configuration)] をクリックして、移行済み Azure 構成を Firewall Management Center に送信します。

Cisco Secure Firewall 移行ツールに、移行の進行状況の概要が表示されます。コンソールに、Firewall Management Center にプッシュされているコンポーネントの詳細な進行状況を行ごとに表示できます。

(注)

一括設定プッシュの実行中にエラーのある設定がある場合、移行ツールは警告をスローし、移行を中止してエラーを手動で修正するか、誤った設定を除外して移行を続行することを求めます。エラーのある設定を表示してから、[移行の続行 (Continue with migration)] または [中止 (Abort)] を選択できます。移行を

中止する場合は、トラブルシューティングバンドルをダウンロードし、分析のために Cisco TAC と共有できます。

移行を続行する場合は、移行ツールは移行を部分的に成功した移行として扱います。移行後レポートをダウンロードして、プッシュエラーが原因で移行されなかった設定のリストを表示できます。

ステップ 3 移行が完了したら、[レポートのダウンロード (Download Report)] をクリックして、移行後レポートをダウンロードして保存します。

移行後レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある Resources フォルダに保存されます。

ステップ 4 移行が失敗した場合は、移行後レポート、ログファイル、および未解析ファイルを慎重に確認して、失敗の原因を把握します。

トラブルシューティングについては、サポートチームに問い合わせることもできます。

移行の失敗のサポート

移行に失敗する場合は、サポートにお問い合わせください。

1. [移行完了 (Complete Migration)] 画面で、[サポート (Support)] ボタンをクリックします。

ヘルプサポートページが表示されます。

2. [サポートバンドル (Support Bundle)] チェックボックスをオンにして、ダウンロードする構成ファイルを選択します。

(注)

ログファイルと DB ファイルは、デフォルトでダウンロード用に選択されています。

3. [ダウンロード (Download)] をクリックします。

サポートバンドルファイルは、ローカルパスに .zip としてダウンロードされます。Zip フォルダを抽出して、ログファイル、DB、および構成ファイルを表示します。

4. [Email us] をクリックして、テクニカルチームに障害の詳細を電子メールで送信します。

ダウンロードしたサポートファイルを電子メールに添付することもできます。

5. [TAC ページに移動 (Visit TAC page)] をクリックして、シスコのサポートページで TAC ケースを作成します。

(注)

TAC ケースは、移行中にいつでもサポートページからオープンできます。

移行後レポートの確認と移行の完了

移行後のレポートには、さまざまなカテゴリの ACL カウント、ACL 最適化、および構成ファイルで実行された最適化の全体的なビューに関する詳細が表示されます。詳細については、[最適化、構成の確認と検証 \(37 ページ\)](#) を参照してください。

移行中に移行後レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行後レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/post_migration_summary_html_format



(注) レポートは、Cisco Secure Firewall 移行ツールの実行中のみダウンロードできます。

手順

ステップ 1 移行後レポートをダウンロードした場所に移動します。

ステップ 2 移行後レポートを開き、その内容を慎重に確認して、Azure 構成がどのように移行されたかを把握します。

- **移行概要**：Azure ファイアウォールから Firewall Threat Defense に正常に移行された構成の概要です。これには、送信元 Azure デバイス、ターゲット Firewall Threat Defense デバイスおよび正常に移行された構成要素の情報が含まれます。
また、移行前の状態と移行後の状態の差異を示す比較チャートも確認できます。
- **一部のポリシー移行**：移行に対して選択された特定の Azure 機能の詳細は、[デバイス構成機能 (Device Configuration Features)]、[共有構成機能 (Shared Configuration Features)]、および [最適化 (Optimization)] の 3 つのカテゴリ内で使用できます。
- **オブジェクト競合処理**：Firewall Management Center の既存オブジェクトと競合していると認識された Azure ファイアウォール オブジェクトの詳細。オブジェクトの名前が同じで構成が異なる場合は、これらのオブジェクトの名前を変更できます。これらのオブジェクトを慎重に見直して、競合が適切に解決されているかを確認します。
- **最適化**：Azure ファイアウォールオブジェクトと ACL 最適化の詳細。オブジェクトの名前と設定が同じ場合、移行ツールは、management center オブジェクトを再利用します。これらのオブジェクトを慎重に見直して、競合が適切に解決されているかを確認します。
- **ACL カテゴリの競合処理**：management center の命名制限と競合していると特定された ACL ルールカテゴリの詳細。カテゴリ名は、management center でサポートされている制限を超えた場合、トリミングされます。これらのカテゴリを慎重に見直してください。
- **Partially Migrated Configuration**：詳細オプションなしでもルールを移行できる詳細オプション付きルールを含む、一部のみ移行されたルールの詳細。これらの行を確認し、詳細オプションが Firewall Management Center でサポートされているかどうかを確認します。サポートされている場合は、これらのオプションを手動で構成します。
- **変換された機能に対して実行するアクション**：移行ツールを使用して移行しないと判断した機能の詳細。
 - **移行しないと判断したアクセスルール**：移行ツールを使用して移行しないと判断したアクセス制御ルールの詳細。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。

- **移行しないと判断したNATルール**：移行ツールを使用して移行しないと判断したネットワークアドレス変換（NAT）ルールの詳細。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
- **ルールアクションが変更されたアクセスルール**：移行ツールを使用して変更された「ルールアクション」を持つすべてのアクセス制御ポリシーの詳細。ルールアクションの値は、Allow、Trust、Monitor、Block、Block with reset です。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
- **「ログ」設定が変更されたルールを持つアクセス制御ルール**：Cisco Secure Firewall 移行ツールを使用して変更された「ログ設定」を持つアクセス制御ルールの詳細。ログ設定の値は、False、Event Viewer、Syslog です。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。
- **移行済み構成のエラー/失敗**：移行済み構成要素のプッシュ中に移行失敗の原因となったエラーの詳細。以下に報告されているエラーは、移行された不正な構成、または既存の構成またはサポートされていない機能による management center の競合に関連している可能性があります。ターゲット management center への構成のプッシュを続行または再開する前に、これらのエラーを確認して検証します。

(注)

サポートされていないルールが移行されなかった場合、不要なトラフィックがファイアウォールを通過する問題が発生します。このトラフィックが Firewall Threat Defense によってブロックされるように、Firewall Management Center でルールを構成することを推奨します。

ステップ 3 移行前レポートを開き、Firewall Threat Defense デバイスに手動で移行する必要がある Azure 構成項目をメモします。

ステップ 4 確認が完了したら、Firewall Management Center から Firewall Threat Defense デバイスに移行された構成を展開します。

サポートされていないルールと一部がサポートされているルールについて、データが**移行後レポート**に正しく反映されていることを確認します。

Cisco Secure Firewall 移行ツールは、ポリシーを Firewall Threat Defense デバイスに割り当てます。変更が実行中の構成に反映されていることを確認します。移行されるポリシーを識別しやすくするために、これらのポリシーの説明には構成のホスト名が含まれています。

解析のサマリー

解析のサマリーには、オブジェクト、インターフェイス、NAT、ポリシー、およびアプリケーションの数が表示されます。サマリーには、[Pre-parse Summary]、[Parse Summary]、および [Pre-push Summary] の 3 つのコンポーネントがあります。

- **Pre-parse Summary**：構成のアップロード後に、解析前サマリーが表示されます。この段階で、Cisco Secure Firewall 移行ツールはさまざまなコンポーネントの数を表示します。カスタムアプリケーション、またはグループで使用されているアプリケーションのみが表示さ

れます。構成がマルチ VSYS の場合、完全な VSYS のインターフェイス数が表示されず、ポリシーで直接呼び出されるアプリケーションはカウントされないため、解析前サマリーには一部のアプリケーションが表示されません。したがって、アプリケーション数は解析のサマリーと異なります。同様の動作が NAT にも適用されます。解析前サマリーの一部のコンポーネントにはゼロカウントが表示される場合がありますが、これはこれらの構成の構成要素が 0 であることを意味しません。

- **Parse Summary** : 変換の開始をクリックすると、解析のサマリーが表示されます。この段階で、Cisco Secure Firewall 移行ツールは構成に対してアクションを実行し、サポートされていないすべての構成がサマリーカウントから削除されます。サポートされていないポリシーは無効として Firewall Management Center に移行されるため、サポートされていないポリシーはカウントの一部になります。構成の各コンポーネントが解析されます。解析のサマリーで表示されるカウントは、移行される正確な構成カウントです。
- **Pre-push Summary** : 構成を Firewall Management Center にプッシュするよう求めるプロンプトが表示される前に、プッシュ前サマリーが表示されます。解析前サマリーのカウントは、Cisco Secure Firewall 移行ツールによって実行されるアクションによって、解析のサマリーと異なる場合があります。NAT で直接参照される IP は、オブジェクトとしてプッシュされます。アプリケーションがポートにマッピングされると、サービスカウントが増加し、アプリケーションがダウンします。アプリケーションマッピングを空白のままにすると、アプリケーション数は減少します。静的ルートに重複するエントリがある場合、そのエントリは削除され、カウントは減少します。

移行の失敗

移行中の解析エラーは次のとおりです。

- **解析の失敗** : 構成が Cisco Secure Firewall 移行ツールにアップロードされた後に解析が失敗します。インターフェイスの不良構成が原因です。複数の IP が構成されているか、/32 または /128 の IP がインターフェイスに割り当てられている場合、解析に失敗します。

インターフェイスに複数の IP が割り当てられている場合、またはトンネリング、ループバック、VLAN インターフェイスがルーティングの一部である場合は、プッシュの失敗が発生します。

回避策 : 移行前レポートをダウンロードし、移行レポートの [Configuration lines with errors] セクションを参照します。このセクションには、問題の原因となっている構成の詳細が表示されます。問題を修正し、Cisco Secure Firewall 移行ツールに構成を再アップロードする必要があります。

ルート内のトンネル、ループバック、または VLAN インターフェイスによってプッシュの失敗が発生した場合は、そのようなルートを削除して移行を再試行する必要があります。このようなインターフェイスは Firewall Management Center でサポートされていないためです。

- **プッシュの失敗** : Cisco Secure Firewall 移行ツールが構成を移行し、Firewall Management Center にプッシュされているときに、プッシュの失敗が発生します。プッシュの失敗は、移行後レポートでキャプチャされます。

回避策：移行後レポートをダウンロードし、移行レポートの [Error Reporting] セクションを参照します。このセクションには、問題の原因となっている構成の詳細が表示されます。[確認と検証 (Review and Validation)] ページで問題を修正する必要があります。これには、失敗が表示されているセクションで [移行しない (do not migrate)] オプションを選択するか、または送信元構成で問題を修正し、Cisco Secure Firewall 移行ツールに構成を再アップロードします。

Cisco Secure Firewall 移行ツールのアンインストール

すべてのコンポーネントは、Cisco Secure Firewall 移行ツールと同じフォルダに保存されます。

始める前に

この手順は、デスクトップバージョンの Cisco Secure Firewall 移行ツールを使用している場合にのみ適用されます。

手順

ステップ 1 Cisco Secure Firewall 移行ツールを配置したフォルダに移動します。

ステップ 2 ログを保存する場合は、log フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 3 移行前レポートと移行後レポートを保存する場合は、resources フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 4 Cisco Secure Firewall 移行ツールを配置したフォルダを削除します。

ヒント

ログファイルはコンソールウィンドウに関連付けられています。Cisco Secure Firewall 移行ツールのコンソールウィンドウが開いている場合、ログファイルとフォルダは削除できません。

移行例：Azure から Threat Defense 2100



(注) 移行の完了後にターゲットデバイスで実行できるテスト計画を作成します。

- [メンテナンス期間前のタスク](#)
- [メンテナンス期間のタスク \(48 ページ\)](#)

メンテナンス期間前のタスク

始める前に

Firewall Management Center をインストールして展開していることを確認します。詳細については、適切な『[Management Center Hardware Installation Guide](#)』 [英語] および適切な『[Management Center Getting Started Guide](#)』 [英語] を参照してください。

手順

-
- ステップ 1** ネットワークに Firepower 2100 シリーズ デバイスを展開し、インターフェイスを接続してアプライアンスの電源をオンにします。
- 詳細については、『[Cisco Threat Defense for the 2100 Series Using Management Center Quick Start Guide](#)』 [英語] を参照してください。
- ステップ 2** Firewall Management Center によって管理される Firepower 2100 シリーズ デバイスを登録します。
- 詳細については、「[Add Devices to the Management Center](#)」を参照してください。
- ステップ 3** Cisco Secure Firewall 移行ツールの最新バージョンを <https://software.cisco.com/download/home/286306503/type> からダウンロードして実行します。
- 詳細については、[Cisco.com](#) からの [Cisco Secure Firewall 移行ツールのダウンロード \(27 ページ\)](#) を参照してください。
- ステップ 4** Cisco Secure Firewall 移行ツールを起動し、接続先パラメータを指定する場合は、Firewall Management Center に登録した Firepower 2100 シリーズ デバイスを選択します。
- 詳細については、[Cisco Secure Firewall 移行ツールの接続先パラメータの指定 \(33 ページ\)](#) を参照してください。
- ステップ 5** このガイドの手順に従って、移行する構成を順に確認および検証し、構成を Firewall Management Center にプッシュします。
- ステップ 6** 移行後レポートを確認し、手動で他の構成をセットアップして Firewall Threat Defense に展開し、移行を完了します。
- 詳細については、「[移行後レポートの確認と移行の完了 \(42 ページ\)](#)」を参照してください。
- ステップ 7** 移行の計画時に作成したテスト計画を使用して、Firepower 2100 シリーズ デバイスをテストします。
-

メンテナンス期間のタスク

始める前に

メンテナンスウィンドウの前に実行する必要があるすべてのタスクが完了していることを確認します。「[メンテナンス期間前のタスク \(47 ページ\)](#)」を参照してください。

手順

-
- ステップ 1** 周辺スイッチングインフラストラクチャの Address Resolution Protocol (ARP) キャッシュをクリアします。
- ステップ 2** 周辺スイッチングインフラストラクチャから Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対して基本的な ping テストを実行し、アクセス可能であることを確認します。
- ステップ 3** Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対するレイヤ 3 ルーティングが必要なデバイスから基本的な ping テストを実行します。
- ステップ 4** Firepower 2100 シリーズ デバイスに新しい IP アドレスを割り当て、に割り当てられた IP アドレスを再利用しない場合は、次の手順を実行します。
1. IP アドレスを参照する静的ルートを更新し、Firepower 2100 シリーズ デバイスの IP アドレスを指すようにします。
 2. ルーティングプロトコルを使用している場合は、ネイバーが Firepower 2100 シリーズ デバイスの IP アドレスを予期される接続先のネクストホップとして認識していることを確認します。
- ステップ 5** 包括的なテスト計画を実行し、Firepower 2100 デバイスの管理 Firewall Management Center 内でログをモニタリングします。
-



第 3 章

Cisco Success Network : テレメトリデータ

- [Cisco Success Network - テレメトリデータ \(49 ページ\)](#)

Cisco Success Network - テレメトリデータ

Cisco Success Network は、Cisco Secure Firewall 移行ツールの常時接続使用状況の情報とメトリックの収集機能であり、移行ツールと Cisco Cloud 間のセキュアなクラウド接続を介して使用統計を収集および送信します。これらの統計は、未使用の機能に関する追加のサポートを提供し、製品を改善するのに役立ちます。Cisco Secure Firewall 移行ツールで移行プロセスを開始すると、対応するテレメトリデータファイルが生成され、固定の場所に保存されます。

移行済み 構成を Firewall Management Center にプッシュすると、プッシュサービスはその場所からテレメトリデータファイルを読み取り、データがクラウドに正常にアップロードされた後に削除します。

移行ツールには、テレメトリデータのストリーミング用に、[限定 (Limited)] と [広範 (Extensive)] の 2 つのオプションが用意されています。

Cisco Success Network を [限定 (Limited)] に設定すると、次のテレメトリデータポイントが収集されます。

表 2: 限定的なテレメトリ

データ ポイント	説明	値の例
時刻	テレメトリデータが収集された日時	2023-04-25 10:39:19
ソース タイプ	送信元デバイスタイプ	Microsoft Azure
Target Management Version	管理センターのターゲットバージョン	7.2 以降
Target Management Type	ターゲット管理デバイスのタイプ、つまり管理センター	Management Center

データ ポイント	説明	値の例
Target Device Version	ターゲットデバイスのバージョン	75
Target Device Model	ターゲットデバイスのモデル	VMware 向け Cisco Secure Firewall Threat Defense
Migration Tool Version	移行ツールのバージョン	1.1.0.1912
Migration Status	Management Center への Azure 構成の移行状態	SUCCESS

次の表に、**Cisco Success Network** が [広範 (Extension)] に設定されている場合のテレメトリデータポイント、その説明、およびサンプル値に関する情報を示します。

表 3: 広範なテレメトリ

データ ポイント	説明	値の例
オペレーティングシステム	Cisco Secure Firewall 移行ツールを実行するオペレーティングシステム。Windows7、Windows10 64-bit、macOS High Sierra を使用できます	Windows 7
ブラウザ	Cisco Secure Firewall 移行ツールの起動に使用されるブラウザ。Mozilla/5.0、Chrome/68.0.3440.106、Safari/537.36 を使用できます	Mozilla/5.0

表 4: ターゲット管理デバイス (Firewall Management Center) 情報

データ ポイント	説明	値の例
Target Management Type	ターゲット管理デバイスのタイプ (Firewall Management Center)	Management Center
Target Device Version	ターゲットデバイスのバージョン	75
Target Device Model	ターゲットデバイスのモデル	VMware 向け Cisco Secure Firewall Threat Defense

表 5: 移行の概要

表 6: Cisco Secure Firewall 移行ツールのパフォーマンスデータ

データ ポイント	説明	値の例
Conversion Time	構成行の解析にかかった時間 (分)	14
Migration Time	エンドツーエンドの移行にかかった合計時間 (分)	592
Config Push Time	最終構成のプッシュにかかった時間 (分)	7

データ ポイント	説明	値の例
Migration Status	構成の Firewall Management Center への移行のステータス	SUCCESS
Error Message	Cisco Secure Firewall 移行ツールによって表示されるエラーメッセージ	null
Error Description	エラーが発生した段階および考えられる根本原因に関する説明	null



第 4 章

移行の問題のトラブルシューティング

- [Cisco Secure Firewall 移行ツールのトラブルシューティング](#) (53 ページ)
- [トラブルシューティングに使用されるログおよびその他のファイル](#) (54 ページ)

Cisco Secure Firewall 移行ツールのトラブルシューティング

移行が失敗するのは、通常、構成ファイルをアップロードしているとき、または移行された構成を Firewall Management Center にプッシュしているときです。

Cisco Secure Firewall 移行ツールのサポートバンドル

Cisco Secure Firewall 移行ツールには、サポートバンドルをダウンロードして、ログファイル、DB、構成ファイルなどの役立つトラブルシューティング情報を抽出するオプションがあります。次の手順を実行します。

1. [移行完了 (Complete Migration)] 画面で、[サポート (Support)] ボタンをクリックします。
ヘルプサポートページが表示されます。
2. [サポートバンドル (Support Bundle)] チェックボックスをオンにして、ダウンロードする構成ファイルを選択します。



(注) ログファイルと DB ファイルは、デフォルトでダウンロード用に選択されています。

3. [ダウンロード (Download)] をクリックします。
サポートバンドルファイルは、ローカルパスに .zip としてダウンロードされます。Zip フォルダを抽出して、ログファイル、DB、および構成ファイルを表示します。
4. [Email us] をクリックして、テクニカルチームに障害の詳細を電子メールで送信します。
ダウンロードしたサポートファイルを電子メールに添付することもできます。

5. [TAC ページに移動 (Visit TAC page)] をクリックして、シスコのサポートページで TAC ケースを作成します。



(注) TAC ケースは、移行中にいつでもサポートページからオープンできます。

トラブルシューティングに使用されるログおよびその他のファイル

問題の特定とトラブルシューティングに役立つ情報は、次のファイルにあります。

ファイル	ロケーション
ログ ファイル	<migration_tool_folder>\logs
移行前のレポート	<migration_tool_folder>\resources
移行後のレポート	<migration_tool_folder>\resources
未解析ファイル	<migration_tool_folder>\resources

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。