Cisco Intersight 管理対象モード移行ツール ユーザー ガイド、4.x

初版：2023 年 9 月 4 日

最終更新：2024 年 5 月 22 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 NONINFRINGEMENT 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)

© 2024 Cisco Systems, Inc. All rights reserved.

通信、サービス、偏向のない言語、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービスリクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

Cisco バグ検索ツール

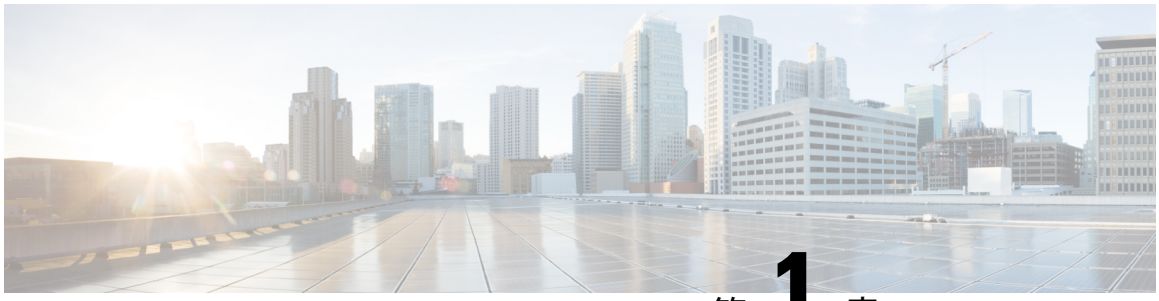
Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

偏向のない言語

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザーインターフェ

通信、サービス、偏向のない言語、およびその他の情報

イスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。



第 1 章

新機能および変更された機能に関する情報

- 新機能と更新情報 （1 ページ）

新機能と更新情報

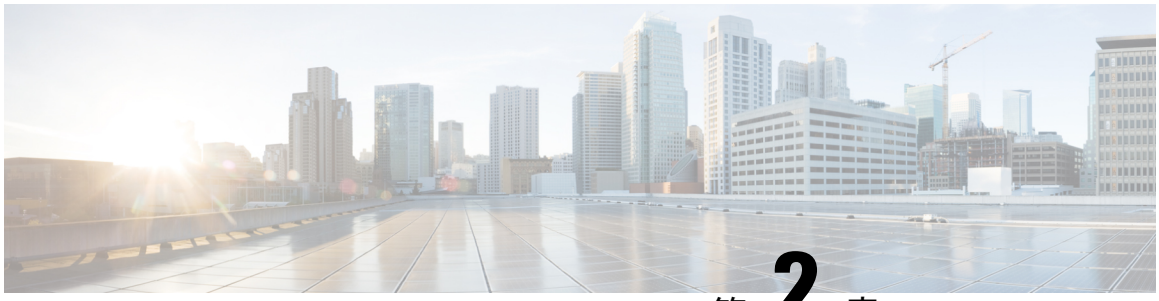
このセクションでは、Cisco Intersight 管理モード移行ツール、リリース 4.0.1 の新機能と変更された動作に関する情報を示します。

表 *1 : Intersight* マネージド モード移行ツール、リリース *4.0.1* の新機能と変更された動作

特長	説明	参照先
オペレーティング システムの変更	ツールの基盤となるオペレーティング システムは、Ubuntu 18.04 から Ubuntu 22.04 に変更されました。したがって、IMM 移行ツール、リリース 3.1.1 を使用した既存のユーザーの場合、ツールの既存のバージョンからデータをバックアップし、新規 ova ファイルをインストールして、ツールの最新バージョンでデータを保存する必要があります。	Cisco Intersight 管理モード ツールのアップグレード

特長	説明	参照先
ソフトウェア レポジトリのサポート	IMM 移行ツール リリース 4.0.1 には、ISO イメージまたはファームウェア パッケージをホストできるソフトウェア レポジトリ機能が含まれています。これを活用し、UCS サーバーでオペレーティング システムのインストールまたはファームウェア アップグレードを簡単に実行できます。	ソフトウェアリポジトリ
新規 Intersight 欧州地域向けサポート	IMM 移行ツール、リリース 4.0.1 は、Intersight SaaS デバイスの米国および EU 地域をサポートします。	変換のための IMM 移行の追加 クローニングのための IMM 移行の追加 Device Management
選択されたクローニングを実行する機能	IMM 移行ツール、リリース 4.0.1 は、クローンする必要がある移行のサーバー プロファイル/テンプレートを選択する機能を提供します。	クローニングのための IMM 移行の追加
変換中にサービス プロファイルの関連付けを保持する機能	UCS Manager/Central で割り当てられたものと同じサーバー シリアル番号に事前に、それぞれの変換されたサーバー プロファイルを割り当てることを選択できます。	デフォルト設定
クローニング中にサーバー プロファイルの関連付けを保持する機能	ソース Intersight デバイスで割り当てられたものと同じサーバー シリアル番号に、それぞれのクローニングされたサーバー プロファイルを事前に割り当てることを選択できます。	デフォルト設定
変換中にシャーシ/ラック サーバー ID を保持する機能	UCS Manager で定義されたものと同じサーバ ポートにシャーシ/ラック サーバー ID を保持するように選択できます。	デフォルト設定

特長	説明	参照先
vCon から PCIe スロットへのマッピングをカスタマイズする機能	デフォルト マッピングをオーバーライドし、変換で各ソース vCon 値それぞれの対応する PCIe スロット番号を手動で提供できます。	デフォルト設定
ドライブ セキュリティおよびファームウェア ポリシーなど追加ポリシーのサポート	IMM 移行ツール、リリース 4.0.1 は、変換およびクローニングの追加ポリシーをサポートします。	サポートされる機能



第 2 章

概要

• 概要 （5 ページ）

概要

Cisco Intersight マネージド モード（IMM）移行ツールは、既存の Cisco UCS Manager（UCSM）および Cisco UCS Central インフラストラクチャの構成属性を複製し、既存のサービスプロファイル テンプレートを IMM サーバー プロファイル テンプレートに変換して IMM での新しいサーバーの展開を加速することにより、新しい IMM 展開をブートストラップするのに役立ちます。

IMM 移行ツール リリース 3.0.1 以降では、物理サーバーがサーバー プロファイルから取得する構成識別子を保持するためのサポートを提供します。これらには、IP アドレス、MAC アドレス、IQN、UUID、WWNN、および WWPN が含まれます。このサポートにより、UCS Manager/Central から IMM へのサービスプロファイルの移行が可能になります。

IMM 移行ツール、リリース 4.0.1 以降で、ソフトウェア レポジトリ機能を使用して、オペレーティング システムをインストールし、サーバーのファームウェアをアップグレードします。

IMM 移行ツールは、次の機能を提供します。

1. Cisco UCS Manager ドメインのハードウェアの互換性を検証する機能。
2. 実行中の UCS Manager ドメインまたは UCS Central インスタンスから構成全体を取得します。
3. 構成のどの部分が Intersight で使用できるかを検証する機能。
4. UCS Manager または UCS Central 構成属性の IMM への変換を実行します。
    - UCS Manager ドメインの実行構成の変換は、主に 2 つの部分で行われます（構成変換の各セクションを選択的に有効 / 無効にすることができます）。

- VLAN / VLAN グループ / VSAN、ポート ロール、QoS、および管理設定（NTP / DNS / SNMP / SYSLOG）を含む UCS Manager ドメインのファブリック構成を変換します。
- UCS Manager ドメインからのサービスプロファイルおよびサービスプロファイル テンプレートと関連するすべてのポリシーを可能な限り変換します。

- UCS Central インスタンスの実行構成の変換は、主に 次のように行われます（構成変換の各セクションを選択的に有効 / 無効にすることができます）。
  - UCS Central インスタンスからのサービスプロファイルおよびサービスプロファイル テンプレートと関連するすべてのポリシーを可能な限り変換します。

（注） UCS Central のファブリック構成の変換は、対応する UCS Manager ドメインのファブリック変換を実行することで実現できます。

  - IMM 移行ツール、リリース 3.1.1 以降は、さまざまなプール、ポリシー、およびプロファイル/テンプレートに割り当てられる UCS Central タグの変換をサポートします。

5. ドメインが UCS Manager または UCS Central から IMM に変換されるときに、ハードウェアと構成の互換性の概要を取得するために使用できる IMM 準備レポートの生成。

（注） Cisco UCS Central は複数の UCS Manager ドメインに登録できるため、ハードウェアの互換性は UCS Manager ドメインに対してのみ使用でき、UCS Central インスタンス自体には使用できません。

IMM 準備レポートには、次の情報が表示されます。

- IMM に移行するための UCS Manager または UCS Central デバイスの準備の概要を示す変換スコアと全体的な概要。
- 変換されたオブジェクトやツールが変換できなかったオブジェクトなど、構成ごとの詳細情報。

6. 2 つの Intersight アカウント間での構成属性のクローン作成。

IMM 移行ツール 3.0.1 では、Intersight アカウントを別の Intersight アカウントにクローン作成できます。この機能は、SaaS および仮想アプライアンス アカウントで

サポートされています。すべてのスタンドアロンおよびIMMサーバーに関連するプール/ポリシー/プロファイル/テンプレートを複製できます。

IMM 移行ツール 3.1.1 以降から、すべての UCS サーバ プロファイルで割り当てられた ID を保存しながら Intersight アカウントをクローニングできます。

IMM移行ツール4.0.1以降から、Intersightアカウント間でクローニングしサーバープロファイルを選択して、選択されたクローニングを実行できます。

7. 送信元 UCS 組織を接続先 Intersight 組織にマッピングします。

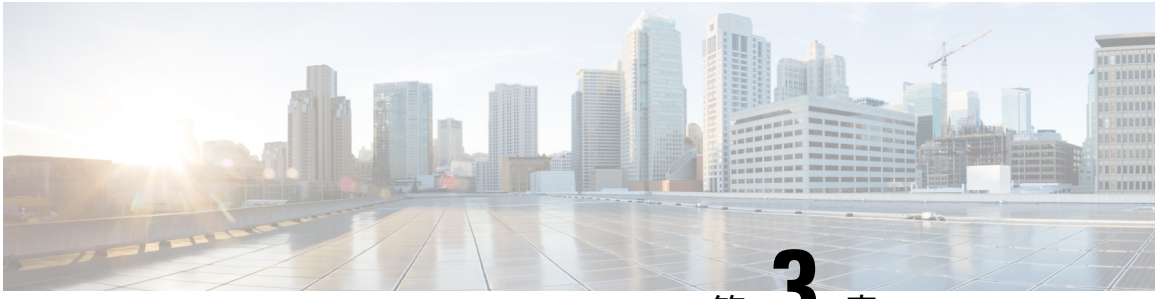
IMM 移行ツール リリース 3.0.1 以降は、組織のマッピングを行う機能を提供します。この新機能により、UCS Manager/Central から Intersight への組織の変換をより柔軟に制御できます。1 対 1 または多対 1 のマッピングを通じて、接続先 Intersight 組織を選択するか、送信元UCS組織に必要な新しい接続先Intersight組織を追加できます。

8. ソフトウェア レポジトリとしてツールの使用

IMM 移行ツール、リリース 4.0.1 以降から、ISO 画像またはファームウェア パッケージをホストできるソフトウェア リポジトリ機能が含まれています。これを活用し、UCS サーバーでオペレーティング システムのインストールまたはファームウェア アップグレードを簡単に実行できます。

（注） UCSM ドメインに HyperFlex クラスタが展開されている場合は、IMM に移行しないでください。HyperFlex サーバーは現在、IMM でサポートされていません。

概要



第 3 章

前提条件

• 前提条件 （9 ページ）

前提条件

このセクションでは、Cisco Intersight マネージド モード移行ツールをインストールするための最小要件について説明します。

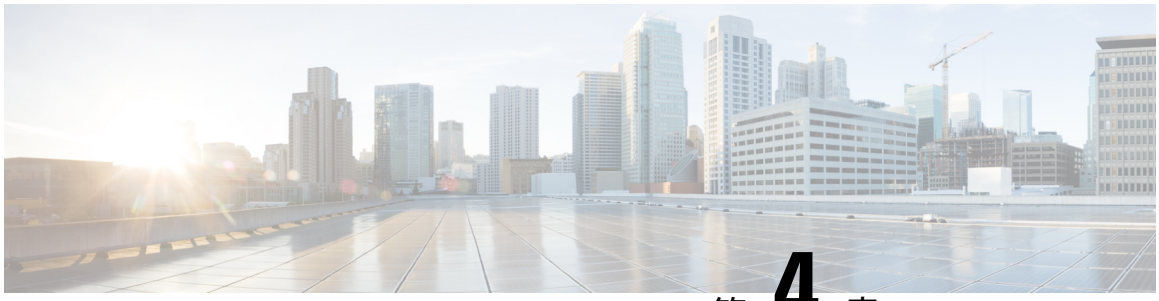
- Cisco UCS Manager: 3.2(1d) 以降のサポートされているバージョン。
- Cisco UCS Central: 2.0(1a) 以降のサポートされているバージョン。
- サポートされている ESX バージョン：ESXi 6.0 以降。
- 最小 VM 要件：
  - vCPU X 2
  - 8 GB RAM
  - 100 GB ストレージ
  - ソフトウェア レポジトリ機能用の追加の 10GB ～ 5000GB（デフォルト 100GB）
- OVA で使用される仮想ハードウェア バージョン：11
- ネットワーク接続の要件：
  - TCP ポート 443（HTTPS）（IMM 移行ツール、リリース 1.0.2 以降）
  - トラブルシューティングまたは高度な構成のための TCP ポート 22（SSH）。
  - 以下へのアクセスが必要です。
    - DNS（TCP/UDP ポート 53 を使用）
    - NTP（UDP ポート 123 を使用）
    - UCS Manager/UCS Central デバイス（TCP ポート 443 [HTTPS] のみ）
    - Intersight デバイス（TCP ポート 443 [HTTPS] のみを使用）

- プロキシサーバー設定への接続（ある場合）

- 構成を Intersight にプッシュするには、Intersight インスタンスへの HTTPS 接続が必要です。
  - SaaS の場合、URL は https://www.intersight.com です
  - アプライアンスの場合、URL はユーザーによって提供されます。

- ソフトウェア リポジトリへのアクセスには、HTTPS（TCP ポート 443）接続がオープンである必要があります。

  Cisco UCS サーバーおよび Intersight OS インストールで使用するには、UCS サーバーの CIMC IP と IMM 移行ツール VM 間の接続がオープンであることを確認します。



第 4 章

Cisco Intersight マネージド モード移行ツールのインストール

• Cisco Intersight マネージド モード移行ツールのインストール （11 ページ）

Cisco Intersight マネージド モード移行ツールのインストール

始める前に

[UCS ツール（UCS Tools）] ページから、OVF テンプレートの展開を開始するときに見つけやすい場所にあるコンピュータに IMM 移行 tool.ova ファイルをダウンロードします。

Cisco Intersight マネージド モード移行ツールのインストール

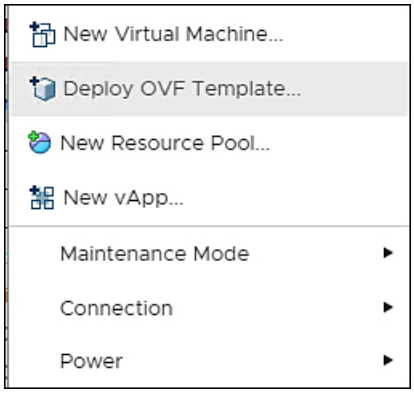
（注）

Cisco Intersight マネージド モード移行ツールのインストール

Open Virtual Appliance（OVA）は、1 つ以上の仮想マシン（VM）から構成されるビルド済みのソフトウェア ソリューションであり、1 つのユニットとしてパッケージ、保守、更新、および管理されます。Cisco Intersight 管理モード移行ツール OVA には、オペレーティング システムがプレインストールされており、IMM 移行ツールの機能に必要なアプリケーション機能が含まれています。OVA としての IMM 移行ツールは、VMware vSphere インフラストラクチャに展開できます。

IMM 移行ツール 3.1.1 以降では、ツール データのバックアップを取り、IMM 移行ツールの同じインスタンスまたは別のインスタンスで復元できます。詳細については、「バックアップ/復元」を参照してください。

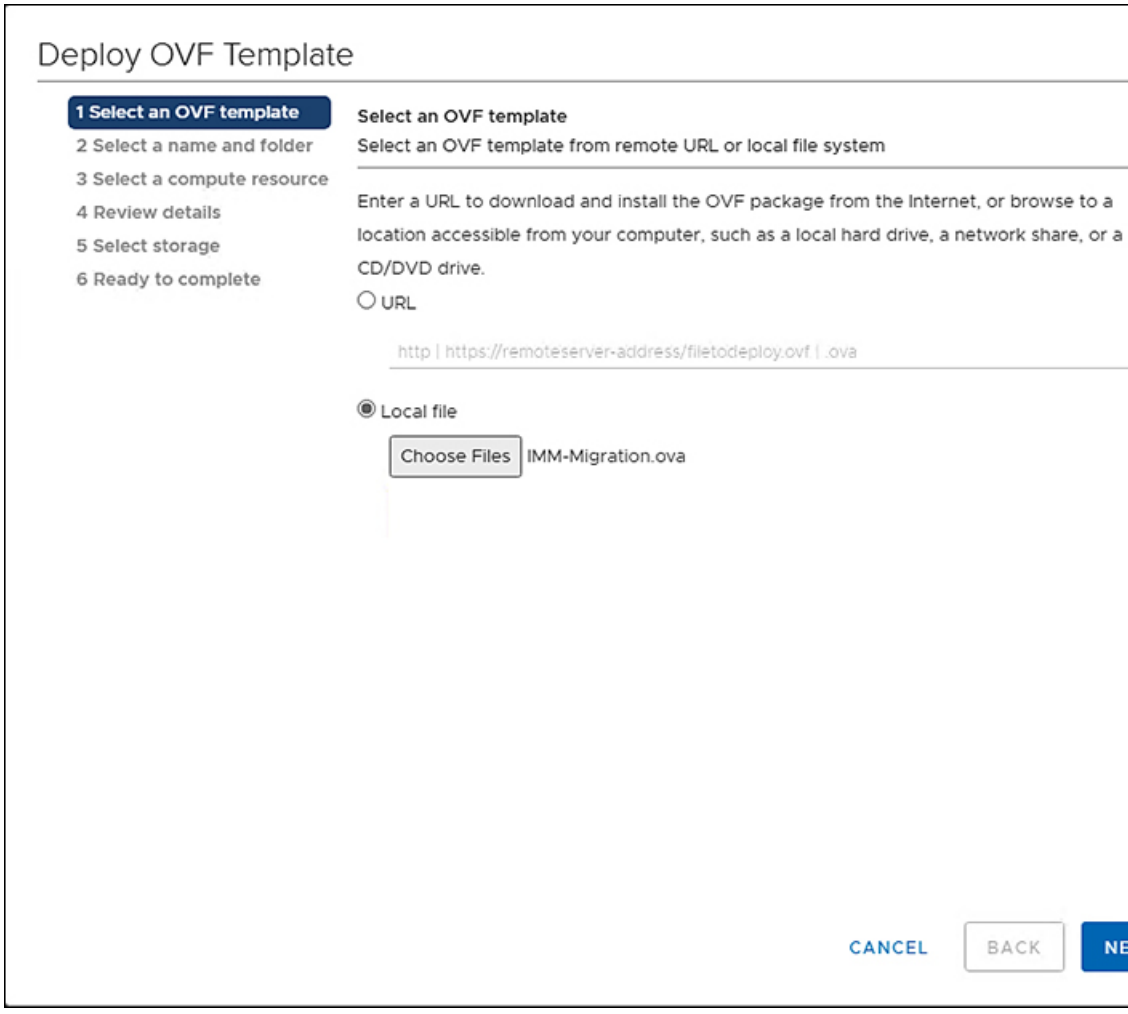
1. HTML5 vSphere Web Client にログインし、**[VM]** タブに移動します。
2. [アクション（Actions）] ドロップダウンリストから [OVF テンプレートの展開（Deploy OVF Template）] アクションボタンを追加します。



3. 追加された [OVF テンプレートの展開（Deploy OVF Template）] ボタンをクリックします。

   テンプレートの選択を求める新しいウィンドウが表示されます。

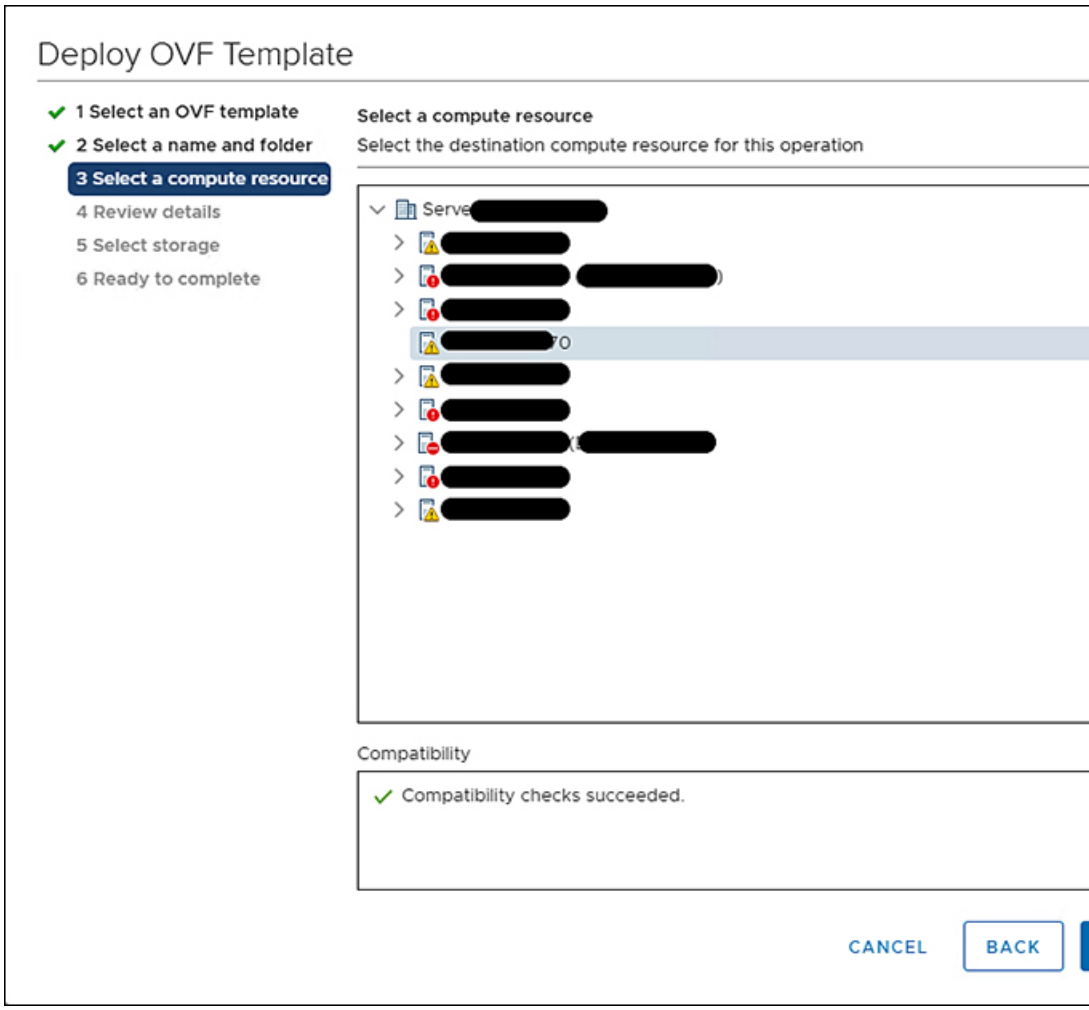
Cisco Intersight マネージド モード移行ツールのインストール



4. **[ファイルの選択（Choose Files）]** をクリックし、ダウンロードした OVA ファイルを選択します。
5. [次へ（Next）] をクリックします。
6. 仮想アプライアンスを展開する場所を選択し、**[次へ（Next）]** をクリックします。

Cisco Intersight マネージド モード移行ツールのインストール

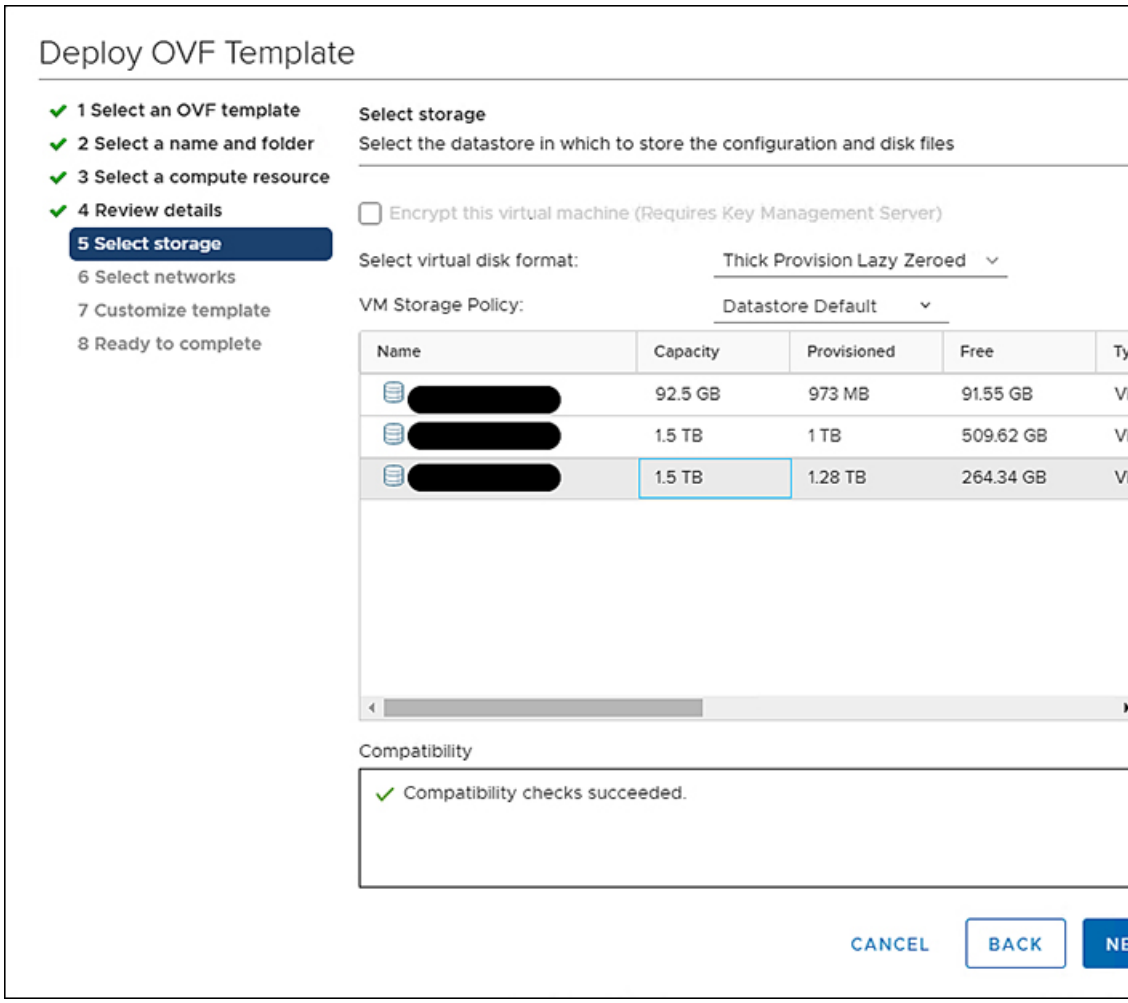
7. 仮想アプライアンスの実行に使用するリソースを選択し、**[次へ（Next）]** をクリックします。



高度な構成オプションを含むパッケージの詳細を確認します。

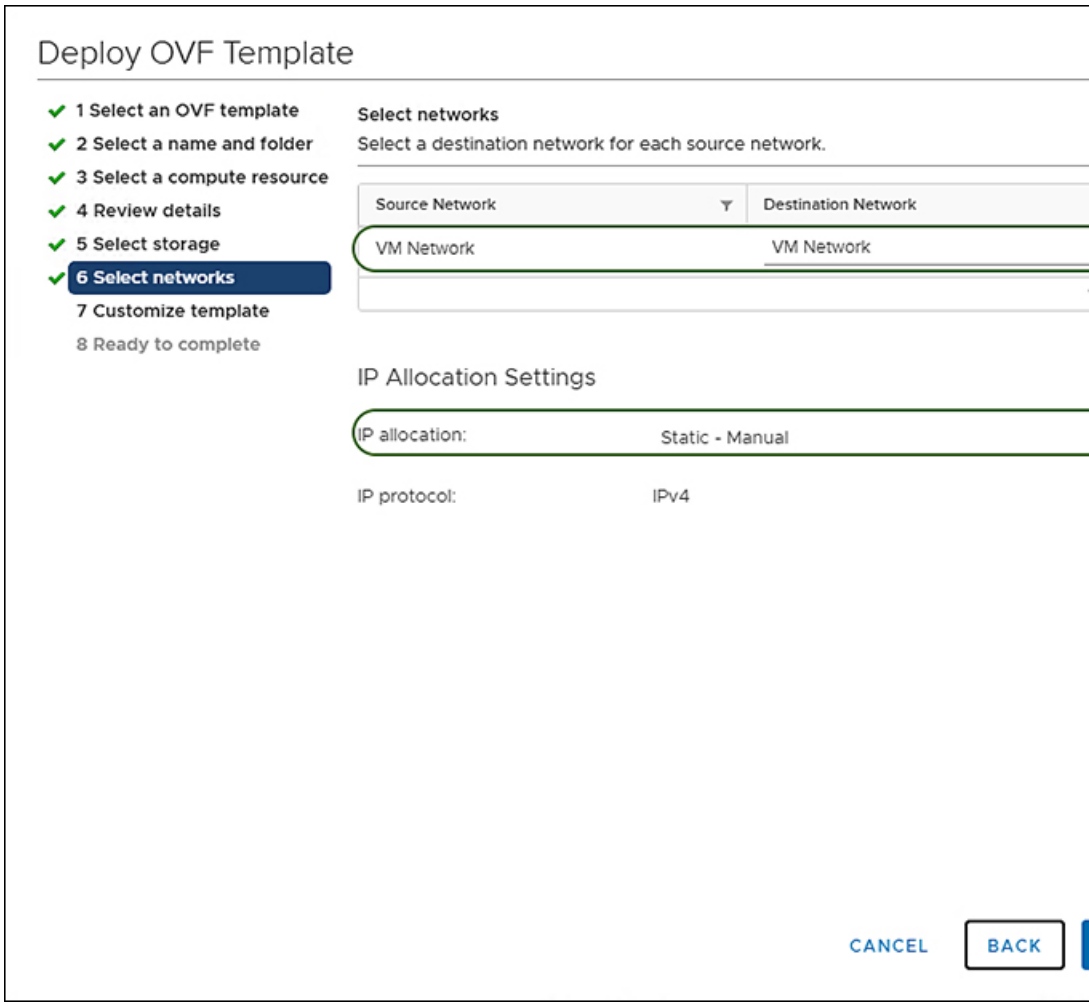
Cisco Intersight マネージド モード移行ツールのインストール

8. [次へ（Next）] をクリックして、これらのオプションを受け入れます。
9. データストアのリストから目的の保存場所を選択し、**[次へ（Next）]** をクリックします。



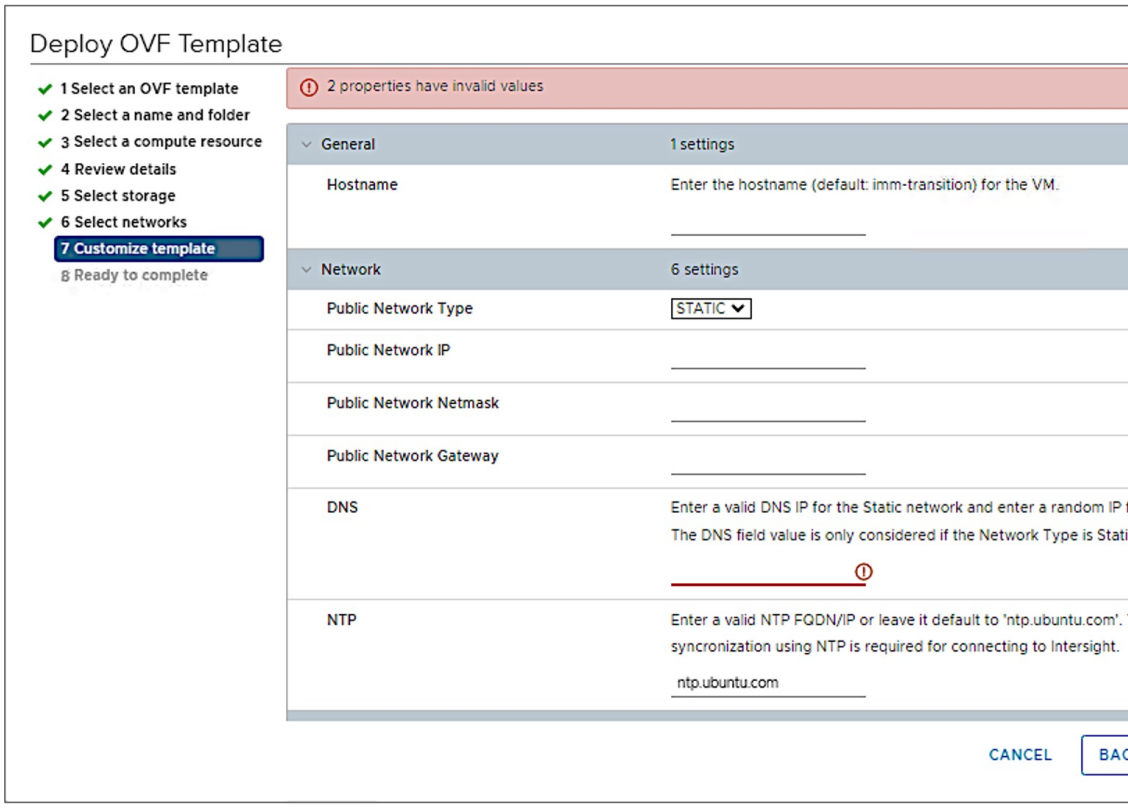
Cisco Intersight マネージド モード移行ツールのインストール

10. 各送信元ネットワークのドロップダウンリストから宛先ネットワークを選択し、[次へ（Next）] をクリックします。



Cisco Intersight マネージド モード移行ツールのインストール

11. **[ネットワーク（Network）]**設定値を入力し、**[システム パスワード（System Password）]**を設定することにより、展開プロパティをカスタマイズします。



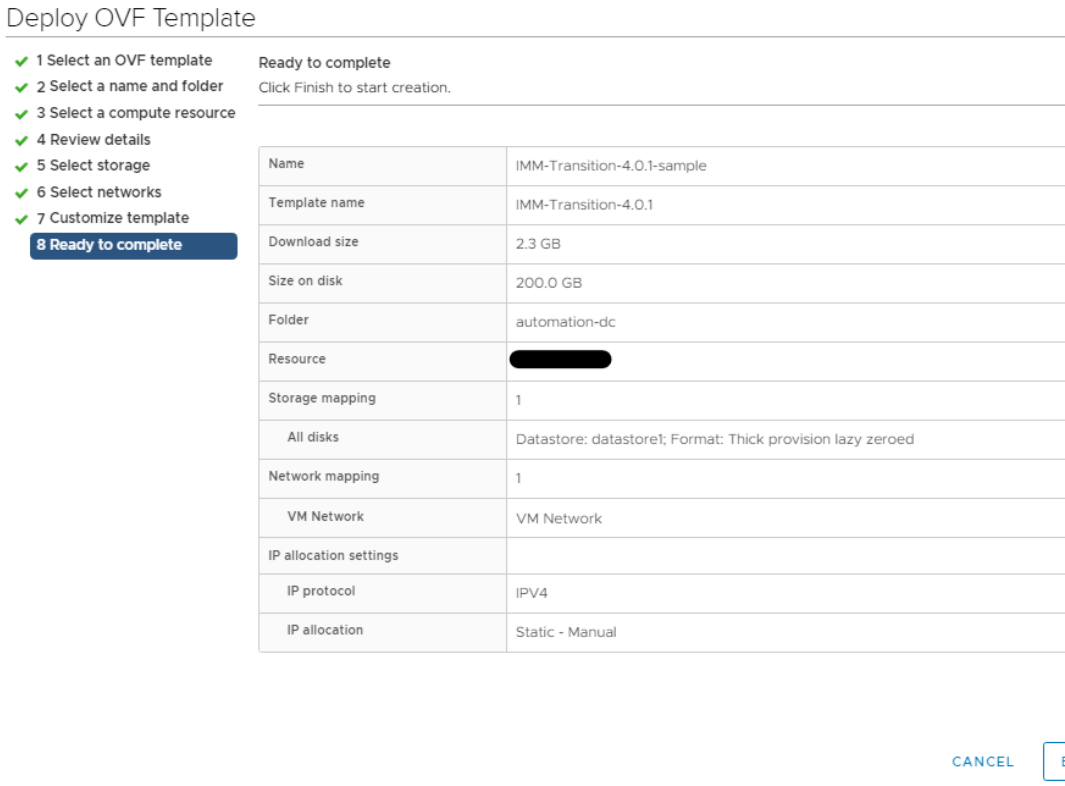
自動生成されたデフォルト パスワードは、変換された仮想メディア、iSCSI ブートなどの UCS Manager ポリシー/USC Central ポリシーの既存のパスワードの代わりに使用されます。同様に、別の自動生成されたパスワードは、iSCSI ブート ポリシーの相互 CHAP 認証に使用されます。変換されたポリシーが Intersight にプッシュされた後、それらのパスワードを変更する必要があります。

（注）
- 変換されたポリシーが Intersight にプッシュされた後、それらの
要があります。
- NTP フィールドの入力が必須です。デフォルト値は、*ntp.ubuntu.*
- ソフトウェア リポジトリ ディスク サイズは、最小値が *10* で最

12. [次へ（Next）] をクリックします。
13. 構成データを確認します。

Cisco Intersight マネージド モード移行ツールのインストール

14. **[終了]** をクリックします。



システムがファイルをインポートして展開します。

15. [更新（Refresh）] ボタンをクリックしてシステムを更新します。

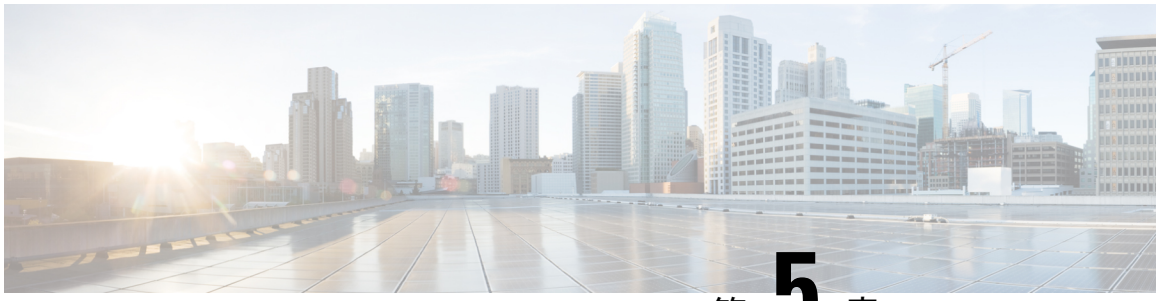
    VM が中央のウィンドウ ペインに表示されます。

16. VM を選択し、[Power On] をクリックします。

17. VM の電源がオンになったら、[コンソールを開く（Open Console）] アイコンをクリックして、新しいウィンドウで VM コンソールを開きます。

    OVA テンプレートが正常に展開され、VM の電源がオンになりました。

Cisco Intersight マネージド モード移行ツールのインストール



第 5 章

Cisco Intersight 管理モード ツールのアップグレード

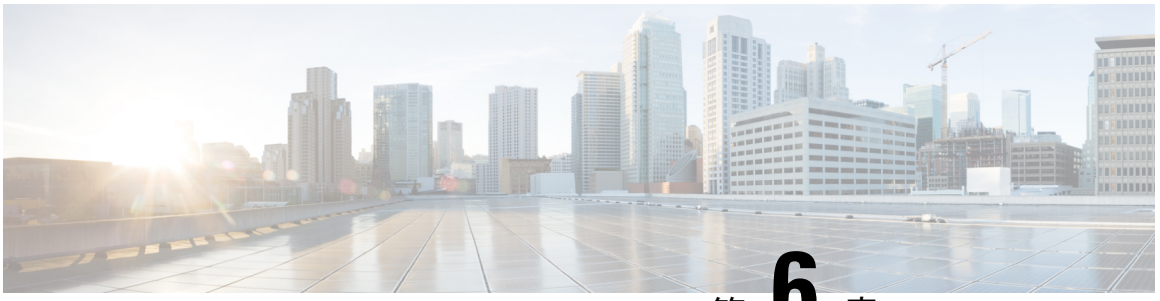
• Cisco Intersight 管理モード ツールのアップグレード （21 ページ）

Cisco Intersight 管理モード ツールのアップグレード

次の手順を実行し、3.x から 4.0.1 以降にツールをアップグレードします。

1. アップグレードを開始する前に、データのバックアップを取る必要があります。詳細については、「バックアップ/復元」を参照してください。
2. コンピュータに IMM 移行ツール .ova ファイルをダウンロードします。
3. .ova ファイルを展開します。詳細については「Installing Cisco Intersight マネージド モード移行ツール」を参照してください。
4. ツールの新規インスタンスでデータを復元します。詳細については、「バックアップ/復元」を参照してください。

Cisco Intersight 管理モード ツールのアップグレード



第 6 章

Intersight マネージド モード移行ツールのへのアクセス

• Intersight マネージド モード移行ツールのへのアクセス （23 ページ）

Intersight マネージド モード移行ツールのへのアクセス

ブラウザ ウィンドウから Cisco IMM 移行ツールのユーザーインターフェイスにアクセスして、移行準備レポートを生成し、UCS ドメインを IMM 設定に変換できます。

1. Web ブラウザ ウィンドウを起動します。
2. `http://<VM IP address>` または `https://<VM IP address>` を入力します。VM IP アドレスは、Cisco IMM 移行ツール OVA を展開した VM の IP アドレスです。

   IMM 移行ツール リリース 1.0.2 以降は、HTTPS サポートを提供します。すべての `http` URL は `https` にリダイレクトされます。
3. [Login（ログイン）] ダイアログボックスに、ユーザー名とパスワードを入力します。

（注） ユーザー名：admin

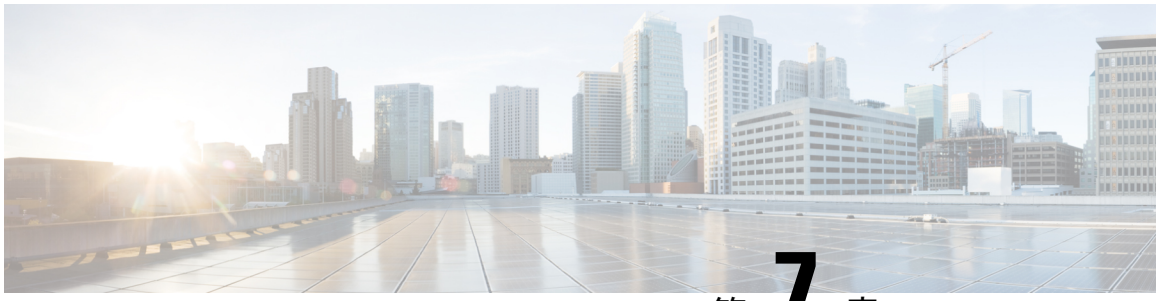
パスワード：インストール時に [テンプレートのカスタマイズ（Customize template）] ページで設定したパスワードを入力します。

4. [サインイン（Sign In）] をクリックします。

   ユーザー セッションを終了するには、右上隅のユーザー設定から [ログアウト（Log Out）] をクリックします。

（注） **セッション タイムアウト** ： IMM 移行ツール リリース 1.0.2 以降では、非アクティブな状態が 30 分間続くと、セッションから自動的にログアウトされます。アプリケーションを再度使用するには、再ログインする必要があります。

Intersight マネージド モード移行ツールのへのアクセス



第 7 章

Transition

- 変換のための IMM 移行の追加 （25 ページ）
- クローニングのための IMM 移行の追加 （30 ページ）
- アップロードした構成をプッシュするための IMM 移行の追加 （33 ページ）
- 移行管理 （35 ページ）
- 移行準備レポートの説明 （35 ページ）

変換のための IMM 移行の追加

現在実行中および後続のすべての移行に適用される移行のデフォルト設定を設定できます。**移行の追加** プロセス中にデフォルト設定を変更することもできます。詳細については、[デフォルト設定（Default Settings）]を参照してください。

[UCSM/Central から Intersight のサーバープロファイルへのサービスプロファイルの変換（Converting Service Profiles from UCSM/Central to Server Profiles in Intersight）]

IMM の移行を開始するには、次の手順を実行します。

1. [IMM 移行の追加（Add IMM Transition）] をクリックします。
2. 移行の名前を入力します。
3. 移行のタイプを選択します。

   (a) UCS Manager ハードウェアおよび構成の互換性/readiness 概要のみを表示する場合、または UCS Central 構成の互換性のみを表示する場合は、**[Readiness レポートの生成（Generate Readiness Report）]**

   （b）準備レポートを表示し、変換された構成を Intersight にプッシュする場合は、**[準備レポートの生成（Generate Readiness Report）] + [構成を Intersight にプッシュ（Push Config to Intersight）]** を選択します。

   （c）構成をクローニングして、ある Intersight アカウントから別のアカウントに移行する場合は、**[Intersight のクローニング（Clone Intersight）]** を選択します。詳細な手順については、「クローニングのための IMM 移行の追加」を参照してください。
4. [次へ（Next）] をクリックします。

5. ソース デバイス（UCS Manager または UCS Central）を選択します。
6. 選択したデバイスの詳細を入力します。

   （a）既存のデバイスの構成を移行する場合は、*[*既存の *UCS Manager* の選択/既存の *UCS Central* の選択（*Select Existing UCS Manager/ Select Existing UCS Central*）*]* オプションを選択します。

   （b）新しいUCS Manager/UCS Central 構成を追加する場合は、*[*新しい *UCS Manager* の追加/新しい *UCS Central* の追加（*Add New UCS Manager/ Add New UCS Central*）*]* オプションを選択します。

   該当のデバイスのドメイン IP/FQDN、ユーザー名とパスワードを入力します。必要に応じて、**[プロキシを使用（Use Proxy）]** トグル ボタンをオンにして、新しく追加されたデバイスのプロキシを有効にします。**プロキシ設定**インターフェイスでプロキシ設定の詳細を追加します。プロキシ設定を有効にする手順については、「プロキシ設定」を参照してください。
7. **[更新（Refresh）]** をクリックして、UCS Manager/Central デバイスから最新の構成とインベントリの詳細を取得します。

   選択したソース デバイスが UCS Central の場合、[UCS Central の選択（Choose UCS Central）] ドロップダウン リストから UCS Central インスタンスを選択できます。

   [ダウンロード（Download）] リンクを使用して、現在のデバイスの構成 JSON ファイルとインベントリ JSON ファイルをダウンロードできます。

   構成 JSON ファイルには、既存の UCS Manager/UCS Central ドメインに存在するソフトウェア構成の詳細情報が含まれています。

   インベントリ JSON ファイルには、UCS Manager ドメインまたは UCS Central インスタンスのすべての UCS ドメインに存在するハードウェア インベントリの詳細情報が含まれています。

   これらのファイルは、トラブルシューティングの目的でテクニカル サポート チームと共有できます。
8. [次へ（Next）] をクリックします。
9. 接続先の Intersight アカウントを選択します。

   （a）既存の Intersight アカウントに構成を移行する場合は、**[既存のアカウントから選択（Choose from existing account）]** オプションを選択します。手順 13 に進みます。

   （b）新しい **[SaaS Intersight]** または新しい **[Intersight アプライアンス VM（Intersight Appliance VM）]** アカウントに構成を移行する場合は、**[新しいアカウントの追加（Add new account）]** オプションを選択します。ステップ 10 に移動します。

（注） リリース 4.0.1 以降から、**[SaaS Intersight]** アカウントを選択する場合、以下に属するアカウントの地域も選択できます。**米国**または **EU**。

（c）宛先の Intersight アカウントの詳細を追加せずに変換準備レポートを生成する場合は、**[Insight デバイスなしで進む（Proceed without Intersight device）]** オプションを選択します。手順 13 に進みます。

10. 次の手順を実行して、Intersight から API キー ID を生成します。

1. Intersight アプリケーションにログインします。

2. 右上隅にある歯車アイコンをクリックし、[設定（Settings）] を選択します。

3. [API] セクションで、[API キー（API Keys）] をクリックします。

4. ページの右上にある [API キーの生成] をクリックします。

5. **[説明（Description）]** フィールドに名前を入力し、**[OpenAPI スキーマ バージョン 2 またはバージョン 3 の API キー（API Key for OpenAPI Schema Version 2 or Version 3）]** を選択します。

（注） OpenAPI スキーマ バージョン 2 は、IMM 移行ツール、リリース 3.0.1 ではサポートされていません。V2 および V3 スキーマの API キーのサポートは、IMM Transition Tool、リリース 3.0.2 以降で利用できます。

6. [生成（Generate）] をクリックします。

API キー ID と秘密鍵が生成されます。**[クリップボードにコピー（Copy to Clipboard）]** の青いアイコンを使用して、これらの値をクリップボードにコピーします。IMM 移行ツール アプリケーションに戻ります。

11. 次のフィールドに入力します。

- API キー ID：前の手順で生成された API キー ID を入力します。
- 秘密鍵：Intersight で生成された秘密鍵を入力します。

また、Intersight アプライアンス VM を選択した場合は、FQDN を入力します。

12. [次へ（Next）] をクリックします。

13. 移行に必要な変換オプションを構成します。

- [移行設定（Transition Settings）] フィールドのそれぞれの詳細については、「デフォルト設定」 の 「**B.変換の移行設定**」を参照してください。
- 作成するすべての新しい移行の既定の構成セットを定義するには、「デフォルト設定」の「**A.変換のデフォルト移行設定**」 を参照してください。

14. [次へ（Next）] をクリックします。

15. 変換する必要があるサービス プロファイル/テンプレートを選択します。

プロファイル名の横に、物理サーバとの関連付けの詳細が表示されます。

上部にある検索バーを使用して、特定のサービス プロファイル/テンプレートを検索できます。

検索バーの横にある **[表示（Show）]** ドロップダウン リストで、テンプレート、組織、プロファイル、テンプレートのみを表示するようにフィルタを適用できます。

16. [次へ（Next）] をクリックします。

17. 選択した送信元組織をマップされた接続先 Intersight 組織に変換する場合は、**[高度な組織マッピング（Advanced Organization Mapping）]** をオンのままにします。宛先 Intersight 組織の名前を手動で入力するには、トグル ボタンをオフにし、ルート組織名を入力して、ステップ 21 に進みます。**[ソース組織パスを Intersight 組織名に保持（Keep source Org path in Intersight Org name）]** オプションを有効にすることで、宛先 Intersight 組織でソース UCS 組織名を保持することもできます。

    - このオプションにより、UCSM から Intersight への変換されたオブジェクトのマッピングを柔軟に制御できます。同じ名前のマッピング動作とは異なり、カスタマイズされたマッピングでは、アカウントに対して複数の Intersight 組織を作成する必要がありません。**[高度な組織マッピング（Advanced Organization Mapping）]** オプションは、単一または複数の UCS 組織を Intersight 組織にマップするのに役立ちます。
    - **[新規追加（Add New）]** オプションを使用して、新しい接続先 Intersight 組織を追加することもできます。

-

（注） **[ソース組織パスを Intersight 組織名に保持（Keep source Org path in Intersight Org name）]** オプションが無効になっている場合、「root/PROD/WINDOWS」および「root/NONPROD/WINDOWS」は、Intersight で同じ「WINDOWS」組織に変換されます。ポリシー/プール/プロファイル/テンプレート オブジェクトの名前が両方のソース UCS 組織で同じである場合、これにより競合が発生する可能性があります。

18. 送信元 UCS 組織、接続先 Intersight 組織を選択し、**[今すぐマップ（Map Now）]** をクリックします。

    送信元組織と接続先組織がマッピングされます。マップされると、接続先の Intersight 組織名の横に「マップ済み」タグが表示されます。また、**[高度な組織マッピング（Advanced Organization Mapping）]** ページの下部にあるマッピング セクションで、マッピングされた送信元組織を表示することもできます。

    [すべてマッピング解除（Un-Map All）] オプションを使用して、選択した Intersight アカウント内の既存の送信元組織から接続先組織へのマッピングをすべて解除します。また、マッピング セクションに移動し、マッピングされたエンティティを選択し、そのエンティティの 3 つのドットをクリックして、マッピング解除オプションを選択することにより、マッピングされた単一のエンティティをマッピング解除できます。

19. [次へ（Next）] をクリックします。

[次へ（Next）] は、すべての送信元 UCS 組織が選択され、それぞれの接続先 Intersight 組織にマップされている場合にのみ有効と表示されます。

準備レポートが生成されます。設定属性が UCS Manager/UCS Central から取得され、IMM に変換され、結果のレポートが生成されるため、このプロセスには数分かかる場合があります。

（注） UCS Manager/Central 構成のサイズと接続されているサーバの数によっては、一部の操作が完了するまでにかなりの時間がかかる場合があります（1 時間以上）。

20. **[レポート（View Report）]** をクリックしレポートを表示するか、**[ダウンロード（Download）]** オプションを使用して PDF 形式でレポートをダウンロードします。

    レポートの解釈の詳細については、「移行準備レポートの解釈」を参照してください。

    選択した構成のレポート生成は 1 回限りのアクティビティであり、再生成することはできません。これにより、移行の履歴が維持され、いつでも参照できるようになります。構成を編集してレポートを生成する場合は、移行を複製できます。詳細については、「移行管理」を参照してください。

21. [次へ（Next）] をクリックします。

    [Intersight へのプッシュ（Push to Intersight）] ページが表示されます。

（注） IMM 移行ツール リリース 1.0.2 以降では、使用可能な構成ファイルをダウンロードして手動で編集し、**[詳細オプション]** を使用して同じものをアップロードできます。

22. **[詳細オプション]** をクリックし、編集したファイルを参照して、**[アップロード]** をクリックします。

    アップロードされたファイルは、構成を Intersight にプッシュするために使用されます。

23. [次へ（Next）] をクリックします。

    Intersight との接続が確立され、変換された構成属性が Intersight にプッシュされます。

（注）
- 遷移が Intersight デバイスを使用する Intersight にプッシュされている場合、または UCS Manager/UCS Central デバイスから UCSM 構成/インベントリをフェッチしている場合、デバイスの前のタスクが完了するまで、同じデバイスを他の遷移で使用することはできません。
- 変換されたポリシーが Intersight にプッシュされている場合は、それらのポリシーのデフォルト パスワードをリセットします。

24. **[プッシュ サマリを表示（View Push Summary）]** をクリックして、変換された各オブジェクトのプッシュ ステータスを表示します。

    この概要により、各オブジェクトのプッシュ ステータスを知ることができます。各オブジェクト ステータスの横にある 3 つのドット（...）をクリックすると、オブジェクトを Intersight にプッシュするために IMM 移行ツールによって実行された詳細なコミットが表示されます。ステータスには、次のいずれかを指定できます。

    - 成功（Success）：変換されたオブジェクトは、Intersight に正常にプッシュされました。
    - スキップ（Skipped）：変換されたオブジェクトは接続先の Intersight アカウントに既に存在し、プッシュ操作でスキップされました。
    - 失敗（Failed）：変換されたオブジェクトを Intersight にプッシュできませんでした。

      オブジェクト ステータスの横にある 3 つのドットをクリックして、プッシュの失敗の理由を確認します。

クローニングのための IMM 移行の追加

Intersight アカウントのクローニングを開始するには、次の手順を実行します。

1. [IMM 移行の追加（Add IMM Transition）] をクリックします。
2. 移行の名前を入力します。
3. 移行のタイプを選択します。

   構成をクローニングして、ある Intersight アカウントから別のアカウントに移行する場合は、**[Intersight のクローニング（Clone Intersight）]** を選択します。このオプションは、2 つの SaaS Intersight アカウント間、2 つの仮想アプライアンス アカウント間で、仮想アプライアンス Intersight アカウントからクラウド Intersight アカウントに、またはその逆に構成ポリシーを移行するために使用できます。クローニングでサポートされる機能の詳細については、「クローニングでサポートされる機能」を参照してください。
4. [次へ（Next）] をクリックします。
5. 送信元 Intersight アカウントを選択します。

   （a）既存の Intersight アカウントの構成を移行する場合は、**[既存のアカウントから選択（Choose from existing account）]** オプションを選択します。

   （b）新しい **[SaaS Intersight]** または新しい **[Intersight アプライアンス VM（Intersight Appliance VM）]** アカウントの構成を移行する場合は、**[新しいアカウントの追加（Add new account）]** オプションを選択します。API キー ID と秘密鍵の詳細については、手順 8 と 9 を参照してください。必要に応じて、プロキシ設定を有効にします。プロキシ設定を有効にする手順については、「プロキシ設定」を参照してください。
6. 接続先の Intersight アカウントを選択します。

（a）既存の Intersight アカウントの構成を移行する場合は、**[既存のアカウントから選択（Choose from existing account）]** オプションを選択し、手順 10 に進みます。

（b）新しい **[SaaS Intersight]** または新しい **[Intersight アプライアンス VM（Intersight Appliance VM）]** アカウントの構成を移行する場合は、**[新しいアカウントの追加（Add new account）]** オプションを選択し、手順 8 に進みます。必要に応じて、プロキシ設定を有効にします。プロキシ設定を有効にする手順については、「プロキシ設定」を参照してください。

（注） リリース 4.0.1 以降から、**[SaaS Intersight]** アカウントを選択する場合、以下に属するアカウントの地域も選択できます。**米国**または **EU**。

7. **[更新（Refresh）]** をクリックして、既存の Intersight アカウントから最新の構成を取得し、手順 10 に進みます。

   [ダウンロード（Download）] リンクを使用して、構成 JSON ファイルをダウンロードできます。

   構成 JSON ファイルには、既存の Intersight アカウントに存在するソフトウェア構成の詳細情報が含まれています。

   このファイルは、トラブルシューティングの目的でテクニカルサポートチームと共有できます。

8. 次の手順を実行して、Intersight から API キー ID を生成します。

   1. Intersight アプリケーションにログインします。
   2. 右上隅にある歯車アイコンをクリックし、[設定（Settings）] を選択します。
   3. [API] セクションで、[API キー（API Keys）] をクリックします。
   4. ページの右上にある [API キーの生成] をクリックします。
   5. **[説明（Description）]** フィールドに名前を入力し、**[OpenAPI スキーマ バージョン 2 またはバージョン 3 の API キー（API Key for OpenAPI Schema Version 2 or Version 3）]** を選択します。
   6. [生成（Generate）] をクリックします。

   API キー ID と秘密鍵が生成されます。**[クリップボードにコピー（Copy to Clipboard）]** の青いアイコンを使用して、これらの値をクリップボードにコピーします。IMM 移行ツール アプリケーションに戻ります。

9. 次のフィールドに入力します。

   • API キー ID：前の手順で生成された API キー ID を入力します。

   • 秘密鍵：Intersight で生成された秘密鍵を入力します。

   また、Intersight アプライアンス VM を選択した場合は、FQDN を入力します。

10. [次へ（Next）] をクリックします。
11. 移行に必要な変換オプションを構成します。
    - IMM 移行ツール 3.1.1 以降では、アカウントのクローン作成中に、すべての UCS サーバー プロファイルで割り当てられた ID を保持できます。^ 詳細については、「デフォルト設定」の「**C. クローンの移行設定**」セクションを参照してください。
12. [Next] をクリックします。
13. 変換する必要があるサーバー プロファイル/テンプレートを選択します。

（注） IMM 移行ツール 4.0.1 で、クローニングが必要な特定のサーバー プロファイルを選択できます。サーバープロファイルに関連付けられているポリシーおよびテンプレートもクローニングされます。

上部にある検索バーを使用して、特定のサーバープロファイル/テンプレートを検索できます。

検索バーの横にある **[表示（Show）]** ドロップダウン リストで、テンプレート、組織、プロファイル、テンプレートのみを表示するようにフィルタを適用できます。

ボタンを無効にする場合、すべてのサーバープロファイル、テンプレート、関連付けられているポリシーもクローニングされます。

14. [次へ（Next）] をクリックします。

    [Intersight へのプッシュ（Push to Intersight）] ページが表示されます。

（注） IMM 移行ツール リリース 1.0.2 以降では、使用可能な構成ファイルをダウンロードして手動で編集し、**[詳細オプション]** を使用して同じものをアップロードできます。

15. **[詳細オプション]** をクリックし、編集したファイルを参照して、**[アップロード]** をクリックします。

    アップロードされたファイルは、構成を Intersight にプッシュするために使用されます。
16. [次へ（Next）] をクリックします。

    Intersight との接続が確立され、変換された構成属性が Intersight にプッシュされます。
17. **[プッシュ サマリを表示（View Push Summary）]** をクリックして、変換された各オブジェクトのプッシュ ステータスを表示します。

    この概要により、各オブジェクトのプッシュ ステータスを知ることができます。各オブジェクト ステータスの横にある 3 つのドット（...）をクリックすると、オブジェクトを Intersight にプッシュするために IMM 移行ツールによって実行された詳細なコミットが表示されます。ステータスには、次のいずれかを指定できます。

- 成功（Success）：変換されたオブジェクトは、Intersight に正常にプッシュされました。
- スキップ（Skipped）：変換されたオブジェクトは接続先の Intersight アカウントに既に存在し、プッシュ操作でスキップされました。
- 失敗（Failed）：変換されたオブジェクトを Intersight にプッシュできませんでした。

  オブジェクト ステータスの横にある 3 つのドットをクリックして、プッシュの失敗の理由を確認します。

アップロードした構成をプッシュするための IMM 移行の追加

JSON 構成ファイルを直接アップロードし、Intersight アカウントにプッシュするには、次の手順を実行します。

1. [IMM 移行の追加（Add IMM Transition）] をクリックします。
2. 移行の名前を入力します。
3. **[構成のアップロード + Intersight にプッシュ（Upload Configuration + Push to Intersight）]** を選択して、JSON 構成ファイルをアップロードし、Intersight にプッシュします。
4. [次へ（Next）] をクリックします。
5. 接続先の Intersight アカウントを選択します。

   （a）**[既存のアカウントから選択（Choose from existing account）]** オプションを選択し、既存の Intersight アカウントの構成を移行する場合は、手順 8 に進みます。

   （b）新しい **[Intersight SaaS]** または新しい **[Intersight アプライアンス VM（Intersight Appliance VM）]** アカウントに構成をアップロードする場合は、**[新しいアカウントの追加（Add new account）]** オプションを選択します。
6. 次の手順を実行して、Intersight から API キー ID を生成します。
   1. Intersight アプリケーションにログインします。
   2. 右上隅にある歯車アイコンをクリックし、[設定（Settings）] を選択します。
   3. [API] セクションで、[API キー（API Keys）] をクリックします。
   4. ページの右上にある [API キーの生成] をクリックします。
   5. **[説明（Description）]** フィールドに名前を入力し、**[OpenAPI スキーマ バージョン 2 またはバージョン 3 の API キー（API Key for OpenAPI Schema Version 2 or Version 3）]** を選択します。
   6. [生成（Generate）] をクリックします。

API キー ID と秘密鍵が生成されます。**[クリップボードにコピー（Copy to Clipboard）]** の青いアイコンを使用して、これらの値をクリップボードにコピーします。IMM 移行ツール アプリケーションに戻ります。

7. 次のフィールドに入力します。

   • API キー ID：前の手順で生成された API キー ID を入力します。

   • 秘密鍵：Intersight で生成された秘密鍵を入力します。

   また、Intersight アプライアンス VM を選択した場合は、FQDN を入力します。

8. [次へ（Next）] をクリックします。

   [構成を Intersight にプッシュする（Push configuration to Intersight）] ページが表示されます。

（注） エラーが発生した場合は、**[強制プッシュ（Force Push）]** トグル ボタンを有効にすると、ツールが失敗したオブジェクトを無視して、Intersight への構成のプッシュに進むことができます。

9. JSON 構成ファイルを選択するために、**[参照（Browse）]** をクリックします。

10. [アップロード（Upload）] をクリックします。

    アップロードされたファイルは、構成を Intersight にプッシュするために使用されます。

11. [次へ（Next）] をクリックします。

    Intersight との接続が確立され、アップロードされた構成属性が Intersight にプッシュされます。

12. **[プッシュ サマリを表示（View Push Summary）]** をクリックして、変換された各オブジェクトのプッシュ ステータスを表示します。

    この概要により、各オブジェクトのプッシュ ステータスを知ることができます。各オブジェクト ステータスの横にある 3 点ドット メニュー（...）をクリックすると、オブジェクトを Intersight にプッシュするために IMM 移行ツールによって実行された詳細なコミットが表示されます。ステータスには、次のいずれかを指定できます。

    • 成功（Success）：変換されたオブジェクトは、Intersight に正常にプッシュされました。

    • スキップ（Skipped）：変換されたオブジェクトは接続先の Intersight アカウントに既に存在し、プッシュ操作でスキップされました。

    • 失敗（Failed）：変換されたオブジェクトを Intersight にプッシュできませんでした。

      オブジェクト ステータスの横にある 3 つのドットをクリックして、プッシュの失敗の理由を確認します。

移行管理

ユーザーによって開始されたすべての遷移は、**[移行（Transition）]**リスト ページに一覧表示されます。このページには、移行の名前、移行の現在のステータス（キャンセル済み、失敗、未完了、進行中、完了）、タイプ（準備状況レポートの生成、Intersight への移行構成、Intersight のクローン）、最終変更時刻が表示されます。

必要なアクションを実行するには、各遷移レコードにある **[...]** をクリックします。

- **[レポート（Report）]** をクリックして、移行の準備状況レポートを表示します。

  このオプションは、キャンセルされた遷移および失敗した遷移では使用できません。

- **[編集（Edit）]** をクリックして、移行名を変更します。

- **[削除（Delete）]** をクリックし、移行を削除します。

  複数のトランジションを選択し、リストビューの左上にあるゴミ箱ボタンをクリックすると、選択したトランジションをまとめて削除できます。

- **[クローン（Clone）]** をクリックして、既存の移行構成をコピーします。

  (a) 移行の名前を指定します。*[*未完了（*Incomplete*）*]* のステータスでリスト ページに表示されます。

  (b) **[移行名（Transition）]** をクリックして構成を編集し、準備状況レポートを生成して、変更した構成を Intersight にプッシュします。

（注） **[クローン（Clone）]** オプションは、タイプが **Intersight のクローン** の移行では使用できません。

- **[ログのダウンロード（Download Logs）]** をクリックして、変換ログをファイルにダウンロードします。

移行準備レポートの説明

IMM 移行準備レポートには、IMM への移行のための UCS Manager または UCS Central デバイスのハードウェア インベントリとソフトウェア構成の互換性の概要が表示されます。

準備レポートは次のセクションに分かれています。

1. **変換スコア**：このセクションには、ハードウェア互換性（UCS Manager ドメインでのみ対応）、ファブリック構成（UCS Manager ドメインでのみ対応）、およびサーバー ポリシー構成のスコア メーターが表示されます。

- スコアメーターの解釈は、次のように説明できます。
  - 優れています：ほとんどすべてのハードウェア / 構成を Intersight に移行できますが、多少の相違はあります。
  - 非常に良い：ほとんどのハードウェア / 構成は移行できますが、一部のハードウェア / 構成はサポートされていないか、Intersight への移行時に矛盾に直面する可能性があります。
  - 良好：ハードウェア / 構成の約半分は Intersight に移行できますが、残りのハードウェア / 構成はサポートされていないか、Intersight への移行中に矛盾に直面する可能性があります。
  - 悪い：少数のハードウェア / 構成のみを Intersight に移行できますが、多くのハードウェア / 構成がサポートされていないか、Intersight への移行中に矛盾に直面する可能性があります。

（注） 上記の評価は、一般的な使用例に基づいています。特定の環境の詳細レポートを確認して、ドメインへの移行の影響を評価することを強くお勧めします。

2. **全体の要約**：全体の要約セクションは、IMM 変換の注意点、ハードウェア互換性の要約（UCS Manager ドメインでのみ）、および IMM 構成変換の要約で構成されます。
   - Intersight マネージド モード変換の注意点：このセクションでは、変換プロセスを開始する前に確認する必要がある注意点を示します。変換プロセスに関連するエラーと Warning（注意）が表示されます。エラーは変換がサポートされていない要素を示し、Warning は完全に変換できない要素のリストを示します。
   - ハードウェア互換性の概要：ファブリック インターコネクト、ファブリック エクステンダ、アダプタ、IO モジュール、シャーシ、ブレード、ラックなど、該当するハードウェア コンポーネントごとに個別の円グラフが表示されます。円グラフのカラー コードは、次のように説明されます。
     - 緑色は、ハードウェアが移行に対応していることを示します。
     - オレンジ色は、ハードウェアの互換性のためにファームウェアのアップグレードが必要であることを示しています。
     - 赤色は、ハードウェアが現在移行に対応していないことを示しています。

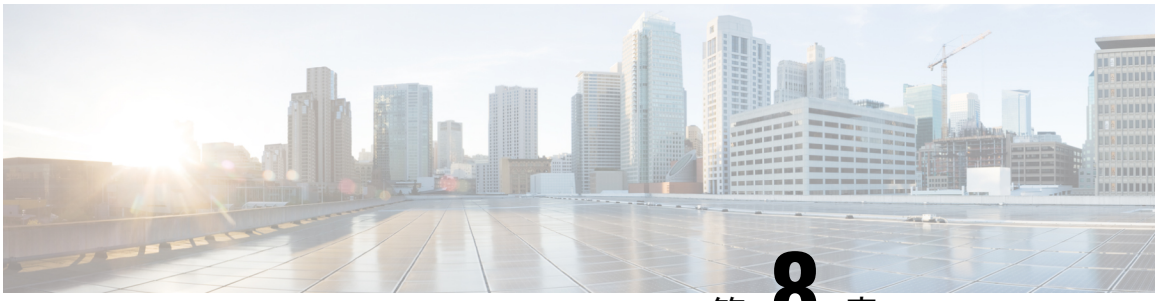
（注） ハードウェア互換性サマリーは、UCS Central ではなく、UCS Manager ドメインに対してのみ生成および表示されます。

- **Intersight 管理モード構成変換の概要**：このセクションには、UCS Manager と UCS Central オブジェクトと、Intersight の対応する変換されたオブジェクトのマッピングテーブルが表示されます。サーバープロファイルテンプレート、サーバープロファイル、ドメインポリシー、プール、サーバーポリシーなどの論理オブジェクトごとに個別のテーブルが表示されます。

3. **ハードウェアの互換性**：このセクションには、UCS Manager ドメインに関して、インベントリの各コンポーネントの互換性レポートが詳細に表示されます。これは、ファブリック ハードウェア互換性レポート、シャーシ ハードウェア互換性レポート、ラック ハードウェア互換性レポートなどで構成されています。各コンポーネントをクリックすると、互換性レポートの表が表示されます。この表は、ハードウェアの詳細をリストし、ハードウェアとファームウェアに互換性があるかどうかを示しています。左側の黄色の見出しは、IMM 対応になるためにファームウェア アップグレードが必要なコンポーネントがほとんどないという Warning（注意）を示しています。左側の赤い色の見出しは、IMM 移行と互換性のないコンポーネントがほとんどないというエラーを示しています。左側の青色の見出しは、Informational（情報提供）メッセージを示しています。

4. **構成変換**：このセクションでは、UCS Manager/Central の選択されたサービス プロファイルテンプレートで各論理オブジェクトの詳細な互換性レポートを示します。各オブジェクトの見出しをクリックすると、説明の表が表示されます。これらの表には、変換中に使用される属性名と値、ソース UCS Manager/Central と変換された Intersight オブジェクトのマッピング、デバイスの起動順序などがリストされています。黄色のアイコンは、一部のオブジェクトを完全に変換できなかったという Warning（注意）を示します。赤色のアイコンは、サポートされていないオブジェクトがほとんどなく、変換できないというエラーを示しています。青色のアイコンは、Informational（情報提供）メッセージを示します。このメッセージに従って対処できます。

5. **ソース構成リファレンス —** このセクションでは、ソース UCS デバイス プールに存在する構成の詳細を示し、サービス プロファイルと物理サーバーに割り当てられた IP アドレスの詳細を提供します。



第 8 章

デバイス管理

- デバイス管理 （39 ページ）
- デバイスの申請 （40 ページ）
- カスタム デバイス ファイルのアップロード （41 ページ）

デバイス管理

IMM 移行ツール、リリース 1.0.2 以降を使用すると、UCS システムと Intersight デバイスをより適切に管理できます。各デバイスに一意のターゲット IP または FQDN を提供することで、デバイスの重複を避けることができます。

デバイスを追加および管理するには、次の手順を実行します。

1. **[デバイス管理（Device Management）]** に移動します。
2. [デバイスの追加（Add Device）] をクリックします。
3. ドロップダウン リストから **[デバイスタイプ（Device Type）]** を選択します。
4. ターゲット IP/FQDN を入力します
5. ステップ 3 で選択したデバイス タイプが **UCS Manager** または **UCS Central** の場合は、デバイスの**ユーザー名**を入力します。そうでない場合は、ステップ 7 に進みます。
6. デバイスの**パスワード**を入力し、ステップ 9 に進みます。
7. ステップ 3 で選択したデバイス タイプが **Intersight** の場合は：

   (a) SaaS アカウントに **[Intersight SaaS]** を選択し、API キー/秘密キーを入力します。

（注） リリース 4.0.1 以降から、**[Intersight SaaS]** アカウントを選択する場合、以下に属するアカウントの地域も選択できます。**米国**または **EU**。

   (b) アプライアンス アカウントに **[Intersight Appliance VM]** を選択し、ターゲット/API キー/秘密キーを入力します。

8. **[プロキシを使用（Use Proxy）]** トグル ボタンをオンにして、プロキシ設定を有効にします。

   プロキシ設定の詳細については、「プロキシ設定」を参照してください。

9. [保存（Save）] をクリックします。

   IMM 移行ツール 3.1.1 以降では、ツールによって検証が実行され、追加されたデバイスのファームウェア バージョンが移行ツールでサポートされる最小バージョンに準拠しているかどうかがチェックされます。準拠していないことが判明した場合、警告メッセージが表示されます。

   [検証のバイパス（Bypass Validation）] トグル ボタンをオンにすることで、検証チェックをオプトアウトできます。

追加されたデバイスは、削除または編集できます。Intersight デバイスで編集できる値は API キーとシークレット キーで、UCS デバイスで編集できる値はユーザー名とパスワードです。

（注）
- 既存のデバイスの削除は、それに関連付けられた遷移がない場合にのみ可能です。
- IMM 移行ツール、3.1.1 で、複数のデバイスを選択し、リスト ビューの左上にあるゴミ箱ボタンをクリックすると、選択したデバイスをまとめて削除できます。

デバイスの申請

Intersight でデバイスを申請する方法：

1. **[Intersight に申請（Claim to Intersight）]** をクリックします。
2. **[デバイスの選択]** 画面の場合：
   1. **[Intersight デバイスの選択（Select Intersight Device）]** ドロップダウン リストから、デバイスを申請するターゲットの Intersight アカウントを選択します。
   2. [テーブル（Table）] ビューから、申請する **Cisco IMC** または **UCS Manager** デバイスを選択します。新しいデバイスを追加する場合は、「**デバイスの追加**」の項の手順に従います。
   3. **[次へ（Next）]** をクリックします。
3. **[デバイス コネクタ（Device Connector）]** 画面で、次の手順を実行します。
   1. アクセス モードを開始します。
   2. 選択したデバイスが Intersight アカウントに接続するために使用するプロキシの詳細を入力します。

（注） これらのオプションは、UCSM または Cisco IMC デバイスの [デバイス コネクタ（Device Connector）] ページから設定することもできます。

3. **[次へ（Next）]** をクリックします。

   構成した設定が選択したデバイスにプッシュされます。

4. **[進行状況（Progress）]** 画面から申請アクションの進行状況をモニタリングします。

   リスト ビューでは、正常に要求されたデバイスは **クラウド** アイコンで示されます。**[クラウド（Cloud）]**アイコンにカーソルを合わせると、要求されたデバイスにリンクされている Intersight アカウントに関する追加情報を表示できます。

カスタム デバイス ファイルのアップロード

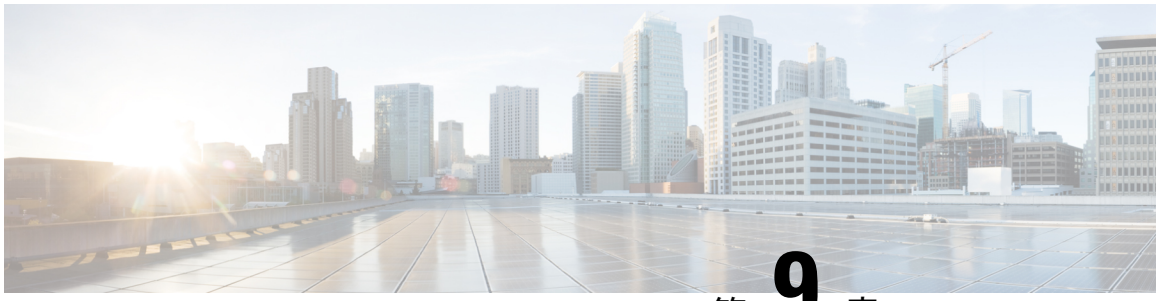
デバイスの構成またはインベントリ ファイルを編集およびアップロードできます。このアップロードされたファイルは、後で Intersight に遷移を追加、クローニング、またはプッシュするときに使用できます。

デバイスのカスタムファイルを追加するには、次の手順を実行します。

1. **[デバイス管理（Device Management）]** に移動します。
2. リストページで、構成またはインベントリを更新する必要があるデバイスに移動します。
3. デバイス名の横にあるその他メニューをクリックします。
4. **[カスタム ファイルのアップロード（Upload Custom File）]** をクリックします。
5. 更新された構成ファイルを参照し、選択します。
6. [アップロード（Upload）] をクリックします。
7. 更新されたインベントリ ファイルを参照し、選択します。
8. [アップロード（Upload）] をクリックします。
9. [OK] をクリックします。

アップロードされたファイルは、トランジションの追加中にソースまたは接続先デバイスのページでデバイスが次に選択されたときに取得されます。

移行の追加中、ライブデバイスから取得された設定/インベントリは で表され、ファイルから取得された設定/インベントリ（ユーザーが手動でアップロード）は、**[ソース UCS/Intersight デバイスの選択（Select Source UCS/Intersight Device）]** ページの で示されます。



第 9 章

ソフトウェアリポジトリ

- 概要 （43 ページ）
- フォルダの作成およびファイルのアップロード （43 ページ）
- フォルダの管理 （45 ページ）
- ファイルの管理 （47 ページ）

概要

IMM 移行ツール 4.0.1 で、ソフトウェア リポジトリとしてツールを使用して、Operating System images（ISO）、Server Configuration Utility（SCU）またはファームウェア パッケージを管理およびホストできます。Intersight でこれらの画像を同期したら、これらの画像を使用して、Cisco UCS サーバーにオペレーティング システムをインストールし、ファームウェアをアップグレードできます。

ソフトウェア リポジトリに新規フォルダを作成し、ファイルをアップロードできます。詳細については、次のセクションを参照してください。

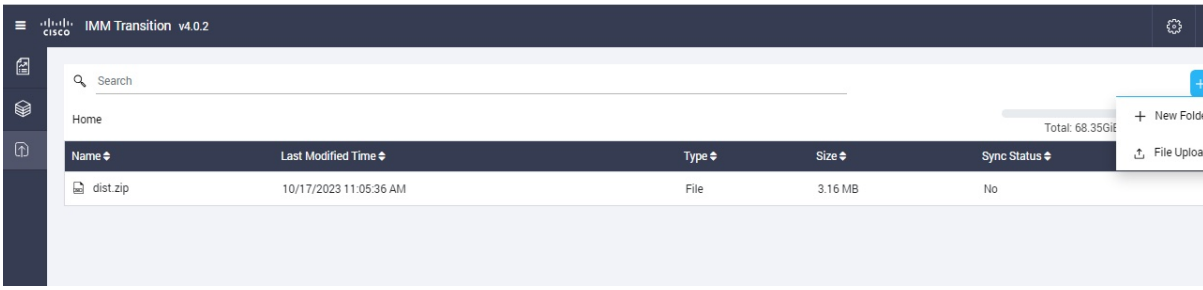
- フォルダの作成およびファイルのアップロード
- フォルダの管理
- ファイルの管理

フォルダの作成およびファイルのアップロード

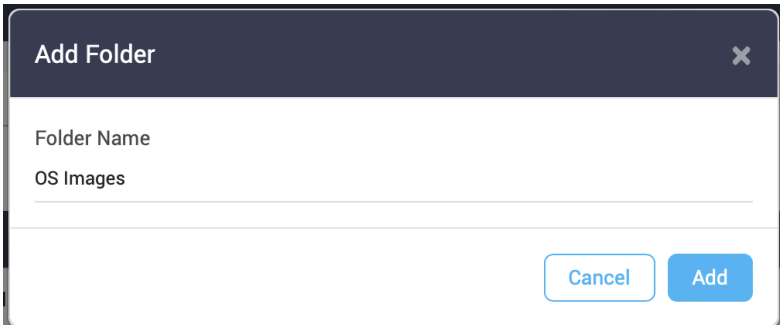
フォルダの追加

要件に従って iso ファイルをグループ化し、別のフォルダに保持できます。以下に説明するように、新規フォルダは IMM 移行ツールのソフトウェア リポジトリで作成できます。

1. **[ソフトウェア リポジトリ（Software Repository）]** に移動します。
2. 以下のスクリーンショットに示すように、**[新規（New）]** をクリックします。



3. **[新規フォルダ（New Folder）]** をクリックします。
4. フォルダの名前を入力します。

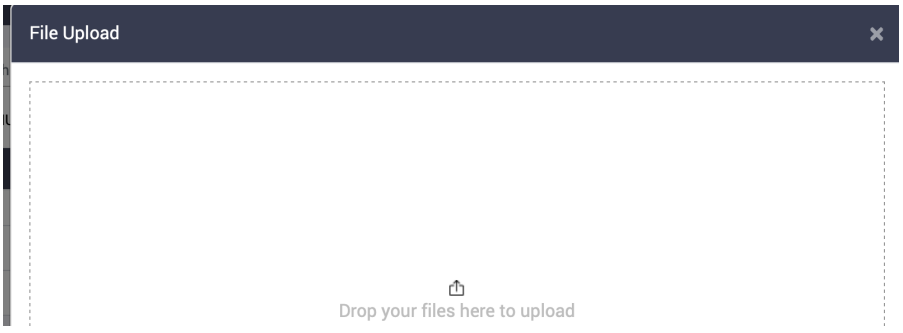


5. [追加（Add）] をクリックします。
   新規フォルダが作成されます。

ファイルをアップロードしています

次の手順を実行し、ソフトウェア リポジトリに iso ファイルをアップロードします。

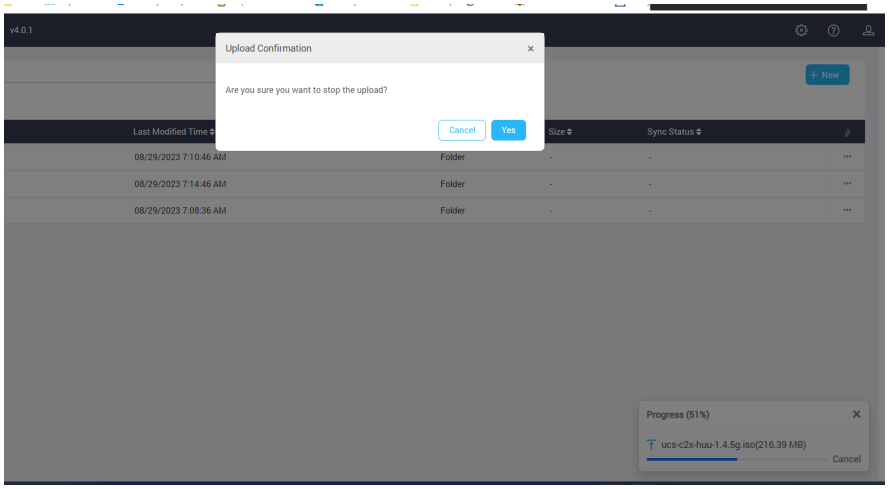
1. **[ソフトウェア リポジトリ（Software Repository）]** に移動します。
2. 以下のスクリーンショットに示すように、**[新規（New）]** をクリックします。
3. **[ファイルのアップロード（File Upload）]** をクリックします。
   ファイル ブラウズ ウィンドウが表示されます。



4. ローカル システムからファイルをドロップします。

5. [Upload] をクリックします。

   ファイルがソフトウェア リポジトリにアップロードされます。



（注） [進行中（Progress）] ポップアップ ウィンドウの **[キャンセル（Cancel）]** をクリックすると、確認ダイアログ ボックスが表示されます。

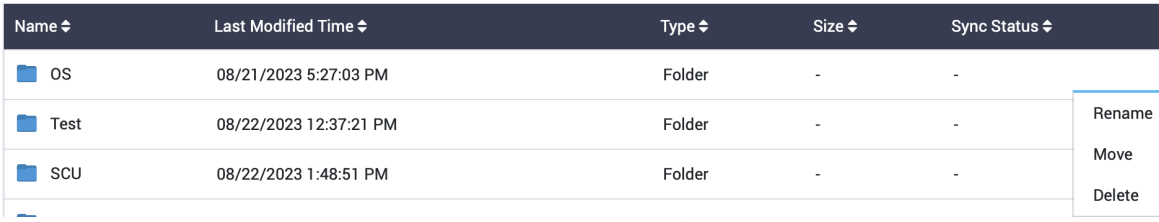
[はい（Yes）] をクリックして、ファイル**[アップロード（Upload）]**操作をキャンセルします。

フォルダの管理

[ソフトウェア リポジトリ（Software Repository）] タブの一覧ページでは、フォルダに属さないフォルダおよびファイルのリストを表示します。フォルダを名前変更、移動、削除してフォルダを管理できます。

以下のアクションを実行して、**Software Repository** 一覧ページからフォルダを管理できます。

- 管理するフォルダ行の横にある **[...]** をクリックします。



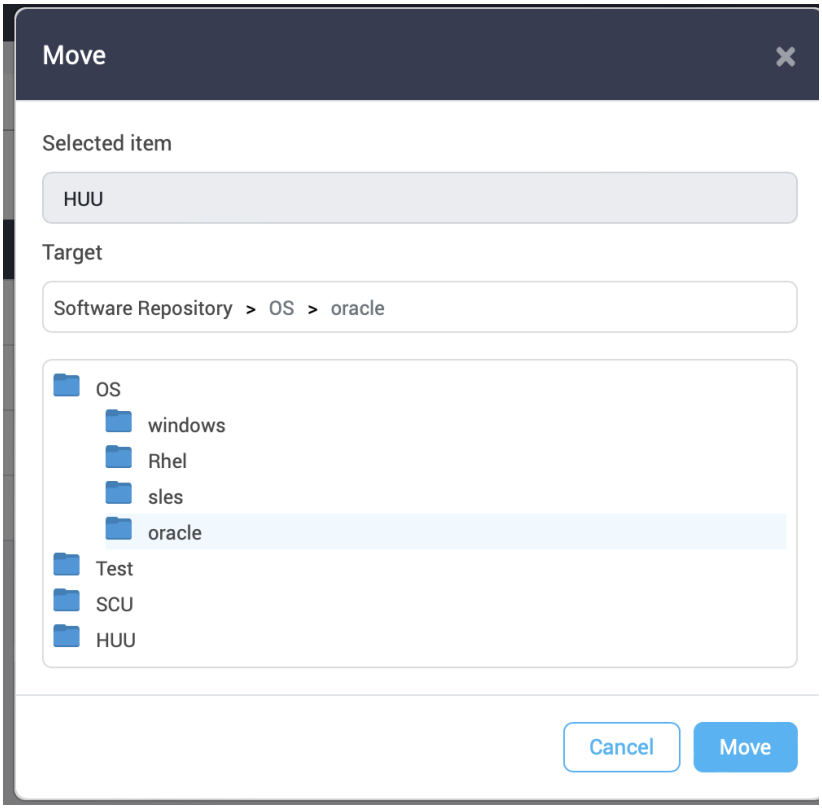
- フォルダの名前を変更する場合には、**[名前の変更（Rename）]** をクリックします。

  1. ポップアップ ウィンドウが表示されます。
  2. フォルダに新しい名前を入力します。

3. **[保存（Save）]** をクリックします。

- フォルダを他のフォルダ内に移動する場合は、**[移動（Move）]** をクリックします。

1. ポップアップ ウィンドウが表示されます。
2. 現在のフォルダを移動する必要があるフォルダをクリックします。



3. [移動（Move）] をクリックします。

- リポジトリからフォルダを削除する場合、 **[削除（Delete）]** をクリックします。

（注）

- フォルダの名前が変更されると、このフォルダ内のファイルへの外部リンクは更新する必要があります。
- フォルダが移動または削除される場合：
  - このフォルダ内のファイルへの外部リンクは更新する必要があります。
  - **[Intersight への同期（Sync to Intersight）]** アクションは、このフォルダ内のすべてのファイルに対して無効になります。
  - このフォルダ内のファイルの計算されたチェックサムはすべて失われます。

ファイルの管理

ソフトウェア レポジトリにアップロードされた iso ファイルは、特定のフォルダに属していない場合、またはアップロードされた特定のフォルダ内にある場合は、一覧ページで表示できます。

以下の手順を実行して、ソフトウェア レポジトリでファイルを管理します。

1. ファイルが存在するフォルダに移動します。
2. 管理するファイル レコードの最後にある **[..]** をクリックします。

ファイルの名前変更：

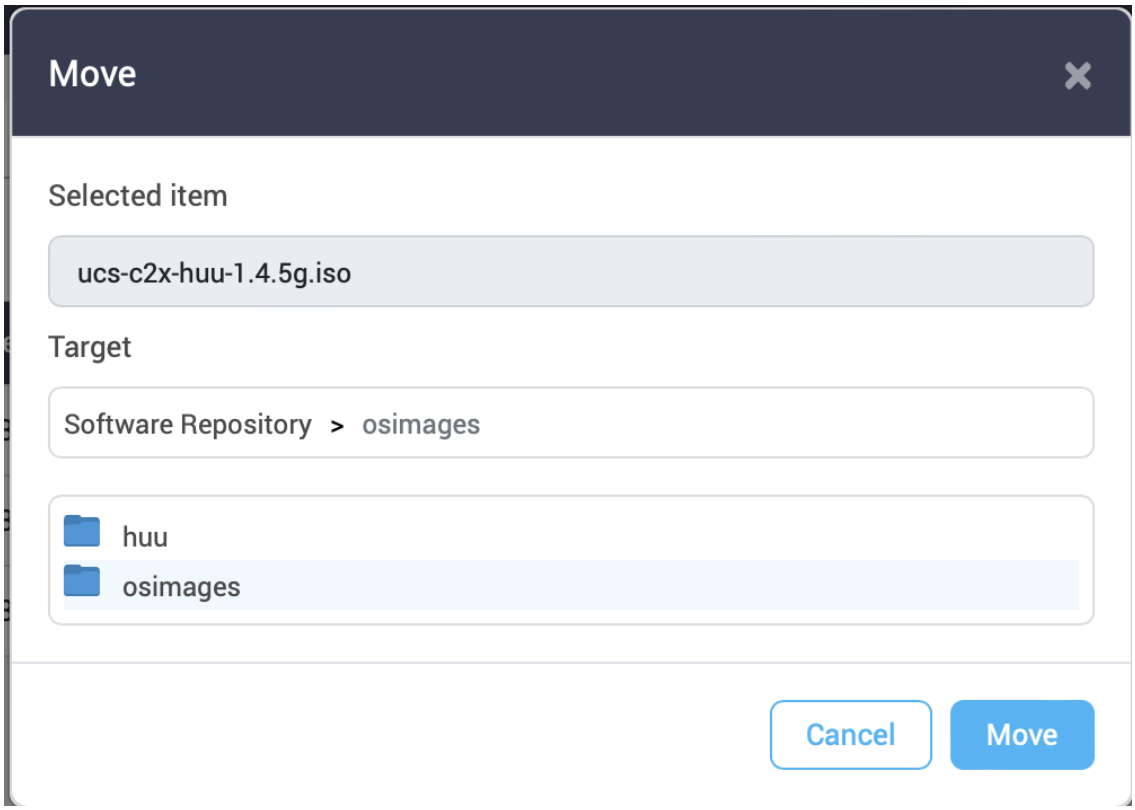
- 1. [Rename] をクリックします。

  ポップアップ ウィンドウが表示されます。
- 2. ファイルの新しい名前を入力します。
- 3. [**Save**] をクリックします。

ファイルの移動：

- 1. [移動（Move）] をクリックします。

  ポップアップ ウィンドウが表示されます。
- 2. ファイルを移動する必要があるフォルダをクリックします。



3. [移動（Move）] をクリックします。

ファイルの削除：

- [削除（Delete）] をクリックします。

別のツールを使用するファイルの場所を共有する：

- 1.**[リンクの共有（Share Link）]** をクリックします。

  ポップアップ ウィンドウが表示されます。

- 2. [Copy] をクリックします。

  ファイルの場所がクリップボードにコピーされ、必要に応じて使用できます。

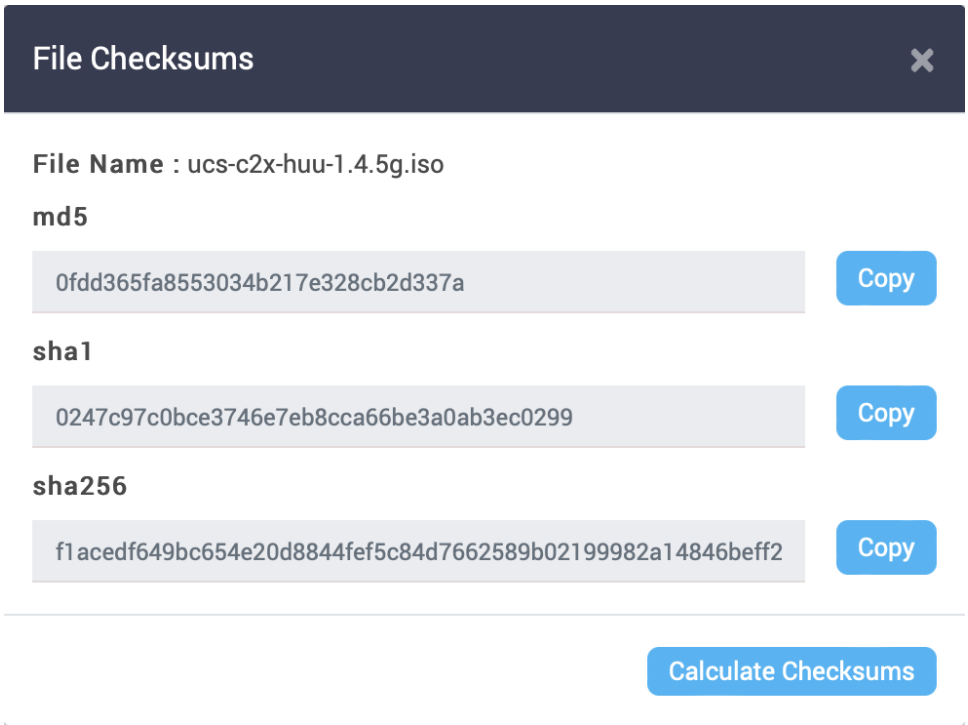
ファイルのチェックサムの計算：

- 1.**[チェックサム（Checksum）]** をクリックします。

  ファイル チェックサムのポップアップ ウィンドウが表示されます。

- 2.**[チェックサムの計算（Calculate Checksums）]** をクリックします。

  チェックサム値が表示されます。



Intersight へのファイルの同期：

- **[Intersight への同期（Sync to Intersight）]** をクリックします。

  詳細については、「Intersight へのファイルの同期」を参照してください。

（注）

- ファイルの名前が変更されると、ファイルへの外部リンクを更新する必要があります。
- ファイルが移動または削除される場合：
  - ファイルへの外部リンクを更新する必要があります。
  - **[Intersight への同期（Sync to Intersight）]** アクションは、ファイルなどに対して無効になります。
  - すべてのファイルの計算されたチェックサムが失われます。

Intersight へのファイルの同期

IMM 移行ツールのソフトウェア レポジトリにあるアップロードされた iso ファイルは、以下の手順を実行して、Intersight ソフトウェア レポジトリへリンク可能です。

1. ファイルが存在するフォルダに移動します。
2. 同期するファイル レコードの最後にある **[..]** をクリックします。

3. **[Intersight への同期（Sync to Intersight）]** をクリックします。

   ポップアップ ウィンドウが表示されます。

4. 利用可能なデバイスのリストから、[Intersight デバイス（Intersight Device）] を選択します。

（注） **[OS/ファームウェア データのフェッチ（Fetch OS/Firmware data）]** を定期的にクリックすることをお勧めします。これにより、最新の OS およびファームウェア データすべてが Intersight アカウントからフェッチされます。

5. ソフトウェア レポジトリ リンクを保存する組織を選択します。
6. 自動選択された値が間違っている場合、またはツールがファイル タイプを自動検出できない場合、ファイルの画像タイプを手動で選択します。
7. 自動選択された値が間違っている場合、またはツールがファイル タイプを自動検出できない場合、OS 画像の詳細を設定または変更します。
8. [送信（Submit）] をクリックします。

画像を Intersight に同期し、Intersight GUI の **[システム> ソフトウェア レポジトリ（System> Software Repository）]** の **[ファームウェア リンク（Firmware Links）]**、**[OS 画像リンク（OS Image Links）]**、または **[SCU リンク（SCU Links）]**、または **[OS 変換ファイル（OS Configuration File）]** タブ に表示されます。

（注） ファイルやフォルダが移動されるたびに、ソフトウェア レポジトリ リンクは自動的更新されません。リンクを手動で削除し、**[Intersight への同期（Sync to Intersight）]** を再度実行する必要があります。

vMedia ポリシーの作成

次の手順で、ソフトウェア リポジトリでホストされている ISO ファイルから Intersight vMedia ポリシーを作成できます。

vMedia ポリシーの作成方法：

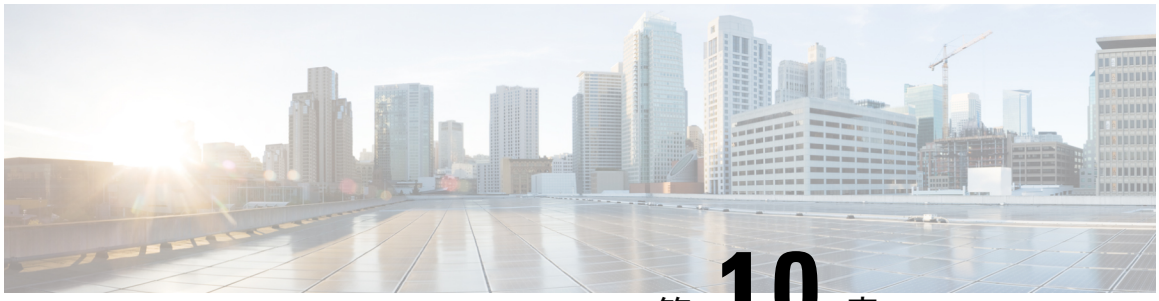
1. **[ソフトウェア リポジトリ（Software Repository）]** ページに移動します。
2. vMedia ポリシーの作成に使用する ISO ファイルの横にある **[…]** をクリックし、ドロップダウンリストから **[vMedia ポリシーの作成（Create vMedia Policy）]** を選択します。

   [vMedia ポリシーの作成（Create vMedia Policy）] ダイアログ ボックスが表示されます。

3. 利用可能なデバイスのリストから、[Intersight デバイス（Intersight Device）] を選択します。

注記：**[OS/ファームウェア データのフェッチ（Fetch OS/Firmware data）]** を定期的にクリックすることをお勧めします。これにより、最新の OS およびファームウェア データすべてが Intersight アカウントからフェッチされます。

4. ソフトウェア レポジトリ リンクを保存する組織を選択します。
5. ポリシーの名前を入力します。
6. （任意）ポリシーの短い説明を入力します。
7. （任意）key value 形式でタグを入力します
8. **[低電源 USBを有効にする（Enable Low Power USB）]** をオンにすると、イメージをマッピングしてホストを再起動した後に、ブート選択メニューに仮想ドライブが表示されます。このプロパティは、デフォルトで有効になっています。
9. 仮想メディア通信の暗号化を有効にするには、[仮想暗号化の有効化（**Enable Virtual Encryption**）] ボタンをオンにします。このプロパティは、デフォルトで無効になっています。
10. デフォルトでは、vMedia マウント名は、vMedia ポリシーの作成に使用される ISO ファイルの名前に設定されます。この名前は必要に応じて変更できます。
11. [Submit] をクリックします。



第 10 章

設定

- デフォルト設定 （53 ページ）
- プロキシ設定 （59 ページ）
- バックアップ/復元 （60 ページ）
- 証明書設定 （60 ページ）

デフォルト設定

A. デフォルト移行設定

ツールで作成されたすべての新しい移行に適用されるデフォルト構成を設定できます。**[デフォルト設定（Default Settings）]** オプションは、右上隅の **[設定（Settings）]** の下にあります。このオプションを使用して、変換されたポリシーのデフォルト パスワードを設定/リセットすることもできます。

デフォルトのトランジション設定で定義されたカスタム タグは、すべてのトランジションに適用されます。

設定フィールドのそれぞれの詳細については、下の「**変換の移行設定**」および「**クローンの移行設定**」セクションを参照してください。

B. [変換の移行設定（Transition Settings for Conversion）]

以下は、IMM 移行ツールの **[移行設定（Transition Settings）]** ページ にある変換オプションです。これらのオプションを設定/設定解除して、遷移の動作を制御できます。

1. **ファブリック ポリシーの変換**
    - このオプションは、デフォルトで有効です。有効にすると、UCS ファブリック構成は同等の Intersight ポリシーに変換されます。
    - 有効にすると、以下が変換されます。
        - VLAN / VLAN グループ / VSAN
        - FI ポートの構成

- UCS ドメイン設定（NTP、DNS、Syslog、SNMP、システム QoS、およびスイッチ制御ポリシー）

（注） ファブリック ポリシーの変換は、UCSM でのみサポートされています。

1. **ファブリック ポリシー名**

   変換後のファブリック ポリシー（VLAN、VSAN、ポート ポリシー）の名前を示します。変換されたポリシーに**手動**の名前を指定するか、変換後にUCS ドメイン名を保持することを選択できます。

2. **ファブリック ポリシーの対象組織名**

   ファブリック ポリシーが属する組織の名前を示します。組織の**手動**名を指定するか、変換後に UCS ドメイン名を保持することを選択できます。

3. **常に個別の VLAN ポリシーを作成する**

   - このオプションは、デフォルトで無効です。
   - 有効にすると、ファブリック A と B に対して個別の VLAN ポリシーが作成されます。無効にすると、ツールでファブリック A と B に対して単一または個別の VLAN ポリシーを作成するかどうかを決定します。

4. **常に個別の VSAN ポリシーを作成する**

   - このオプションは、デフォルトで無効です。
   - 有効にすると、ファブリック A と B に対して個別の VSAN ポリシーが作成されます。無効にすると、ツールでファブリック A と B に対して単一または個別の VSAN ポリシーを作成するかどうかを決定します。

5. **常に個別のポート ポリシーを作成する**

   - このオプションは、デフォルトで無効です。
   - 有効にすると、ファブリック A と B に対して個別のポート ポリシーが作成されます。無効にすると、ツールは、ファブリック A と B に対して単一または個別のポート ポリシーを作成するかどうかを決定します。

6. **シャーシ/ラック サーバー ID の保持**

   - このオプションは、デフォルトで無効です。
   - 有効にすると、シャーシ/ラック サーバー ID は、UCSM/Central で使用されているものと同じサーバー ポートに移行後に保持されます。

2. **サーバー ポリシーの変換**

- このオプションは、デフォルトで有効です。
- 有効にすると、選択したサーバーー ポリシー/プール/プロファイル/テンプレートが同等の Intersight ポリシー/プール/プロファイル/テンプレートに変換されます

1. **サービス プロファイルの変換**
   - このオプションは、デフォルトで有効です。
   - サービスプロファイルの変換が有効になっている場合、ユーザーは**[プロファイル/テンプレート（Select Profiles/Templates）]**手順で変換するプロファイルを選択できます。
   - 有効にすると、次の識別子が維持されない場合があります。
     - IP
     - MAC
     - IQN
     - UUID
     - WWN
2. **グローバル サービス プロファイルの変換**
   - このオプションは、デフォルトで無効です。
   - 有効にすると、選択したグローバル サービス プロファイルが同等の Intersight サーバー プロファイルに変換されます。

（注） この変換は UCSM にのみ適用されます。

3. **[アイデンティティの保存（Preserve Identities）]**
   - このオプションは、デフォルトで有効です。
   - 有効にすると、UCSからIMMへのサービスプロファイルの変換中に、IP、IQN、MAC、UUID、WWPN、WWNNなどの構成アイデンティティが保持されます。
4. **ルート組織名**
   - UCS 組織がマッピングされる Intersight 組織の名前を手動で入力できます。
   - または、接続先 Intersight 組織のデフォルトの UCS ドメイン名を選択します。
5. **ソース組織パスを Intersight 組織名に保持**
   - このオプションは、デフォルトで有効です。

- 有効にすると、UCS 組織「root/Org1/Org2」は、宛先の Intersight 組織で「Org1_Org2」という名前になります。
- 無効にすると、UCS 組織「root/Org1/Org2」は、宛先の Intersight 組織で「Org2」という名前になります。

6. **vNIC/vHBA オーダーに vCon 配置情報を使用**
   - このオプションは、デフォルトで無効です。
   - 有効にすると、vNIC/vHBA は、ソース vCon に応じて異なる PCIe スロットに静的にマッピングされます。
   - vCon any、1:「PCIe MLOM」、vCon2:「PCIe スロット 1」、vCon3:「PCIe スロット 2」および vCon4:「PCIe スロット 3」。
   - 入力を提供し、dafult マッピングを上書きすることで、vCon を PCIe スロットに手動でマッピングできます。

     vCon スロット値でサポートされる範囲は 1 ～ 15 です。
   - 無効にすると、vNIC/vHBA は自動 PCIe スロットで設定され、最初の VIC アダプタに解決されます。
7. **vNIC/vHBA 順序にホストポート情報を使用（VIC1300 の場合のみ使用）**：
   - このオプションは、デフォルトで無効です。
   - 有効にすると、vNIC/vHBA は、送信元管理ホスト ポートの値に対応する 2 つの PCI リンクに配置されます。これは、変換されたプロファイルが VIC 1300 モデルのサーバーに割り当てられている場合にのみ使用する必要があります。
   - 無効にすると、すべての vNIC/vHBA が単一の PCI リンクにマッピングされます。
8. **長い組織名（>17 文字）を自動的に変更する**
   - このオプションは、デフォルトで無効です。
   - 有効にすると、17 文字を超える組織名が自動生成された名前に変更されます。これにより、組織名と QoS ポリシーを合わせた長さが 40 文字を超える場合のエラーを防ぎます。
9. **電源ポリシーの変換（C シリーズ サーバーでは無効にする）**
   - このオプションは、デフォルトで無効です。
   - 電源ポリシーは、Cisco UCS B シリーズおよび Cisco UCS X シリーズ サーバーでサポートされるようになりましたが、Cisco UCS C シリーズ サーバーではサポートされません。Cisco UCS B シリーズおよび Cisco UCS X シリーズ サーバーに割り当てられたプロファイルを変換する場合にのみ、このオプションを有効にします。

10. UCS Central タグの変換

- このオプションは、デフォルトで有効です。
- 有効にすると、プール、ポリシー、およびプロファイル/テンプレートに割り当てられた UCS Central タグが変換され、準備状況レポートの対応する Intersight オブジェクトの「変換された UCS Central タグ」行で簡単に表示できます。

（注）
- この変換は、UCS Central にのみ適用されます。
- さまざまなタグ値を持つ UCS Central タグ タイプの重複を Intersight にプッシュすることはできません。これは、Intersight がタグ キーの重複を許可していないためです。ただし、最初の発生は Intersight にプッシュされます。

11. UCS Central タグ プレフィックス

IMM 移行ツール、リリース 3.1.1 は、UCS Central タグへのプレフィックスの追加をサポートしています。変換されたタグに**手動**プレフィックスを指定するか、変換後にデフォルトのプレフィックスを選択することができます。

（注） この変換は、UCS Central にのみ適用されます。

12. サービス プロファイルの関連付けの保持

- このオプションは、デフォルトで無効です。
- 有効にすると、サーバープロファイルは、UCSM/Central で使用されているものと同じサーバー シリアル番号に移行後に事前に割り当てられます。

3. 変換されたオブジェクトに自動的にタグを付ける

- このオプションは、デフォルトで有効です。
- 有効にすると、Intersight オブジェクトは "imm_migration_version": "4.0.1"、"imm_transition_name": "_imm_transition_name_" でタグ付けされます。
- **[+ 新規を追加]** ボタンをクリックし、**キーと値**のペアを入力することで、新しいタグを追加できます。
- 既存のタグは変更および削除できます。
- キーが「imm_migration_version」および「imm_transition_name」のタグは変更できませんが、削除できます。
- すべてのタグには一意のキーが必要ですが、値は複製できます。

- 同じ**キーと値**のペアを持つ重複タグは許可されていません。

4. **既存の Intersight オブジェクトを上書きする**
   - このオプションは、デフォルトで無効です。
   - 有効にすると、同じ名前とタイプのオブジェクトが組織に既に存在する場合、既存の Intersight オブジェクトは上書きされます。無効にすると、既存のオブジェクトは変更されません。
5. **共有組織のリソース グループ メンバーシップの削除**
   - このオプションは、デフォルトで無効です。

     共有組織の変換とクローニングがサポートされるようになりました。
   - 共有組織へのリソース グループ メンバーシップはサポートされていません。
   - 有効にしたときに、変換後に同じ組織が共有組織になる場合、Intersight の組織の既存のリソース グループ メンバーシップが削除されます。このオプションを無効にすると、Intersight は共有組織とのリソース グループ マッピングをサポートしていないため、共有組織のプッシュ中にエラーが発生します。
6. **変換されたポリシーのデフォルト パスワード**

   デフォルトのパスワードは、仮想メディア、iSCSI ブート、IPMI over LANなど変換されている UCS Manager/Central ポリシーで、既存のパスワードの代わりに使用されます。このパスワードは、ツールのインストール中に自動生成されます。このパスワードは、変換されたポリシーが Intersight にプッシュされた後、ユーザーがリセットする必要があります。
7. **iSCSI 相互チャップ認証のパスワード**

   このパスワードは、iSCSI ブート ポリシーの相互 CHAP 認証に使用されます。**変換されたポリシーのデフォルト パスワード**とは異なる必要があります。

C. クローニングの移行設定

以下は、IMM 移行ツールの **[移行設定（Transition Settings）]** ページにあるクローニング オプションです。これらのオプションを設定/設定解除して、遷移の動作を制御できます。

1. **既存の Intersight オブジェクトを上書きする**
   - このオプションは、デフォルトで無効です。
   - 有効にすると、同じ名前とタイプのオブジェクトが送信元組織に既に存在する場合、接続先 Intersight 内の既存のオブジェクトは上書きされます。
2. **[Intersight 設定のトリミング（Trim Intersight Settings）]**
   - このオプションは、デフォルトで有効です。
   - 有効にすると、ユーザーグループ、ユーザー、ロールなど、一部の Intersight 設定がクローニング中にトリミングされます。

3. **[アイデンティティの保存（Preserve Identities）]**
   - このオプションは、デフォルトで有効です。
   - 有効にすると、すべての UCS サーバー プロファイルで割り当てられた ID を保持しながら、Intersight アカウントを複製できます。
4. **サーバー プロファイルの関連付けの保持**
   - このオプションは、デフォルトで無効です。
   - 有効にすると、複製中にサーバー プロファイルの関連付けが保持されます。

プロキシ設定

IMM 移行ツール 3.1.1 には、デバイス レベルでプロキシ設定を有効または無効にするオプションがあります。**[プロキシを使用]** トグルボタンを使用して、各デバイスのプロキシ設定を個別に有効化/無効化できます。デバイスで **[プロキシを使用]** が有効になっている場合、デバイスへの接続にプロキシ設定が使用されます。

プロキシ設定は、**[プロキシ設定]** ページで構成できます。

プロキシ設定を構成するには、次の手順を実行します。

1. 右上隅の歯車アイコンの下にある **[プロキシ設定（Proxy Settings）]** をクリックします。
2. [プロキシホスト名（Proxy Hostname）] または [IP] を入力します
3. プロキシポート番号を入力します。
4. プロキシ設定で認証が必要な場合は、[認証（Authentication）] を切り替えてオンにするか、手順 7 に進みます。
5. ユーザ名を入力します。
6. パスワードを入力します。
7. [保存（Save）] をクリックします。

   プロキシ設定が保存されます。

（注）
1. 移行中の場合、プロキシ設定の変更はできません。
2. 次の操作中、**[プロキシを使用]** トグル ボタンをオンにします。
   - **[デバイス管理]** ページでデバイスを追加している間に有効にすることができます。
   - **IMM 移行の追加**手順で新しいソース UCS デバイス/Intersight アカウントを追加します。

バックアップ/復元

IMM 移行ツール、リリース 3.1.1 は、ツールからデータをバックアップし、ツールの同じインスタンスまたは別のインスタンスに復元する機能を備えています。

バックアップコンテンツを復元するには、次の手順を実行します。

1. 右上隅の歯車アイコンの下にある **[バックアップ/復元（Backup/Restore）]** をクリックします。
2. バックアップ データを暗号化するための秘密キーを入力します。
3. [Download] をクリックします。

   データは圧縮ファイルでダウンロードされ、ローカル システムに保存されます。
4. データを復元する必要がある場合は、ツールのインスタンスにログインします。
5. 右上隅の歯車アイコンの下にある **[バックアップ/復元（Backup/Restore）]** をクリックします。
6. **[復元（Restore）]** タブに移動します。
7. データのバックアップ時に使用したのと同じキーを入力します。
8. バックアップデータを含む、システムにダウンロードされたファイルを参照して選択します。
9. [復元（Restore）] をクリックします。

   ファイルに存在するデータが復元されます。

（注）
- データを復元すると、ツールの既存のデータがすべて削除され、圧縮ファイルに存在するデータに置き換えられます。
- データは、ツールの下位バージョンから上位バージョンにのみ復元でき、その逆はできません。
- 移行が進行中の場合は、バックアップ/復元アクションを開始できません。

証明書設定

IMM 移行ツール リリース 4.1.2 では、ツールへのセキュアな接続を認証できます。Web サーバーの認証局（CA）署名付き Secure Sockets Layer（SSL）証明書を作成してアップロードできるようになりました。この証明書をリセットまたは更新することもできます。

IMM移行ツール4.1.3以降では、信頼できる認証局（CA）証明書をアップロードして追加し、プロキシの背後にあるデバイスに接続するときにプロキシSSL証明書を信頼できます。

信頼できる証明書の追加

信頼できるCA証明書をアップロードするには、次の手順を実行します。

1. 右上隅の歯車アイコンの下にある**[証明書設定（Certificate Settings）]**をクリックします。
2. **[信頼済み（Trusted）]**タブに移動します。
3. [証明書の追加（Add Certificate）]をクリックします。
4. **[参照（Browse）]**をクリックします。
5. 追加するCA証明書を選択します
6. [保存（Save）]をクリックします。

信頼できる証明書が追加されます。

SSL証明書の追加

CA署名付きSSL証明書を作成してアップロードするには、次の手順を実行します。

- 右上隅の歯車アイコンの下にある**[証明書設定（Certificate Settings）]**をクリックします。
- **[SSL]**タブに移動します。
- 以下のフィールドに入力して、証明書署名要求（CSR）を作成します。
  1. **組織（Organization）**：組織の名前を入力します。
  2. **組織単位（Organization Unit）**：証明書の組織単位の名前を入力します。
  3. **市区町村**：組織が所在する市区町村の名前を入力します。
  4. **都道府県**：組織が所在する都道府県の名前を入力します。
  5. **国（Country）**：組織がある国の名前を入力します。
  6. **電子メール アドレス**：組織に連絡する電子メールアドレスを入力します。
  7. **モジュール**：秘密キーと公開キーの両方について、ビット単位で表されるRSAキーの長さ。
  8. **[CSRの作成（Create CSR）]**をクリックします。
- **[CSRのダウンロード（Download CSR）]**をクリックして作成したCSRをダウンロードし、それを使用してCAから署名付きSSL証明書を取得します。
- 署名付き証明書を取得したら、**[証明書の適用（Apply Certificate）]**タブに移動します。
- 参照して、署名済みの証明書をアップロードします。

- **[証明書の適用**（Apply Certificate）] をクリックします。

証明書は IMM 移行ツールに適用されます。

（注） 証明書署名要求（CSR）を生成するには：

1. 仮想マシン（VM）に有効な完全修飾ドメイン名（FQDN）があることを確認します。
2. 次のコマンドを使用して FQDN を設定します。

```
sudo hostname --fqdn <fqdn>
```

3. <fqdn> を VM の目的の FQDN に置き換えます。

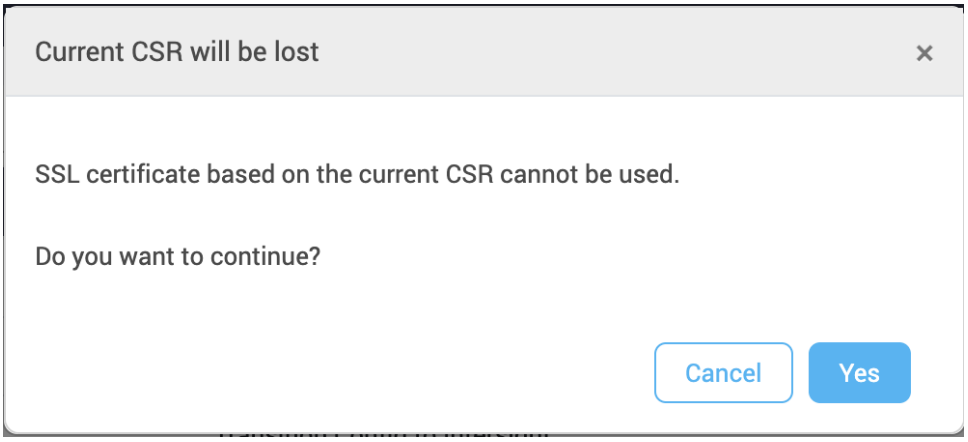
新しい CSR の作成

[新しい CSR（New CSR）] オプションを使用して、現在の CSR の詳細を再生成できます。この場合、既存の CSR または現在の CSR は失われ、新しい SSL 証明書をアップロードする必要があります。

新しい CSR を作成するには、次の手順を実行します。

1. 右上隅の歯車アイコンの下にある **[証明書設定（Certificate Settings）]** をクリックします。
2. **[SSL]** タブに移動します。
3. **「証明書の作成とアップロード」** セクションの説明に従って、詳細を入力します。
4. **[新しい CSR （New CSR）]** をクリックします。

   次に示すような確認ウィンドウが表示され、既存の SSL 証明書を使用できないことを示すメッセージが表示されます。



5. **[はい（Yes）]** をクリックして続行します。

   新しい CSR が作成されます。

SSL 証明書の更新

SSL 証明書をリセットまたは更新するには、次の手順を実行します。

1. 右上隅の歯車アイコンの下にある **[証明書設定（Certificate Settings）]** をクリックします。
2. 「証明書の作成とアップロード」セクションに記載されている手順を使用して CSR を作成します。
3. 証明書は、認証局（CA）によって署名されている必要があります。

（注） 自己署名証明書を更新する場合は、「付録 A：CLI を使用した管理操作」に記載されている CLI コマンドに従います。

4. CA 署名付き証明書を取得したら、**[証明書の適用（Apply Certificate）]** タブに移動します。
5. 参照して、署名済みの証明書をアップロードします。
6. **[証明書の適用（Apply Certificate）]** をクリックします。

第 11 章

変換の前提条件

• UCS Manager/Central 構成の変換 （65 ページ）

UCS Manager/Central 構成の変換

IMM移行ツールでUCSデバイスを追加し、**[次へ（Next）]**をクリックすると、ユーティリティがバックエンドで実行され、ハードウェア インベントリと構成を検証して、デバイスが IMM と互換性があるかどうかを確認します。

デバイスに接続し、既存の論理属性を複製します。これらには、プロファイル、ポリシー、プール、およびテンプレートが含まれます。

[Intersight へのプッシュ（Push to Intersight）] タスクが正常に完了すると、Intersight アプリケーションは変換されたオブジェクトを更新時に反映します。

換算の前提

IMM 移行ツールでの変換プロセスの前提条件は次のとおりです。

1. **イーサネット ネットワーク制御ポリシー**：Intersight のイーサネット ネットワーク制御ポリシーは、UCS Manager/Central の 2 つの異なる情報ソースを使用して作成できます。
   - サーバー vNIC：UCS Manager/Central のネットワーク制御ポリシーへのマッピング
   - アプライアンス ポート：UCS Manager のアプライアンス ネットワーク制御ポリシーへのマッピング

   UCS Manager/Central のネットワーク制御ポリシーを使用して Intersight のイーサネット ネットワーク制御ポリシーを作成する場合、Intersight のイーサネット ネットワーク制御ポリシーの名前は UCS Manager/Central のネットワーク制御ポリシーと同じになります。

   UCS Manager のアプライアンス ネットワーク制御ポリシーを使用して Intersight のイーサネット ネットワーク制御ポリシーを作成しているときに、Intersight のイーサネット ネットワーク制御ポリシーの名前は、UCS Manager のネットワーク制御ポリシーの名前に [_appliance] というサフィックスが付けられます。

2. **イーサネット ネットワーク グループ ポリシー**：UCS Manager/Central には、同等のイーサネット ネットワーク グループ ポリシーはありません。イーサネット ネットワーク グループ ポリシーの詳細は、VLAN グループから取得できます。各 VLAN グループには VLAN の詳細があり、それらの詳細はイーサネット ネットワーク グループ ポリシーの作成に使用されます。イーサネット ネットワーク グループ ポリシーの名前は、VLAN グループの名前と同じになります。

3. **イーサネット QoS ポリシー**：UCS Manager/Central の QoS ポリシーは、Intersight でイーサネットと FC QoS ポリシーに分割されます。

4. **ファイバ チャネル ネットワーク ポリシー**：UCS Manager/Central には同等のファイバ チャネル ネットワーク ポリシーはありません。ファイバー チャネル ネットワーク ポリシーの詳細は、サーバー プロファイル（Intersight）の作成中に取得できます。ファイバー チャネル ネットワーク ポリシーの名前は、SAN 接続ポリシーと vHBA の名前に由来します。

5. **ファイバ チャネル QoS ポリシー**：UCS Manager/Central の QoS ポリシーは、Intersight でイーサネットと FC QoS ポリシーに分割されます。

6. **IMC アクセス ポリシー**：インバンド ネットワーク設定の IPv4 および IPv6 アドレスの異なる IP プールを持つ UCS Manager/Central のサービスプロファイルの IMC アクセスポリシーの作成は、現在サポートされていません。UCS Manager/Central には、同等の IMC アクセスポリシーはありません。IMC ポリシーの詳細は、サービスプロファイルから取得できます。各サービスプロファイルには、インバンドネットワーク、IPv4 および IPv6 プールがあります。この情報を使用して、IMC アクセスポリシーが作成されます。

   - IMC アクセスポリシーの名前は、インバンド ネットワーク VLAN およびインバンド プールの名前を使用して派生します。名前は、最大 64 文字まで指定できます。
   - UCS Manager/Central では、サービスプロファイルで IPv4 プールと IPv6 プールを選択するための個別のオプションがありますが、Intersight では、IMC アクセスポリシーで IP プールを選択するオプションは 1 つだけです。Intersight で IMC アクセスポリシーを作成する前に、UCS Manager/Central の IPv4 および IPv6 プールを単一のプールにマージすることをお勧めします。しかし、これは実装が複雑です。変換中に、2 つの異なる IP プールに属するインバンド IPv4 および IPv6 アドレスを持つサービスプロファイルがある場合、IPv4 固有のプールのみが IMC アクセスポリシーの作成に考慮されます。

7. **IPMI オーバー LAN ポリシー**：Intersight の IPMI オーバー LAN ポリシーは、UCS Manager/Central の IPMI アクセスプロファイルにマッピングされます。IPMI アクセスプロファイルの IPMI ユーザー関連情報は、Intersight のローカル ユーザー ポリシーに移動されます。

8. **iSCSI ブート ポリシー**：UCS Manager/Central に相当する iSCSI ブート ポリシーはありません。 iSCSI ブート ポリシーの詳細は、サービス プロファイルから取得できます。各サービスプロファイルには、独自の iSCSI vNIC セクションがあります。iSCSI vNIC の詳細は、サービスプロファイルの iSCSI ブート パラメータ セクション内にあります。この情報を使用して、iSCSI ブート ポリシーが作成されます。

- iSCSI ブート ポリシーの名前は、サービスプロファイルと iSCSI vNIC の名前を使用して派生します。
- UCS Manager/Central には、iSCSI vNIC ノードおよび個々の iSCSI vNIC の IQN プール/イニシエータ名を提供するオプションがあります。Intersight には、個々の iSCSI vNIC 用のそのようなオプションはありません。Intersight の場合、IQN は LCP レベルにあります（vNIC にはありません）。
- 通常、UCS Manager/Central には、vNIC 用に 2 つの iSCSI ブート ターゲットを作成するオプションがあり、各ターゲットには独自の CHAP 詳細があります。ただし、Intersight には、iSCSI ターゲットの CHAP 詳細を提供するオプションが 1 つしかありません。
- CHAP 認証では、ポリシーの作成中にデフォルト パスワードが考慮されます。

9. **iSCSI 静的ターゲット ポリシー**：UCS Manager/Central に同等の iSCSI 静的ターゲット ポリシーはありません。 iSCSI 静的ターゲット ポリシーの詳細は、サービス プロファイルから取得できます。各サービスプロファイルには、独自の iSCSI ブート パラメータ セクションがあります。これらの iSCSI ブート パラメータを使用して、Intersight で iSCSI 静的ターゲット ポリシーが作成されます。単一の iSCSI インターフェイスの場合、優先順位に基づいて複数のターゲットが存在する可能性があります。したがって、iSCSI ターゲット名は、サービスプロファイル名、iSCSI インターフェイス名、および iSCSI ターゲットの優先度の組み合わせとして設計されます。
10. **LAN 接続ポリシー**：UCS Manager/Central では、vNIC を複数の方法で設定できます。
    1. インライン vNIC
        - スタンドアロン vNIC の使用
        - vNIC テンプレートの使用
    2. LAN 接続ポリシー
        - スタンドアロン vNIC の使用
        - vNIC テンプレートの使用

    UCS Manager/Central では、LAN / SAN 接続ポリシー、または vNIC / vHBA テンプレートを使用するかどうかにかかわらず、インライン vNIC / vHBA のいずれかにすることができます。接続を構成する唯一の方法であるため、考えられるすべての組み合わせが考慮され、それに応じて Intersight の LAN / SAN 接続ポリシーに変換されます。
11. **電源ポリシー**：UCS Manager では、グローバル ポリシーの電源ポリシー セクションが、Intersight のシャーシ プロファイルで使用され電源ポリシーとして変換されます。
12. **SD カード ポリシー**：UCS Manager/Central に相当する SD カード ポリシーはありません。このポリシーは、UCS Manager/Central のローカル ディスク構成ポリシーから情報を読み取ることで作成できます。UCS Manager/Central のローカル ディスク構成ポリシーで構成された Flexflash がある場合、同等の SD カード ポリシーが Intersight で作成されます。

13. **[ストレージ ポリシー（Storage Policy）]**：

    - ストレージ プロファイルのローカル LUN での自動展開

      すべての仮想ドライブは、デフォルトで [自動展開（Auto Deploy）] です。オプションが [no-auto-deploy] に設定されている場合、サービスプロファイルでマップされた VD とストレージ ポリシー VD は同じ名前にする必要があります。名前が異なる場合は、無効な構成です。

    - UCS Manager/Central の LUN セットは、Intersight のシングル ドライブ RAID 構成に相当します。

      - LUNセット内のすべてのディスク スロットを単一の番号のアレイにマージします。
      - すべてのドライブの VD 構成は同一である必要があります。各 LUN セットに異なる VD 構成がある場合は、無効な構成としてフラグを立てます。

    - M.2 ドライブの構成
    - UCS Manager/Central で **[未指定（Unspecified）]** に設定されている LUN サイズは、ExpandToAvail フラグが True に設定されている仮想ドライブに対してのみ使用する必要があります。フラグが False に設定されている場合、それは無効な構成です。
    - 特定のストレージ プロファイルと汎用ストレージ プロファイルを持つ UCS Manager/Central のサービスプロファイルをマージして、Intersight で単一のストレージ プロファイルを形成します。

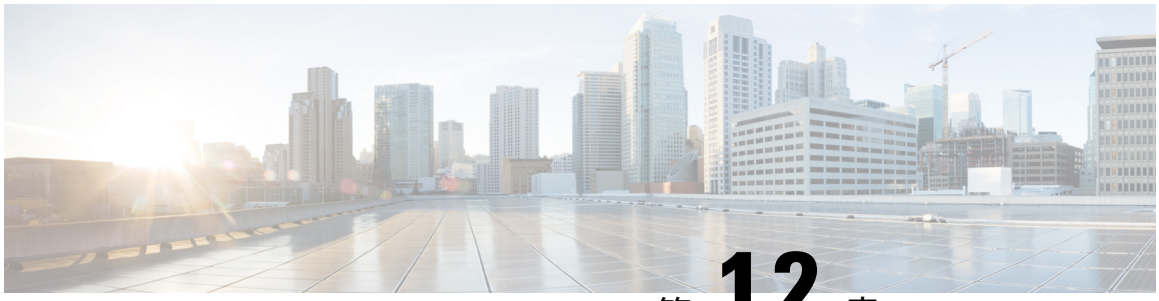
14. **[VLAN ポリシー（VLAN Policy）]**：

    Intersight の VLAN ポリシーは、UCS Manager の VLAN セクションにマップされます。UCS Manager では、VLAN の作成中にファブリック ID（A または B、または両方）を選択するオプションがありますが、Intersight では同じ状態ではありません。変換の一環として、ファブリック ID の値が VLAN ポリシーの名前にサフィックスとしてファブリック ID を付加することによって **[A]** または **[B]** に設定されている場合、2 つの異なる VLAN ポリシーが作成されます。ファブリック ID 値が **[両方（Both）]** に設定されている場合、単一の VLAN ポリシーが作成されます。共有タイプをプライマリ/分離/コミュニティとして選択して、プライベート VLAN を作成することもできます。プライマリ VLAN は必須オプションです。指定しない場合、プライベート VLAN の構成はスキップされます。したがって、**デフォルト**のマルチキャスト ポリシーで割り当てられた通常の VLAN に変換します。

15. **[VSAN ポリシー（VSAN Policy）]**：

    Intersight の VSAN ポリシーは、UCS Manager の VSAN セクションにマッピングされます。UCS Manager では、VSAN の作成中にファブリック ID（A または B、または両方）を選択するオプションがありますが、Intersight では同じ状態ではありません。変換の一環として、ファブリック ID の値が VSAN ポリシーの名前にサフィックスとしてファブリック ID を付加することによって **[A]** または **[B]** に設定されている場合、2 つの異なる

VSAN ポリシーが作成されます。ファブリック ID 値が **[両方（Both）]** に設定されている場合、単一の VSAN ポリシーが作成されます。



第 12 章

サポートされる機能

- 変換でサポートされる機能 （71 ページ）
- サポート対象のクローン機能 （77 ページ）

変換でサポートされる機能

A. [UCS から IMM への変換でサポートされる機能（Supported Features for Conversion from UCS to IMM）]

このセクションでは、IMM 移行ツールでの変換がサポートされている機能のリストと、Cisco UCS Manager/Central と Intersight 間のポリシーマッピングを示します。

（注） UCS Central 設定に VLAN/VSAN エイリアシングが含まれている場合、IMM 移行ツールは vNIC/vHBA の変換を実行するときに、エイリアスの 1 つを自動的に選択します。結果の構成を慎重に見直して、適切であることを確認してください。

表 *2*：（*I*）*UCS* と *Intersight* 機能間の変換マッピング

UCS Manager/ UCS Central 機能カテゴリ	ソース UCS Manager/UCS Central の機能名	同等の IMM ポリシー
Admin	通信サービス*3	SNMP ポリシー
	構成	Intersight の組織
	Syslog *4	Syslog ポリシー
	タイムゾーン管理	NTPポリシー
	MACアドレステーブルエージング	スイッチ制御ポリシー
	VLAN ポート数の最適化	スイッチ制御ポリシー
	予約済み VLAN 範囲 *11	スイッチ制御ポリシー
	インバンドプロファイル VLAN グループ	イーサネット ネットワーク グループ ポリシー
	インバンド プロファイル ネットワーク	IMC アクセスポリシー
	インバンド プロファイル IP プール名	IMC アクセスポリシー
	FC アップリンク トランキング	VSAN ポリシー
	DNS *5	ネットワーク接続ポリシー

UCS Manager/ UCS Central 機能カテゴリ	ソース UCS Manager/UCS Central の機能名	同等の IMM ポリシー
サーバー ポリシーとシャーシ ポリシー	BIOS ポリシー	BIOS ポリシー
	起動ポリシー	ブート ポリシー iSCSI スタティック ターゲット ポリシー
	ディスクグループポリシー	ストレージ ポリシー
	IPMI アクセス プロファイル	IPMI over LAN ポリシー
	iSCSI アダプタ ポリシー	iSCSI アダプタ ポリシー
	iSCSI ブート ポリシー	iSCSI ブート ポリシー
	KVM 管理ポリシー	仮想 KVM ポリシー
	ローカル ディスク構成ポリシー *6	ストレージポリシー、SD カードポリシー
	QoS ポリシー	イーサネット QoS ポリシー / FC QoS ポリシー
	Serial over LAN ポリシー	Serial over LAN ポリシー
	サービス プロファイル	サーバプロファイル
	サービス プロファイル テンプレート *7	サーバ プロファイル テンプレート
	保管プロファイル（Storage Profiles）	ストレージ ポリシー
	ストレージ プロファイル - セキュリティ ポリシー *11	ドライブ セキュリティ
	vMedia ポリシー	仮想メディア ポリシー
	vNIC/vHBA 配置ポリシー *8	LAN 接続ポリシー / SAN 接続ポリシー
	イーサネット アダプタ ポリシー	イーサネット アダプタ ポリシー
	フロー制御ポリシー	フロー制御ポリシー
	LACP ポリシー	リンク集約ポリシー
	LAN 接続ポリシー	LAN 接続ポリシー
	リンク プロトコル ポリシー	スイッチ制御ポリシー
	マルチキャスト ポリシー	マルチキャストポリシー
	ネットワーク制御ポリシー	イーサネット ネットワーク制御ポリシー
	ファイバ チャネル アダプタ ポリシー	ファイバ チャネル アダプタ ポリシー

UCS Manager/ UCS Central 機能カテゴリ	ソース UCS Manager/UCS Central の機能名	同等の IMM ポリシー
	SAN 接続ポリシー	SAN 接続ポリシー
	ストレージ接続ポリシー	FC ゾーン分割ポリシー
プール	IP プール	IPプール
	IQN サフィックス プール	IQNプール
	MAC プール	MAC プール
	WWNN プール	WWNN プール
	WWPN プール	WWPN プール
	サーバー プール *9	リソースプール

次の表に、IMM 移行ツールでの変換がサポートされている UCS Manager 機能を示します。

表 *3*：（*II*）*UCS Manager* と *Intersight* 機能間の変換マッピング

UCS Manager 機能カテゴリ	ソース UCS Manager の機能名	同等の IMM ポリシー
ファブリック構成 *1	アプライアンス VLAN	VLAN ポリシー
	QoS システム クラス	システム QoS ポリシー
	VLAN グループ	イーサネット ネットワーク グループ ポリシー
	VLANs	VLAN ポリシー
	VSAN	VSAN ポリシー
	ストレージ VSAN *9	VSAN ポリシー
	LAN/SAN ピン グループ *10	LAN/SAN ピン グループ
ファブリック ポリシー *2	アプライアンス ネットワーク制御ポリシー	イーサネット ネットワーク制御ポリシー
	UDLD リンク ポリシー	リンク制御ポリシー

UCS Manager機能カテゴリ	ソース UCS Manager の機能名	同等の IMM ポリシー
ポートロール	アプライアンス ポート	ポート ポリシー
	アプライアンス ポートチャネル	ポート ポリシー
	FCoE アップリンク ポート	ポート ポリシー
	FCoE アップリンク ポートチャネル	ポート ポリシー
	LAN アップリンクポート	ポート ポリシー
	LAN アップリンク ポートチャネル	ポート ポリシー
	SAN ユニファイドポート	ポート ポリシー
	SAN アップリンクポート	ポート ポリシー
	SAN アップリンク ポートチャネル	ポート ポリシー
	サーバ ポート	ポート ポリシー
	FC ストレージ ポート *9	ポート ポリシー
	SANストレージポート *9	ポート ポリシー
	ブレークアウト ポート *10	ポート ポリシー

*1：通常の VLAN と統合

*2：通常のネットワーク制御ポリシーと統合

*3：セッション / HTTP 設定は、Intersight 設定で定義されます。Telnet / SSH 設定はサポートされていません

*4：最大 2 つのリモート宛先サーバーのみをサポート

*5：UCS Manager では、[管理] > [通信管理] > [DNS 管理] の下にあります。

*6：ストレージポリシーに置き換わります。ローカルディスク構成ポリシーは、自動ポリシーオプションではなく手動作成のみをサポートします。

*7：テンプレートの更新のみ：初期テンプレートのサポートはありません（ただし、複製は可能です）

*8：配置は、次のマッピングで PCIe スロットに静的にマッピングされます。

- vCon 1：スロット MLOM
- vCon 2：スロット PCIe1
- vCon 3：スロット PCIe2
- vCon 4：スロット PCIe3

このマッピングは静的ですが、移行設定で調節可能です。詳細については、「デフォルト設定」の B. 変換の移行設定セクションを参照してください。

*9：IMM 移行ツール、リリース 1.0.2 以降でサポートされています。

*10：IMM 移行ツール、リリース 3.0.1 以降でサポートされています。

（注） エイリアスされた VLAN/VSAN のエイリアスを含むテーブルは、変換がサポートされていません。

*11：IMM 移行ツール、リリース 4.0.1 以降でサポートされています。

B.[変換のためのファブリック インターコネクト（FI）マッピング（Fabric Interconnect (FI) Mapping for Conversion）]

ポート ポリシーが UCSM から IMM に変換されると、そのポリシーのポート構成は、次に示すように、サポートされていない FI（Cisco UCS 6200 および 6300 シリーズ）をマッピングすることによって調整されます。

表 *4:* ポート ポリシー変換のための *UCSM FI* と *IMM FI* 間のマッピング

UCSM FI	同等の IMM FI
Cisco UCS-FI-6248UP	Cisco UCS-FI-6454
Cisco UCS-FI-6296UP	Cisco UCS-FI-6454
Cisco UCS-FI-6296	Cisco UCS-FI-64108
UCS-FI-M-6324	Cisco UCS-FI-6454
Cisco UCS-FI-6332	Cisco UCS-FI-6536
Cisco UCS-FI-6332-16UP	Cisco UCS-FI-6536
Cisco UCS-FI-6454	Cisco UCS-FI-6454
Cisco UCS-FI-64108	Cisco UCS-FI-64108
Cisco UCS-FI-6536	Cisco UCS-FI-6536

（注）

- ユニファイドポートのハードウェア特性が異なるため、Cisco UCS 6200 シリーズまたは Cisco UCS 6300 シリーズ FI から IMM に変換する場合、既存のユニファイドポートおよび SAN ポートの構成は無視されます。
- Cisco UCS-FI-6332-16UP から Cisco UCS 6536 への移行では、すべての SFP+ ポート構成が無視され、すべての QSFP+ ポート構成が 16 ポート左にシフトされます（Cisco UCS-FI-6332-16UP のポート 1/17 は Cisco UCS-FI-6536 のポート 1/1 になります）。

サポート対象のクローン機能

[Intersight アカウントのクローニングでサポートされる機能（Supported Features for Cloning an Intersight account）]

このセクションでは、UCSサーバー、シャーシ、およびドメインポリシーのリストと、Intersight アカウントのクローン作成でサポートされるプロファイル、プール、リソース、設定、およびテンプレートのリストを提供します。

（注）

- Intersight アカウントのクローニングは、スタンドアロン モードおよび Intersight 管理モードの構成でのみサポートされます。
- 送信元 Intersight アカウントで要求されたターゲット デバイスは、クローニング時に接続先 Intersight アカウントに移動されません。

表 *5 : Intersight* アカウントのクローニングでサポートされる機能

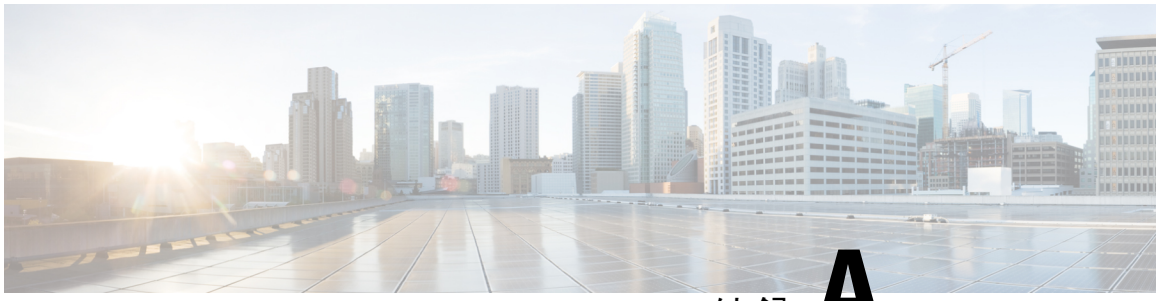
機能カテゴリ	サポートされる機能
UCS サーバ ポリシー	アダプタの設定
	BIOS
	ブート順序
	証明書の管理
	デバイス コネクタ
	ドライブ セキュリティ *2
	イーサネットアダプタ
	イーサネット ネットワーク
	イーサネットネットワーク制御
	イーサネット ネットワーク グループ
	イーサネットQoS
	[FC Zoning]
	ファイバチャネルアダプタ
	ファイバチャネルネットワーク
	ファイバチャネルQoS
	ファームウェア *2
	IMCアクセス
	IPMI over LAN
	iSCSI アダプタ
	iSCSI ブート
	iSCSI 静的ターゲット
	LAN の接続
	LDAP
	ローカルユーザー
	ネットワーク接続
	NTP
	永続的なメモリ
	電力
	SAN接続

機能カテゴリ	サポートされる機能
	SDカード
	Serial over LAN
	SMTP
	SNMP
	SSH
	ストレージ
	Syslog
	仮想 KVM
	仮想メディア
UCS ドメイン ポリシー	フロー制御
	リンクアグリゲーション
	リンク制御
	マルチキャスト
	ポート
	スイッチ制御
	システムQoS
	VLAN
	VSAN
	SNMP
UCS シャーシ ポリシー	サーマル
	SNMP
プール	IP
	IQN
	MAC
	技術情報
	UUID
	WWNN
	WWPN

機能カテゴリ	サポートされる機能
プロファイル	UCSサーバプロファイル
	UCSシャーシプロファイル
	UCSドメインプロファイル
テンプレート	UCSサーバー プロファイル テンプレート
アクセスと権限設定	ユーザー *1
	グループ *1
	ロール *1
	構成
	リソース グループ

- *1：[Intersight 設定のトリミング（Trim Intersight Settings）] オプションが設定されていない場合にのみクローニングされます。デフォルトでは、オブジェクトはクローニングされません。
- *2：IMM 移行ツール、リリース 4.0.1 以降でサポートされています。

（注）
- 証明書管理ポリシーを持つ Intersight アカウントをクローニングしているときに、自己署名証明書が生成され、Intersight にプッシュされます。
- パスワードを含むポリシーは、自動生成されたパスワードを使用してクローニングされます。



付録 A

付録

- 付録 A : CLI を使用した管理オペレーション （81 ページ）
- 付録 B：ログのダウンロード/技術サポート （82 ページ）
- 付録 C：フィードバックの提供 （83 ページ）

付録 A : CLI を使用した管理オペレーション

(I) [/etc/hosts ファイルの編集（Edit the /etc/hosts File）]

`sudo hosts` コマンドを使用して、`/etc/hosts` ファイルを編集できます。

```
hosts [options...] -- Command to update the hosts file
options:
    add :adds the host to host file
    remove :remove the host from the host file
    list :lists the host in the host file
example:
    add:     $ sudo hosts add 1.2.3.4 localhost
    remove:  $ sudo hosts remove 1.2.3.4 localhost
    list:    $ sudo hosts (or) sudo hosts list
```

(II) [IMM 移行ツール VM の IP アドレスを変更する（Change the IP Address of the IMM Transition Tool VM）]

IMM 移行ツール VM の IP アドレスを変更するには、次の手順を実行します。

1. VM に SSH 接続します。
2. 以下のコマンドを使用して、`/etc/netplan/00-installer-config.yaml` ファイルを編集します。

   ```
   $ sudoedit /etc/netplan/00-installer-config.yaml
   ```

3. 必要に応じて、IP、ネットマスク、ゲートウェイ、およびDNSフィールドを変更します。
4. 以下の文書を使用して、netplan 構成を編集します。https://netplan.readthedocs.io/en/latest/examples/
5. ファイルを保存します。

6. 次のコマンドを使用して VM を再起動します。

```
sudo reboot
```

(III) [IMM 移行ツール VM の NTP を変更する（Change the NTP of the IMM Transition Tool VM）]

以下の手順を実行して、IMM 移行ツール VM の NTP を変更します。

1. VM に SSH 接続します。
2. 以下のコマンドを使用して、`/etc/systemd/timesyncd.conf` ファイルを編集します。

```
$ sudoedit /etc/systemd/timesyncd.conf
```

3. コメントを解除し、'NTP=' フィールドの値のコメントを削除します。
4. ファイルを保存します。
5. 次のコマンドを使用して VM を再起動します。

```
sudo reboot
```

(IV) admin パスワードを変更します

admin のパスワードを変更するには、次の手順に従います。

1. VM に SSH 接続します。
2. 次のコマンドを実行します。

```
sudo passwd admin
```

3. 新しいパスワードを入力します。

付録 B：ログのダウンロード/技術サポート

サポートが必要な場合は、ログファイルをテクニカル チームと共有できます。

クエリを送信するには、次の手順を実行します。

1. すべての遷移レコードを表示するリスト ビューに移動します。
2. テクニカル サポートが必要な移行レコードまでスクロールします。
3. レコードに対して [...] をクリックします。
4. [ログのダウンロード（Download Logs）] をクリックします。
5. ログファイルをコンピュータに保存します。
6. 保存したログファイルを電子メールに添付し、クエリ / フィードバックを含む電子メールを imm-transition-feedback@cisco.com グループに送信します。
   mailto:imm-transition-feedback@cisco.com

付録 C：フィードバックの提供

右上隅にある **[フィードバック（Feedback）]** を使用して、ツールに関するフィードバックを提供するか、不足している機能に関する情報を提供します。

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。