



## **Cisco Intersight 管理モード移行ツール ユーザー ガイド、2.0**

初版：2022年4月29日

最終更新：2022年5月31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/](http://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](http://www.cisco.com/go/offices).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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)

© 2022 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、[Cisco Services](#) 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ル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インターフェイ

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

- [新機能および変更された機能に関する情報 \(1 ページ\)](#)

## 新機能および変更された機能に関する情報

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 2.0 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 ツール、リリース 2.0.1 の新機能と変更された動作

特長	説明	参照先
UCS Central のサポート	Cisco Intersight 管理モード (IMM) 移行ツールリリース 2.0.1 には、サービスプロファイル テンプレートを UCS Central から Intersight に移行する機能が導入されています。	<a href="#">概要</a>
サービスプロファイル/テンプレート ベースの変換	IMM 移行ツールリリース 2.0.1 は、選択したテンプレートに添付されているポリシーのみを変換します。	<a href="#">Cisco Intersight 管理モードツールの作業</a>
サービスプロファイルテンプレートの選択的変換	IMM 移行ツールリリース 2.0.1 では、サービスプロファイルテンプレートを選択的に Intersight に変換できます。	<a href="#">Cisco Intersight 管理モードツールの作業</a>
移行のクローニング	IMM 移行ツールリリース 2.0.1 を使用すると、既存の移行を複製し、複製された構成を編集し、準備状況レポートを生成できます。	<a href="#">Cisco Intersight 管理モードツールの作業</a>

特長	説明	参照先
移行設定	IMM 移行ツールリリース 2.0.1 では、変換オプションを設定して、遷移の動作を制御できます。	<a href="#">付録 B : 移行設定</a>



## 第 2 章

### 概要

---

- [概要 \(3 ページ\)](#)

### 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 移行ツールは、次の機能を提供します。

- 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。
- 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。
- 構成のどの部分が Intersight で使用できるかを検証する機能。
- 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 インスタンスからサービス プロファイル テンプレートと、可能な限りテンプレートに関連するすべてのポリシーを変換します。



---

(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。

---

- 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。



---

(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。

---





## 第 3 章

# Cisco Intersight 管理モード移行ツールのスタートアップガイド

- [前提条件 \(5 ページ\)](#)
- [Cisco Intersight マネージドモード移行ツールのインストール \(6 ページ\)](#)
- [グラフィカルユーザーインターフェイスを使用した Cisco Intersight 管理モード移行ツールへのアクセス \(13 ページ\)](#)

## 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 : 2 つの vCPU、8 GB RAM、100 GB ストレージ。
- 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。

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

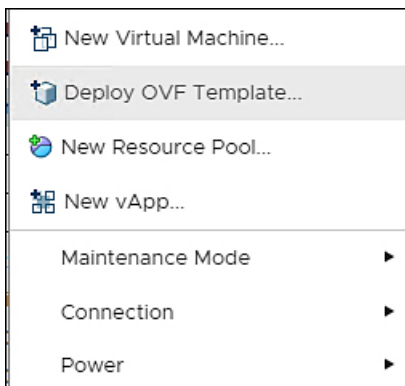
Open Virtual Appliance (OVA) は、1つ以上の仮想マシン (VM) から構成されるビルド済みのソフトウェアソリューションであり、1つのユニットとしてパッケージ、保守、更新、および管理されます。Cisco Intersight 管理モード移行ツール OVA には、オペレーティングシステムがプレインストールされており、IMM 移行ツールの機能に必要なアプリケーション機能が含まれています。OVA としての IMM 移行ツールは、VMware vSphere インフラストラクチャに展開できます。

### 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。

**ステップ 1** HTML5 vSphere Web Client にログインし、**[VM]** タブに移動します。

**ステップ 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。



**ステップ 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。

## Deploy OVF Template

- Select an OVF template**
- Select a name and folder
- Select a compute resource
- Review details
- Select storage
- Ready to complete

**Select an OVF template**  
Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

Local file

IMM-Migration.ova

- ステップ 4** [ファイルの選択 (Choose Files) ] ボタンをクリックし、ダウンロードした OVA ファイルを選択します。
- ステップ 5** [次へ (Next) ] をクリックします。
- ステップ 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。
- ステップ 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。

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- 3 Select a compute resource**
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a compute resource  
Select the destination compute resource for this operation

▼ Server [redacted]

- > [redacted]
- > [redacted]
- > [redacted]
- > [redacted]
- > [redacted]
- > [redacted]
- > [redacted]
- > [redacted]
- > [redacted]

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

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。

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

**Review details**  
Verify the template details.

Publisher	No certificate present
Download size	2.1 GB
Size on disk	5.2 GB (thin provisioned)
	100.0 GB (thick provisioned)

[CANCEL](#) [BACK](#) [NEXT](#)

**ステップ 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。

**ステップ 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。

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 Select storage**
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

**Select storage**  
Select the datastore in which to store the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed ▾

VM Storage Policy: Datastore Default ▾

Name	Capacity	Provisioned	Free	Type
[REDACTED]	92.5 GB	973 MB	91.55 GB	VM
[REDACTED]	1.5 TB	1 TB	509.62 GB	VM
[REDACTED]	1.5 TB	1.28 TB	264.34 GB	VM

Compatibility

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

**ステップ 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。

### Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**
- 7 Customize template
- 8 Ready to complete

**Select networks**  
Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

1 items

**IP Allocation Settings**

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL
BACK
NEXT

**ステップ 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)] と [変換されたポリシーのデフォルトパスワード (Default Password For Converted Policy)] と [相互 CHAP 認証のパスワード (Password For Mutual CHAP Authentication)] を設定して、テンプレートをカスタマイズします。

[変換済ポリシーのデフォルトパスワード (Default Password For Converted Policy)] は、変換された仮想メディア、iSCSI ブートなどの UCS Manager ポリシーの既存のパスワードの代わりに使用されます。12 ~ 16 文字で、スペース、タブ、改行を除いた特殊文字を含める必要があります。相互 CHAP 認証のパスワードは、iSCSI ブートポリシーの相互 CHAP 認証に使用されます。これは、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。12 ~ 16 文字で、スペース、タブ、改行を除いた特殊文字を含める必要があります。

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- 7 Customize template**
- 8 Ready to complete

### Customize template

Customize the deployment properties of this software solution.

✓ All properties have valid values ✕

Network		6 settings
Public Network Type		STATIC ▾
Public Network IP		<input type="text"/>
Public Network Netmask		<input type="text"/>
Public Network Gateway		<input type="text"/>
DNS		Enter a valid DNS IP for Static network and enter a random IP for DHCP. The DNS field value is only considered if the Network Type is Static. <input type="text"/>
NTP		<input type="text"/>
Root Credential		2 settings

CANCEL BACK NEXT



Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Customize template**
- 8 Ready to complete

Root Credential 3 settings

System Password Please provide the password for the admin user. Use the same to login to the tool.

Password  ⓘ

Confirm Password

Default Password For Converted Policy This password is used as a replacement for any existing password in UCS Manager/Central policies such as Virtual Media, iSCSI Boot that are converted.

Password Standard - Enter between 12 and 16 characters, including special characters except for spaces, tabs, line breaks.

Password  ⓘ

Confirm Password

Password For Mutual CHAP Authentication This password is used for Mutual CHAP Authentication in iSCSI Boot Policy. And it should be different from the "Default Password For Converted Policy". Password Standard - Enter between 12 and 16 characters, including special characters except for spaces, tabs, line breaks.

Password  ⓘ

Confirm Password

CANCEL BACK NEXT

ステップ 12 [次へ (Next)] をクリックします。

構成データを確認します。

ステップ 13 [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。

ステップ 14 VM を選択し、[Power On] をクリックします。

ステップ 15 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。

## グラフィカルユーザーインターフェイスを使用した Cisco Intersight 管理モード移行ツールへのアクセス

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。

ステップ 1 Web ブラウザ ウィンドウを起動します。

**ステップ 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。

**ステップ 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。

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。

**ステップ 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。



## 第 4 章

# Cisco Intersight 管理モード移行ツールの作業

- [Cisco Intersight 管理モード移行ツールの作業](#) (15 ページ)
- [移行準備レポートの説明](#) (19 ページ)
- [UCS Manager/Central 構成の変換](#) (21 ページ)

## Cisco Intersight 管理モード移行ツールの作業

### 変革

IMM の移行を開始するには、次の手順を実行します。

**ステップ 1** [IMM 移行の追加 (Add IMM Transition) ] をクリックします。

**ステップ 2** 移行の名前を入力します。

**ステップ 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、**[構成を Intersight に移行 (Transition Config to Intersight) ]** を選択します。

**ステップ 4** [次へ (Next) ] をクリックします。

**ステップ 5** 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、「[付録 C : プロキシ設定](#)」を参照してください。

**ステップ 6** ソース デバイス (UCS Manager または UCS Central) を選択します。

**ステップ 7** 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。該当のデバイスのデバイス IP / FQDN、ユーザー名とパスワードを入力します。

**ステップ 8** **[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。

**ステップ 9** **[次へ (Next)]** をクリックします。

**ステップ 10** 移行に必要な変換オプションを構成します。

各移行設定フィールドの詳細については、「[付録 B : 移行設定](#)」を参照してください。

**ステップ 11** **[次へ (Next)]** をクリックします。

**ステップ 12** 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。サービス プロファイル名にマウス ポインタを合わせると、サービス プロファイルまたはテンプレートの説明が表示されます。

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。

フィルタを適用して、検索バーの横にある**[表示 (Show)]** ドロップダウンリストに、サービスプロファイル テンプレートのみ、またはサービス プロファイルとテンプレートの両方を表示することができます。

**ステップ 13** **[次へ (Next)]** をクリックします。

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かなりの時間がかかる場合があります (1 時間以上)。

**ステップ 14** (注) 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。

[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。

**ステップ 15** 手順 3 で (b) を選択した場合は、[次へ (Next)] をクリックします。

**ステップ 16** Intersight アカウントのラジオボタンを選択します。有効なオプションは、Intersight SaaS または Intersight アプライアンス VM です。

**ステップ 17** 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 3 の API キー (API Key for OpenAPI Schema Version 3)] を選択します。

(注) OpenAPI スキーマバージョン 2 は、IMM 移行ツールではサポートされていません。

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。

**ステップ 18** 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。

**ステップ 19** (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。

[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。

**ステップ 20** [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。

## 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)、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。

---

**ステップ 1** **[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。

**ステップ 2** **[編集 (Edit)]** をクリックして、移行名を変更します。

**ステップ 3** **[削除 (Delete)]** をクリックし、移行を削除します。

**ステップ 4** **[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。

4(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。

4(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。

**ステップ 5** **[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。

---

## 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。各デバイスに一意的ターゲット 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。

---

**ステップ 1** **[デバイス管理 (Device Management)]** に移動します。

**ステップ 2** **[デバイスの追加 (Add Device)]** をクリックします。

**ステップ 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。

**ステップ 4** ターゲット IP/FQDN を入力します

**ステップ 5** ステップ 3 で選択したデバイス タイプが **UCS システム** 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。

**ステップ 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。

**ステップ 7** ステップ 3 で選択したデバイス タイプが **Intersight** の場合は、**API キー** を入力します。

**ステップ 8** **秘密キー** を入力します。

**ステップ 9** **[保存 (Save)]** をクリックします。

デバイスの詳細は、[デバイス管理] リスト ページに表示されます。

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。

## 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。

## UCS Manager/Central 構成の変換

IMM 移行ツールで UCS Manager/Central 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。

- **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。

- **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。

- **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。
- **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。
- **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。
- **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。
- **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。
- **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 認証の場合、ツールへの入力として CHAP パスワードを提供する必要があります。それ以外の場合は、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。
- **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。

- **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。

- **電源ポリシー** : UCS Manager では、Intersight の電源ポリシーとしては、グローバル ポリシーの電源ポリシー セクションが変換されます。
- **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。
- **ストレージ ポリシー** :
  - 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する必要があります。

#### • VLAN ポリシー :

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。

#### • VSAN ポリシー :

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。



## 付録 **A**

# 付録

---

- 付録 A : サポートされる IMM 機能 / ポリシー (25 ページ)
- 付録 B : 移行設定 (30 ページ)
- 付録 C : プロキシ設定 (33 ページ)
- 付録 D : サンプル使用例 (35 ページ)
- 付録 E : フィードバックの送信 (37 ページ)
- 付録 F : テクニカル サポート (38 ページ)

## 付録 A : サポートされる IMM 機能 / ポリシー

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。
-

<b>UCS Manager/UCS Central</b> 機能カテゴリー	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 *4	SNMP ポリシー
	構成	Intersight の組織
	Syslog *5	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
	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 トランッキング	VSAN ポリシー
	DNS *6	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 *7	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 *8	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
	vMedia ポリシー	仮想メディア ポリシー
	vNIC / vHBA 配置ポリシー *9	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
	SAN 接続ポリシー	SAN 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
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 *10	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。

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
	VLAN *2	VLAN ポリシー
	VSAN	VSAN ポリシー
	ストレージ VSAN *10	VSAN ポリシー
ファブリック ポリシー *3	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 ポートチャンネル	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 ポートチャンネル	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 ポートチャンネル	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 ポートチャンネル	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 *10	ポート ポリシー
	SAN ストレージポート *10	ポート ポリシー

\*1 : 通常の VLAN と統合

\*2 : PVLAN には対応していません。

\*3 : 通常のネットワーク制御ポリシーと統合

\*4 : 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

\*5 : 最大 2 つのリモート宛先サーバーのみをサポート

\*6 : UCS Manager では、[管理] > [通信管理] > [DNS 管理] の下にあります。

\*7 : ストレージ ポリシーに置き換わる

\*8 : 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)

\*9 : 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

この配置は、変換の実行後に必要に応じて手動で調整できます。

\*10 - IMM Transition Tool リリース 1.0.2 以降でサポート



(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。

## 付録 B : 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。

## 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 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、デフォルトで無効です。
- 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。UCS Central テンプレートはデフォルトで変換されません。

### 3. ルート組織名

これは、UCS ルート組織がマップされる Intersight 組織の名前です。

### 4. 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、Intersight 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」の名前は「Org2」になります。



(注) 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。

### 5. 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」。
- 無効にすると、すべての vNIC/vHBA が PCIe スロット「MLOM」にマップされます。

### 6. 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。

### 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\_transition\_version': "2.0.1」、  
「imm\_transition\_name': "transition\_name」でタグ付けされます。

### 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. 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。

#### 6. 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。

## 付録 C : プロキシ設定

IMM 移行ツールには、UCS デバイスおよび Intersight との接続を確立する際に、プロキシ設定を有効または無効にするオプションが用意されています。要件のシナリオに応じてプロキシ設定を変更できます。

### シナリオ 1 : UCS デバイス接続のみのプロキシ設定

[UCS の追加 (Add UCS)] ページで、UCS ドメインに接続するためだけにプロキシ設定を有効にする必要がある場合は、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 [設定 (Settings)] をクリックします。
2. [プロキシを有効にする (Enable Proxy)] を切り替えてオンにします。
3. [プロキシホスト名 (Proxy Hostname)] または [IP] を入力します
4. プロキシポート番号を入力します。
5. 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 8 に進みます。
6. ユーザ名を入力します。
7. パスワードを入力します。
8. [保存 (Save)] をクリックします。  
プロキシ設定が保存されます。
9. [Cisco Intersight マネージド モード移行ツールの操作](#)で説明されている手順に従って、準備状況レポートを生成します。
10. [設定 (Settings)] セクションに移動し、[プロキシを有効にする (Enable Proxy)] を切り替えてオフにします。
11. [Cisco Intersight マネージド モード移行ツールの操作](#)で説明されている手順に従って、変換されたオブジェクトを Intersight にプッシュします。

## シナリオ 2: Intersight 接続のみのプロキシ設定

[Intersight へのプッシュ (Push to Intersight)] ページで、Intersight に接続するためののみプロキシ設定を有効にする必要がある場合は、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 [設定 (Settings)] をクリックします。
2. [プロキシを有効にする (Enable Proxy)] を切り替えてオンにします。
3. [プロキシホスト名 (Proxy Hostname)] または [IP] を入力します
4. プロキシポート番号を入力します。
5. 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 8 に進みます。
6. ユーザ名を入力します。
7. パスワードを入力します。
8. [保存 (Save)] をクリックします。  
プロキシ設定が保存されます。
9. [次へ (Next)] をクリックします。
10. [Cisco Intersight マネージド モード移行ツールの操作](#)で説明されている手順に従って、変換されたオブジェクトを Intersight にプッシュします。
11. [設定 (Settings)] セクションに移動し、[プロキシを有効にする (Enable Proxy)] を切り替えてオフにします。

## シナリオ 3 : UCS デバイスおよび Intersight 接続のプロキシ設定

IMM 移行ツールにログインしたら、次の手順を実行してプロキシ設定を有効にします。

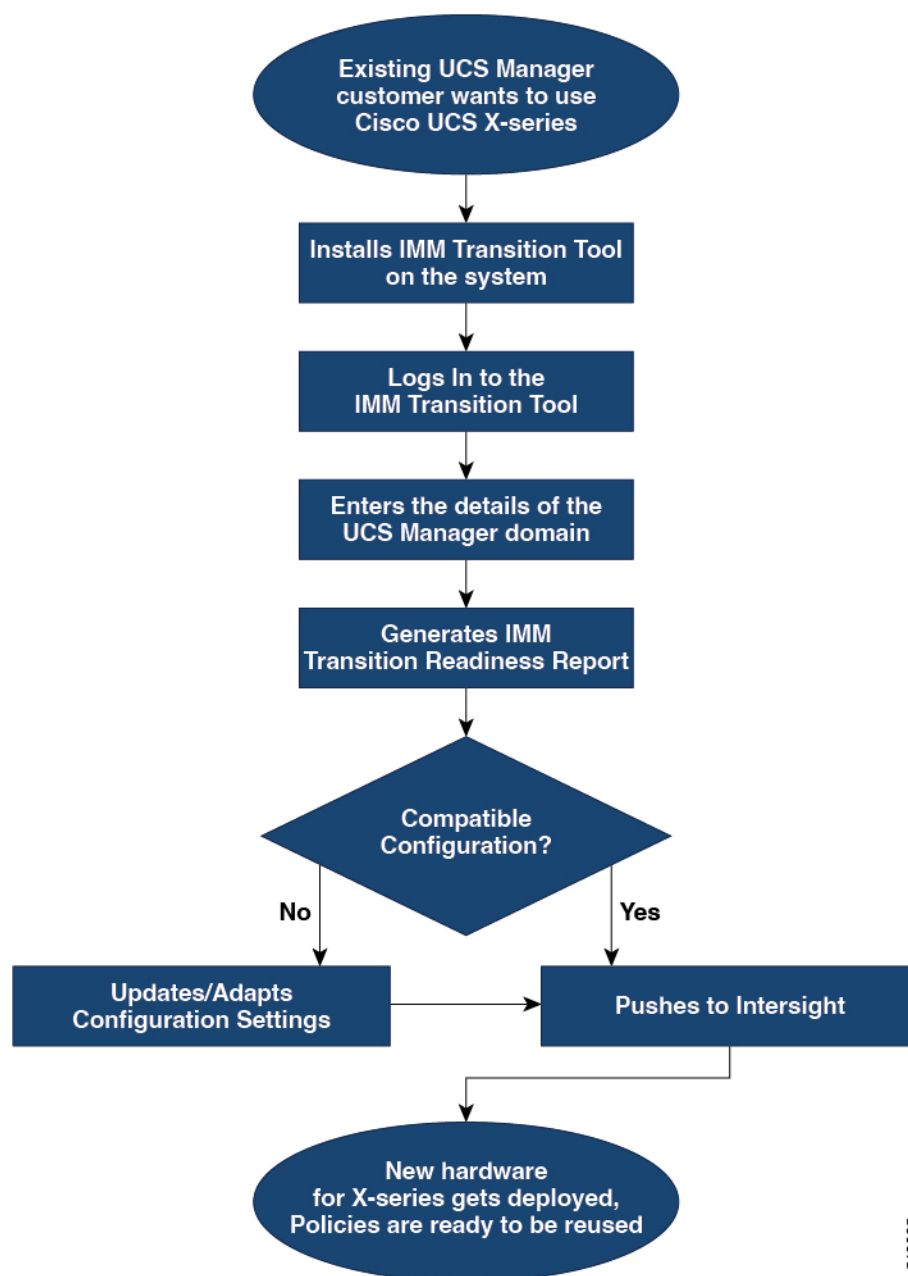
1. 右上隅の歯車アイコンの下にある [設定 (Settings)] をクリックします。
2. [プロキシを有効にする (Enable Proxy)] を切り替えてオンにします。
3. [プロキシホスト名 (Proxy Hostname)] または [IP] を入力します
4. プロキシポート番号を入力します。
5. プロキシ設定で認証が必要な場合は、[認証 (Authentication)] を切り替えてオンにするか、手順 8 に進みます。
6. ユーザ名を入力します。
7. パスワードを入力します。
8. [保存 (Save)] をクリックします。  
プロキシ設定が保存されます。

## 付録 D : サンプル使用例

### UCS X シリーズの展開の拡張

ファブリック インターコネクトは UCS X シリーズをサポートする際、Intersight 管理モードで動作します。Cisco UCS Manager を使用していて、UCS X シリーズを使用する場合は、IMM に移行する必要があります。この移行

- 既存のサービスプロファイル テンプレートを Intersight に拡張します。
- ブート、BIOS、LAN/SAN 接続など、関連するサーバー ポリシーを自動的に変換します。
- VLAN / VSAN、ポート構成などのファブリック構成を変換します。



次の手順を実行して、既存の UCS Manager ドメイン オブジェクトを Intersight オブジェクトに変換します。

#### 始める前に

システムは、[前提条件 \(Prerequisites\)](#) セクションに記載されている前提条件を満たしている必要があります。

---

**ステップ 1** システムに Cisco IMM 移行ツールをインストールします。



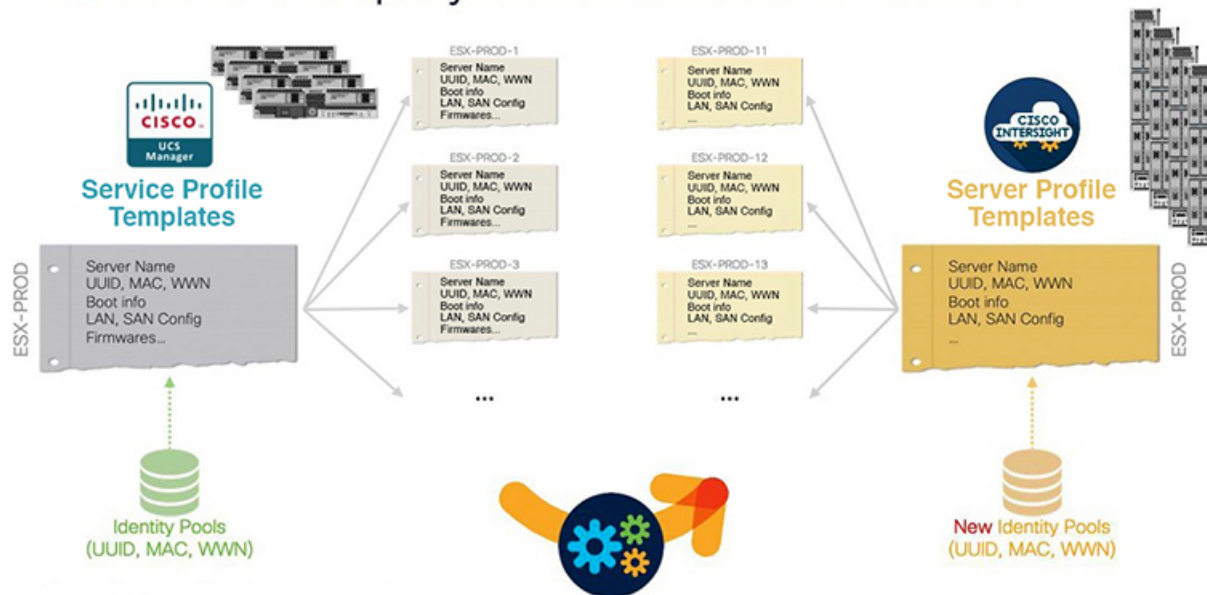
Cisco Intersight マネージド モード移行ツールのインストールに記載されているインストール手順に従います。

- ステップ 2 IMM 移行ツールにログインします。
- ステップ 3 UCS Manager ドメインの詳細を入力します。
- ステップ 4 準備状況レポートを生成して、移行の互換性を確認します。
- ステップ 5 a) 互換性がない場合は、構成設定を更新します。  
b) 互換性がある場合は、変換された構成を Intersight にプッシュします。

### 次のタスク

新しいハードウェアが展開されます。UCS Manager ドメインのソフトウェア構成、および既存のポリシーを再利用する準備ができています。どこからでも Cisco UCS X シリーズシステムを監視し、サーバー全体でポリシーベースの管理を実行できるようになりました。

## Accelerate deployments of UCS X-Series



この移行を実行する手順については、「[Cisco Intersight マネージド モード移行ツールの使用](#)」を参照してください。

## 付録 E : フィードバックの送信

右上隅にある [フィードバック (Feedback)] アイコンを使用して、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。

## 付録 F : テクニカル 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](mailto:imm-transition-feedback@cisco.com) グループに送信します。  
<mailto:imm-transition-feedback@cisco.com>