設定

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 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。

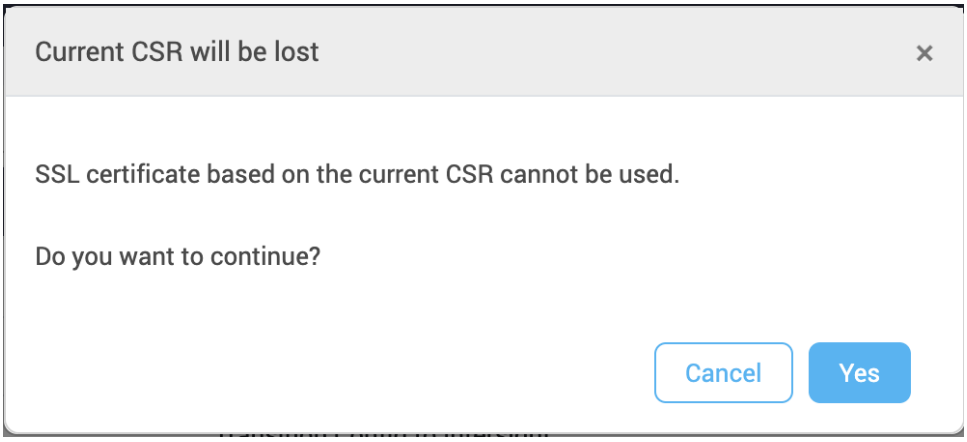
新しい CSR の作成

[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。

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。