デバイス コネクタ

- Intersight 管理モード （1 ページ）
- デバイス コネクタ （2 ページ）

Intersight 管理モード

Intersight 管理モード (IMM)は、Cisco Intersight で導入された新しい機能セットで、B シリーズブレードおよび FI の管理対象 C シリーズのサーバのサーバ プロファイルを設定、展開、管理することができます。IMM は、Cisco UCS Manager で最初に導入されたコンセプトを新しく実装しており、ポリシー モデルのオーナーシップを Cisco Intersight に移行しています。それで、ポリシー、VLAN、VSAN を前もって作成し、サーバ プロファイルに組み込むことができます。その後、サーバプロファイルは、B シリーズのブレードまたは管理対象 C シリーズのサーバで検出された Cisco Intersight に割り当てられ、展開されます。

第 4 世代のファブリック インターコネクト (FI) で IMM を有効にするには、Cisco UCS インフラストラクチャとサーバ ファームウェア (FW)(4.1(2)) で通常どおりのアップグレードを実行し、アップグレードが正常に完了してから、FI をリセットします。FI のリセット後に、セットアップ プロンプトで、Intersight を管理ノードとして選択します。FI のうちの一方を IMM モードでセットアップし、もう一方はクラスタに参加させることができます。それから、IMM ドメインを Cisco Intersight に対して要求します。IMM では、UCS のためのすべての設定と処理は、 Cisco Intersight から行われます。IMM では、FI をユニファイド ポート (イーサネットと FC) およびポート ロール)(アップリンクとサーバ) によって FI-A と FI-B にプログラムできるように、UCS のドメイン プロファイルを設定し、展開します。新しい UCS ドメイン プロファイルは、新しい UCS ドメインが Cisco Intersight ですばやくオンボードされるようにします。

（注） Cisco UCS インフラストラクチャおよびサーバ FW バージョン 4.1(2) では、IMM のテクニカル プレビューをオプトインできます (FI および接続されたサーバ用のポリシー駆動型設定プラットフォーム)。IMM を有効にすると、UCS ドメイン全体が工場出荷時のデフォルトにリセットされ、ドメイン内のサーバで実行されているワークロードが中断されます。この機能はテクニカル プレビューであり、実稼働ワークロードやアプリケーションには推奨されません。

デバイス コネクタ

デバイス コネクタは、Cisco UCS Manager をクラウドホスト型のサーバ管理システムである Cisco Intersight に接続します。これにより、Cisco UCS Manager を Cisco Intersight を使用して管理およびモニタできるようになります。

クラウド内の Cisco Intersight にデバイスを登録するには、次の手順を実行します。

1. 必要に応じて、デバイス コネクタのプロキシ設定を行って、Cisco UCS Manager を Cisco Intersight と接続します。
2. デバイスのシリアル番号とセキュリティ コードを使用して、Cisco Intersight からデバイスへのアクセスを検証し、デバイスを要求します。

Cisco Intersight 管理の有効化または無効化

Cisco Intersight 管理を有効にすると、Intersight クラウドアプリケーションとデバイス間の双方向通信が確立されます。

始める前に

デバイス コネクタを設定するには、管理者である必要があります。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[すべて (All)]** > **[デバイス コネクタ (Device Connector)]** の順に展開します。

[デバイス コネクタ (Device Connector)] タブに、接続ステータスと、セットアクセス モードが表示されます。**[デバイス コネクタ (Device Connector)]** タブに表示されるデバイス ID と要求コードは、Cisco Intersight で Cisco UCS Manager を要求するために使用されているものです。

ステップ 3 [設定（Settings）] をクリックします。

ステップ 4 **[設定 (Settings)]** ウィザードで、**[全般 (General)]** をクリックします。

ステップ 5 Intersight 管理を有効にするには **[デバイス コネクタ (Device Connector)]** スライダを有効にし、Intersight 管理を無効にするには **[デバイス コネクタ(Device Connector)]** スライダを無効にします。

デフォルトで、Cisco Intersight び管理状態が**有効**なっています。

ステップ 6 [アクセス モード（Access Mode）] で [読み取り専用（Read-only）] または [制御を許可（Allow Control）] を選択します。

[Read-only (読み取り専用)] アクセス モードを選択すると、Cisco Intersight を使用してデバイスを構成できなくなります。したがって、クラウドからデバイス コネクタに送信される構成は、エラー コードを伴って拒否されます。

[Allow Control (制御を許可)] モードを選択すると、Cisco Intersight を使用したデバイスの構成を完全に制御できます。

ステップ 7 Intersight 管理を無効にするには、**[デバイスコネクタ (Device Connector)]** スライダを無効にします。

Intersight 管理を無効にすると、[接続（Connection）] 領域に接続状態が [管理上無効（Administratively Disabled）] として表示されます。

ステップ 8 **[Save]** をクリックします。

Intersight デバイス コネクタのプロパティの表示

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[すべて (All)]** > **[デバイス コネクタ (Device Connector)]** の順に展開します。

[デバイス コネクタ (Device Connector)] タブに、接続ステータスと、セット アクセス モードが表示されます。**[デバイス コネクタ (Device Connector)]** タブに表示されるデバイス ID と要求コードは、Cisco Intersight で Cisco UCS Manager を要求するために使用されているものです。

ステップ 3 [設定（Settings）] をクリックします。

ステップ 4 **[設定 (Settings)]** ウィザードで、次の情報を確認します。

名前	説明
[General] タブ	Cisco UCS Manager と Cisco Intersight 間の接続の状態。 **[デバイス コネクタ (Device Connector)]** スライダ：Cisco Intersight の管理を有効または無効にできます。次のいずれかを実行できます。 • **[デバイス コネクタ (Device Connector)]** スライダをオンにする： Cisco Intersight 管理を有効にします。このシステムを要求（請求）して、Cisco Intersightの機能を活用できます。 （これがデフォルトの接続ステータスです）。 • **[デバイス コネクタ (Device Connector)]** スライダをオフにする：Cisco Intersight 管理を無効にします。Cisco Intersight との通信は許可されません。 **[Access Mode]**：**[Read-only]** または **[Allow Control]** としてアクセスを構成します。 • **[Read-only]**：**[Read-only]** アクセス モードを選択すると、Intersight を使用してデバイスを設定できなくなります。 • **[Allow Control]** — **[Allow Control]** アクセス モードを選択すると、Intersight を使用したデバイスの構成を完全に制御できます。
[DNS の構成 (DNS Configuration)] タブ	DNS 設定を行います。 • **[ドメイン名 (Domain name)]** フィールド：ドメイン名を追加します。 • **[DNS サーバ (DNS Server)]** フィールド：DNS 名前解決を有効にするように少なくとも 1 つの DNS サーバを設定します。Intersight Device Connector は、DNS レコードを正常に解決できる必要があります。 （注） DNS 設定が Cisco UCS Central のグローバル ポリシーで管理されている場合、DNS 設定はグレー表示されます。このような場合は、Cisco UCS Central から DNS 設定を更新します。

名前	説明
[NTP の設定（NTP Configuration）] タブ	NTP 設定を行います。時刻同期用に少なくとも 1 つの NTP サーバを設定することを強く推奨します。システム クロックの時刻がインターネットの時刻と同期していない場合でも、Intersight デバイス コネクタは、時間オフセットが大きすぎない限り、Intersight サービスと通信できます。タイムオフセットが Intersight X.509 証明書の有効期間外の場合、デバイスコネクタは Intersight サービスと通信できません。 • **[NTPサーバ (NTP Server)]** フィールド：少なくとも 1 つの NTP サーバを設定します。 （注） NTP 設定が Cisco UCS Central のグローバルポリシーで管理されている場合、NTP 設定はグレー表示されます。このような場合は、Cisco UCS Central から NTP 設定を更新します。
[Proxy Configuration (プロキシ設定)] タブ	HTTPS プロキシ設定が無効か、または手動で設定されているかどうかを示します。次のいずれかになります。 • **[プロキシの有効化 (Enable Proxy)]** をオフにする：HTTPS プロキシ構成を無効にします。 • **[プロキシの有効化 (Enable Proxy)]** をオンにする：HTTPS プロキシ構成を有効にします。 • [Proxy Hostname/IP]：プロキシのホスト名または IP アドレスを入力します。 • [Proxy Port]：プロキシ ポート番号を入力します。 • [Authentication]：プロキシ サーバへのアクセスを認証するには、このオプションを有効にします。 アクセスを認証する**ユーザ名**と**パスワード**を入力します。 （注） デバイス コネクタで必須となるログイン クレデンシャルのフォーマットはなく、入力したクレデンシャルがそのまま構成済み HTTP プロキシ サーバに渡されます。ドメイン名でユーザ名を限定する必要があるかどうかは、HTTPプロキシサーバの設定によって異なります。

名前	説明
[Certificate Manager (証明書マネージャ)] タブ	信頼できる証明書のリストを表示し、有効な信頼できる証明書をインポートできます。 • **[Import]**：CA 署名付き証明書をインポートすることができます。 **重要** インポートされた証明書が *.pem (base64 エンコード) 形式である必要があります。 • 次の情報と証明書のリストを表示することができます。 • **[Name]**：CA 証明書の共通名。 • **[In Use]**：信頼ストアで証明書を正常にリモートサーバの確認に使用されたかどうか。 • **[Issued By]**: 証明書の発行認証局。 • **[Expires]**—証明書の有効期限。 （注） バンドルされた証明書は削除できません。

ステップ 5 [閉じる（**Close**）] をクリックします。

デバイス コネクタの更新

Cisco UCS Manager をアップグレードすると、デバイス コネクタは Cisco UCS Manager バージョンと統合されたイメージに自動的に更新されます。Cisco UCS Manager バージョンをダウングレードしても、デバイス コネクタはダウングレードされません。

Cisco Intersight GUI を使用して、デバイス コネクタを更新できます。Cisco UCS Manager CLI でローカル管理シェルを使用して、デバイス コネクタを更新することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **connect local-mgmt**	ローカル管理モードを開始します。
ステップ 2	UCS-A(local-mgmt)# **copy** [*from-filesystem*:] [*from-path*] *filename to-path* [*dest-filename*]	指定されたファイル転送プロトコルを使用して、デバイス コネクタのイメージ ファイルをリモート サーバからローカルの宛先にコピーします。ファイルは、1 つのファブリック インターコネクトにのみコピーする必要があります。

	コマンドまたはアクション	目的
		• *from-filesystem*：コピー元のファイルを含んでいるリモート ファイル システム。 このファイルは、次のオプションのいずれかを使用して指定できます。 • **ftp:** [// [*username@*] *server*] • **scp:** [// [*username@*] *server*] • **sftp:** [// [*username@*] *server*] • **tftp:** [//*server* [*:port*]] ファイル システムを指定しない場合、現在の作業ファイル システムが表示されます。 サーバ名を指定せずに、リモート プロトコルを指定した場合、サーバ名の入力が求められます。 • *from-path*：コピー元のファイルの絶対パスまたは相対パス。パスを指定しない場合、現在の作業ディレクトリが前提とされます。 • *filename*：コピー元のファイルの名前。 • *to-path*：コピー先のファイルの絶対パスまたは相対パス。パスを指定しない場合、現在の作業ディレクトリが前提とされます。このパスにはローカル ファイル システムが組み込まれており、コピー先のファイルが含まれています。 このファイル システムは、次のオプションのいずれかから指定できます。 • **volatile:** • **workspace:** • *dest-filename*：コピー先のファイルの新しいファイル名。dest-filename

	コマンドまたはアクション	目的
		を指定すると、コピー元のファイルはコピー先で名前変更されます。 （注） Cisco UCS Manager GUI を使用してデバイス コネクタのイメージ ファイルをダウンロードすることはできません。
ステップ 3	UCS-A(local-mgmt)# **update-device-connector workspace:** | **volatile:**/*filename* [**skip-upgrade-on-peer**]	ピアのファブリック インターコネクトでデバイス コネクタ イメージを更新してから、ローカルのファブリック インターコネクトを更新します。 **skip-upgrade-on-peer** オプションを使用すると、ピアのファブリック インターコネクトの更新がスキップされます。

例

次に、両方のファブリック インターコネクトでデバイス コネクタを更新する例を示します。

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin
Update Started
Updating Device Connector on peer Fabric interconnect
Successfully updated device connector on peer Fabric interconnect
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```

次に、ローカルのファブリック インターコネクトのみでデバイス コネクタが更新される例を示します。

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin skip-upgrade-on-peer
Update Started
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```