



Device Connector の管理

- [Intersight 管理モード \(1 ページ\)](#)
- [デバイス コネクタを有効化または無効化 \(2 ページ\)](#)
- [プロキシ設定 \(2 ページ\)](#)
- [証明書のインポートまたは、表示 \(3 ページ\)](#)
- [アプライアンス接続のチェック \(4 ページ\)](#)

Intersight 管理モード

Cisco Intersight は、シスコとサードパーティの IT インフラストラクチャ向けの分析機能が組み込まれた SaaS 方式の管理プラットフォームです。Intersight Managed Mode (IMM) は、Redfish ベースの標準モデルを通じて UCS ファブリックインターコネクトシステムを管理する新しいアーキテクチャです。Intersight マネージドモードは、UCS システムの機能と Intersight のクラウドベースの柔軟性を統合し、スタンドアロンおよびファブリックインターコネクト接続システムの管理エクスペリエンスを統合します。

Cisco ベースボード管理コントローラ 2.0 REST API ガイド、リリース 2.0 デバイス コネクタが Cisco Intersight サービスへの接続を検出しない場合、次の警告を表示します。

デバイス コネクタは、Cisco Intersight に対しての接続を検出できません。設定を確認し、サーバーが Intersight インフラストラクチャ サービス ライセンスに準拠して Intersight で要求されていることを確認してください。(1/5)

以下をクリックします **[OK]** をクリックします [デバイス コネクタ (Device Connector)] に移動し、設定を構成するか、**キャンセル** をクリックして続行します。

警告とは別に、Cisco BMC 2.0 画面の上部に次の静的リボンも表示します：

注：このサーバーには、Intersight インフラストラクチャ サービス ライセンス ライセンスが必要です。詳しくはこちら

詳細をクリックすると、Intersight ヘルプ センターから詳細情報を取得できます。



(注) このメッセージは、デバイス コネクタが構成されている場合は表示されません。デバイス コネクタを一度構成し、後で無効にすると、メッセージが再度表示されます。

デバイス コネクタを有効化または無効化

手順

ステップ1 [Navigation] ペインから、[管理]>[デバイス コネクタ]をクリックします。

ステップ2 [設定] アイコンをクリックします。

[設定] ナビゲーションが表示されます。

ステップ3 選択 **全般** をクリックします。

次のプロパティを表示または、アップデートすることができます：

名前	説明
デバイス コネクタ トグル ボタン	Intersight の管理を有効または無効にできます。次のいずれかになります。 <ul style="list-style-type: none"> • 点灯：Intersight の管理を有効にします。このシステムに対し要求を行って、Cisco Intersight の機能を活用できます。 • 消灯：Intersight 管理を無効にします。Cisco Intersight への通信は許可されません。

ステップ4 [保存 (Save)] をクリックします。

プロキシ設定

手順

ステップ1 [Navigation] ペインから、[管理]>[デバイス コネクタ]をクリックします。

ステップ2 [設定] アイコンをクリックします。

[設定] ナビゲーションが表示されます。

ステップ3 選択 プロキシ設定。

次のプロパティを表示または、アップデートすることができます：

名前	説明
プロキシを有効にする トグル ボタン	HTTPS プロキシ設定を有効または無効にすることができます。
プロキシホスト名/IP field	プロキシ サーバーの IP アドレスまたはホスト名。
プロキシポート field	プロキシ サーバーのポート番号。
認証 トグル ボタン	このオプションを有効にすると、プロキシサーバーのクレデンシアルを提供できます。
[ユーザー名 (Username)] field	プロキシ サーバーのクレデンシアルです。
パスワード (Password) field	

ステップ4 [保存 (Save)] を [Save]。

証明書のインポートまたは、表示

手順

ステップ1 [Navigation] ペインから、[管理]>[デバイス コネクタ]をクリックします。

ステップ2 [設定] アイコンをクリックします。

[設定] ナビゲーションが表示されます。

ステップ3 選択 証明書マネージャ。

次のプロパティを表示または、アップデートすることができます：

表 1: 証明書マネージャ

名前	説明
インポート (Import) ボタン	CA 署名付き証明書を選択してインポートすることができます。 (注) 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。

名前	説明
[名前 (Name)] column	CA 証明書の共通名。
使用中 column	トラストストアでリモートサーバーを正しく確認するため証明書を使用したかどうか。
発行元 (Issued By) column	証明書の発行機関。
Expires column	証明書の有効期限日。
[View Certificate] アイコン	クリックして証明書の詳細を表示します。
証明書の削除 ボタン	証明書を削除できます。 (注) バンドルされている証明書(ロックアイコンが証明書)を削除することはできません。

アプライアンス接続のチェック

手順

ステップ1 [Navigation] ペインから、[管理]>[デバイス コネクタ]をクリックします。

ステップ2 [設定] アイコンをクリックします。

[設定] ナビゲーションが表示されます。

ステップ3 選択 **接続** をクリックします。

ステップ4 From the **接続の確認** ドロップダウン リストから、接続を確認するアプライアンスを選択します。

次のプロパティを表示することができます：

表 2: 接続

名前	説明
詳細を表示	以下を表示できます。 アドレス および 遅延 (Latency) DNS 解決の値を入力します。
デバッグ ログ	デバッグ ログを表示できます。

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。