Cisco APIC および Intersight デバイス コネクタ

改訂：2023 年 1 月 27 日

新規および変更情報

次の表は、この最新リリースまでのガイドでの主な変更点の概要を示したものです。ただし、このリリースまでのこのガイドの変更点や新機能の中には一部、この表に記載されていないものもあります。

表 *1*：新機能と変更された動作

Cisco APIC リリース	機能	説明
6.0(1)	スイッチは自動的に要求されます	Cisco APIC を要求すると、ファブリック内のすべてのスイッチも Cisco Intersight で自動的に要求されます。 詳細については、GUI を使用したデバイスの要求 （11 ページ）を参照してください。
5.2(1)	DNS とプロキシは、**[サイト間デバイス コネクタ（Intersight-Device Connector）]**ページでは構成しなくなりました。	DNS とプロキシは、**[サイト間デバイス コネクタ（Intersight-Device Connector）]**ページでは構成しなくなりました。代わりに、これらの設定は Cisco APIC の一元管理されたエリアで構成されます。**[サイト間デバイス コネクタ（Intersight-Device Connector）]** ページではありません。
4.2(5)	**[自動更新（Auto Update）]**がデフォルトで有効になっています。	**[自動更新（Auto Update）]**オプションがデフォルトで有効になっています。
4.1(2)	この機能の初期リリースです。	この機能の初期リリースです。

デバイス コネクタについて

デバイスは、各システムの管理コントローラに組み込まれているデバイスコネクタを介して Intersight ポータルに接続されます。デバイス コネクタは、接続されているデバイスに対して、セキュリティで保護されたインターネット接続を使用して情報を送信し、Cisco Intersight ポータルから制御命令を受信できる安全な方法を提供します。

Intersight 対応のデバイスまたはアプリケーションが起動すると、デフォルトではブート時にデバイス コネクタが起動してクラウドサービスに接続しようとします。**[自動更新（Auto Update）]**オプションが有効になっている場合、Cisco Intersight に接続するときに、Cisco Intersight サービスによる更新を介してデバイスコネクタが自動的に最新バージョンに更新されます。**[自動更新（Auto Update）]** オプションの詳細については、自動更新オプションについて （3 ページ） を参照してください。

自動更新オプションについて

[自動更新（Auto Update）] オプションを有効にした場合、デバイス コネクタは Cisco Intersight クラウドからアップグレードメッセージを受信した後、自動的にアップグレードを開始します。この間、デバイス コネクタは Cisco Application Policy Infrastructure Controller（APIC）がアップグレードされているかどうかを確認します。がアップグレードされている場合、デバイス コネクタのアップグレードは最大 24 時間延期され、その後、アップグレードされているかどうかに関係なくデバイス コネクタがアップグレードされます。Cisco APICCisco APICアップグレード中の Cisco APIC がない場合、デバイス コネクタはすぐにアップグレードを開始します。同様に、Cisco APIC のアップグレードの事前検証プロセスは、Cisco APIC のアップグレードを開始するときに、デバイス コネクタがアップグレードされているかどうかを確認します。このような場合、アップグレード ページには対応する警告メッセージが表示されます。

デバイス コネクタのアップグレードが進行中の場合、次のメッセージが表示されます。

```
DC upgrade is in progress. Wait for DC upgrade to complete before triggering APIC upgrade
```

Cisco APIC のアップグレード前の検証でデバイス コネクタのアップグレード ステータスを確認できない場合、次のメッセージが表示されます。

```
Could not check DC upgrade status
```

この場合、Cisco APIC のアップグレードを再開始します。同じメッセージが表示されてアップグレードが再度失敗する場合は、1 ～ 2 分待ってから再試行してください。

[自動更新（Auto Update）] オプションが無効になっていて、新しいデバイス コネクタ ソフトウェア バージョンが利用可能な場合、新しいリリースが利用可能になったときに、デバイス コネクタ GUI ページでソフトウェアを手動で更新するように求められます。さらに、デバイス コネクタが古くなる可能性があり、デバイス コネクタが Cisco Intersight に接続する機能に影響を与える可能性があります。

[自動更新（Auto Update）] オプションを有効にすることが推奨されています。Cisco APIC リリース 4.2(5) 以降、このオプションはデフォルトで有効になっています。

Cisco APIC を 4.2(4) 以前のリリースにダウングレードすると、4.2(5) 以降のリリースでポリシーが **[自動（Auto）]** に設定されていた場合、デバイス コネクタのアップグレード ポリシーは **[手動（Manual）]** に設定されます。

クラスタ済み APIC ノードでのデバイス コネクタ構成の変更について

Cisco APIC アプライアンスはクラスタとして展開されます。クラスタには、スケールアウト Cisco ACI ファブリックを制御するために、少なくとも 3 台の Infrastructure Controller またはノードが構成されます。

Cisco APIC ファブリック内のクラスタ化されたノードのいずれかでデバイス コネクタの構成を変更すると、その構成変更は、その Cisco APIC クラスタ内の他のノードの他のデバイス コネクタに自動的に反映されます。

たとえば、クラスタ内の APIC ノードの 1 つにあるデバイス コネクタの **[DNS 構成（DNS Configuration）]** ページで構成されている 2 つの DNS サーバーがあるとします。クラスタ内の他の 2 つの APIC ノードでデバイス コネクタの同じページに移動すると、それらのノードで構成されている同じ 2 つの DNS サーバーも表示されます。次に、クラスタ内のいずれかの APIC ノードのデバイス コネクタの **[DNS 構成（DNS Configuration）]** ページで 3 番目の DNS サーバーを追加し、そのページで **[保存（Save）]** をクリックした場合、DNS の変更が有効になるまでの 2 分間のサイクルの後、

変更は、クラスタ内の他の 2 つの APIC ノードのデバイス コネクタの **[DNS 構成（DNS Configuration）]** ページに表示されます。

この構成変更の動作は、Cisco APIC ファブリックのクラスタ化されたノード内の要求されたデバイス コネクタと要求されていないデバイス コネクタにも適用されます。たとえば、クラスタ内の 3 つの APIC ノードのいずれかでデバイス コネクタを構成して要求した場合、そのクラスタ内の他の 2 つの APIC ノードでデバイス コネクタが自動的に構成され、要求されていることがわかります。同様に、クラスタ内のいずれかの APIC ノードでデバイス コネクタを要求解除すると、そのクラスタ内の他の APIC ノードでデバイス コネクタが自動的に要求解除されることがわかります。

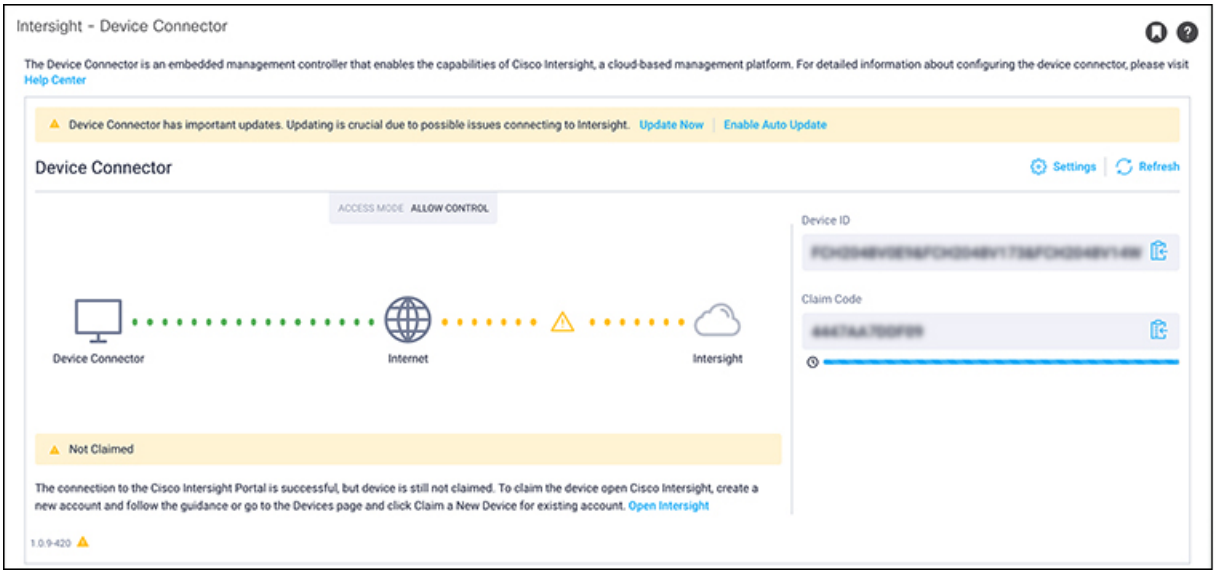
Intersight デバイス コネクタの設定

手順

ステップ 1 Cisco Application Policy Infrastructure Controller（APIC）で、メニュー バーで、**[システム（System）]**> > **[システム設定（System Settings）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで **[VM]** をクリックします。

[Intersight デバイス コネクタ（Intersight Device Connector）] の概要ページが表示されます。このページの **[デバイス コネクタ（Device Connector）]** の図で、デバイス コネクタはインターネットへ接続済み（緑色の点線）であることが表示されています。



- **[デバイス コネクタ（Device Connector）]** の図で **[インターネット（Internet）]** から **[Intersight]** へ接続する緑色の点線と、その図の下に **[要求済み（Claimed）]** というテキストが表示されている場合、Intersight デバイス コネクタはすでに構成されており、Intersight サービスに接続され、デバイスは要求済みです。
- **[デバイス コネクタ（Device Connector）]** の図に黄色い点線と **[インターネット（Internet）]** から **[Intersight]** へ接続する注意アイコンと、**[要求が未完了（Not Claimed）]** というテキストが表示され

ている場合、Intersight デバイス コネクタの構成、Intersight サービスへの接続、およびデバイスの要求は完了していません。次の手順に従って、Intersight デバイス コネクタの設定、Intersight サービスへの接続、およびデバイスの要求を行います。

（注） **[デバイス コネクタ（Device Connector）]** の図で **[インターネット（Internet）]** を **[Intersight]** に接続する赤い点線が表示されている場合は、ステップ 12 （9 ページ） でプロキシが正しく構成されていないことを示します。

ステップ 3 使用可能な新しいデバイス コネクタ ソフトウェア バージョンがある場合は、この時点でソフトウェアを更新するかどうかを決定します。

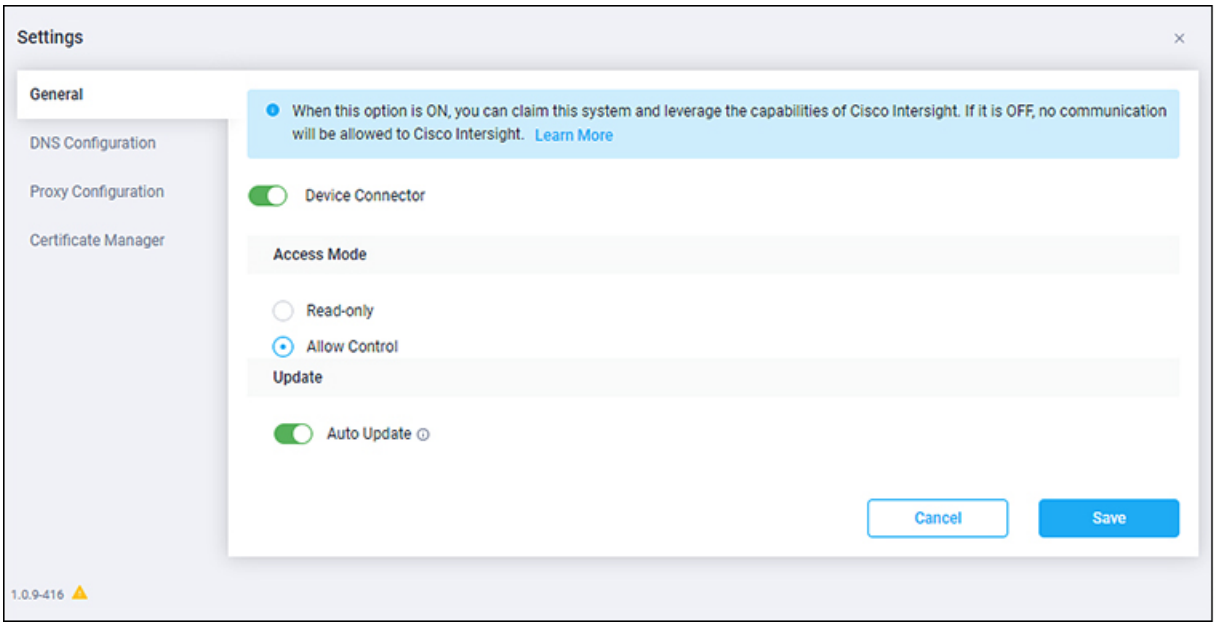
使用可能な新しいデバイス コネクタのソフトウェアバージョンがあり、**[自動更新（Auto Update）]** オプションが有効になっていない場合は、デバイス コネクタに重要な更新プログラムがあることを通知するメッセージが画面の上部に表示されます。

- この時点でソフトウェアを更新しない場合は、ステップ 4 （5 ページ） に進み、Intersight デバイス コネクタの構成を開始します。
- この時点でソフトウェアを更新する場合は、ソフトウェアの更新方法に応じて、ページ上部にある黄色のバーの 2 つのリンクのいずれかをクリックします。
  - **[今すぐ更新（Update Now）]**: デバイスコネクタソフトウェアをすぐに更新するには、このリンクをクリックします。
  - **[自動更新の有効化（Enable Auto Update）]**: **[一般（General）]**ページに移動するには、このリンクをクリックします。**[自動更新（Auto Update）]** フィールドを [オン（On）] に切り替えると、システムはデバイス コネクタ ソフトウェアを自動的に更新できます。詳細については、「自動更新オプションについて （3 ページ）」を参照してください。

ステップ 4 **[デバイス コネクタ（Device Connector）]** 見出しの右側にある **[設定（Settings）]** リンクを見つけ、**[設定（Settings）]** リンクをクリックします。

[設定（Settings）] ページが表示され、**[General（設定）]** タブがデフォルトで選択されています。

（注） 次のスクリーンショットは、リリース 5.2(1) より前のリリースで表示される [設定（Settings）] ページのタブを示しています。ステップ 7 （7 ページ） で説明されているように、これらのタブはリリース 5.2(1) から変更されました。



ステップ 5 **[全般（General）]** ページで、次の設定を行います。

a) **[デバイス コネクタ（Device Connector）]**フィールドで、デバイスと Cisco Intersight 間の通信を許可するかどうかを決定します。

[デバイス コネクタ（Device Connector）] オプション（デフォルトで有効）を使用すると、デバイスを要求し、Intersight の機能を活用できます。オフになっている場合、Intersight への通信は許可されません。

b) **[アクセスモード（Access Mode）]** フィールドで、Intersight がこのデバイスに変更を加えることを許可するかどうかを決定します。

[アクセス モード（Access Mode）] では、クラウドからの完全な読み取り/書き込み操作を許可したり、Intersight からこのデバイスに加えられた変更を制限したりできます。

- [接続を許可（Allow Control）] オプション（デフォルトで選択）を使用すると、Cisco Intersight で使用可能な機能に基づいて、クラウドからすべての読み取り/書き込み操作を実行します。
- [読み取り専用（Read-only）] オプションは、Intersight からこのデバイスに変更が加えられないことを保証します。たとえば、ファームウェアのアップグレードやプロファイルの展開などのアクションは読み取り専用モードでは許可されません。ただし、アクションは特定のシステムで使用可能な機能によって異なります。

c) **[自動更新（Auto Update）]** フィールドで、システムによるソフトウェアの自動更新を許可するかどうかを決定します。

- システムがソフトウェアを自動的に更新できるようにするには、[オン（ON）] を切り替えます。
- 必要に応じて手動でソフトウェアを更新できるように、[オフ（OFF）] に切り替えます。この場合、新しいリリースが利用可能になると、ソフトウェアを手動で更新するように求められます。

詳細については、「自動更新オプションについて （3 ページ）」を参照してください。

ステップ 6　**[全般（General）]** ページの設定を完了したら **[Save（保存）]** をクリックします。

[Intersight - デバイス コネクタ] の概要ページが再度表示されます。

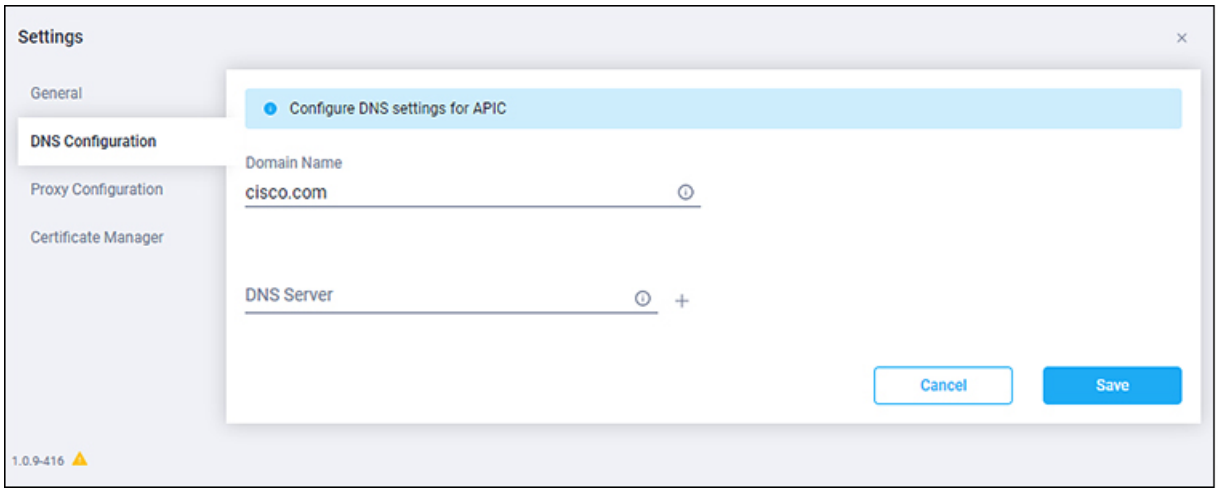
ステップ 7　ソフトウェアのリリースに応じて、構成プロセスの次のステップに進みます。

- リリース 5.2(1) より前のリリースを実行している場合は、**[Intersight デバイス コネクタ（Intersight - Device Connector）]** ページで、Intersight デバイス コネクタの DNS またはプロキシ構成の設定を作成または確認できます。
  - DNS 設定を構成または確認する場合は、ステップ 8 （7 ページ） に進みます。
  - デバイス コネクタが Intersight クラウドとの通信に使用するプロキシを構成する場合は、ステップ 11 （8 ページ） に進みます。

  さらに、デバイス コネクタを使用して証明書を管理する場合は、ステップ 14 （9 ページ） に進みます。
- リリース 5.2(1) 以降を実行している場合、DNS とプロキシ構成は、**[Intersight デバイス コネクタ（Intersight-Device Connector）]** ページでは構成しなくなりました。代わりに、APIC の一元管理されたエリアでこれらの設定を構成します。**[Intersight デバイス コネクタ（Intersight - Device Connector）]** ページではありません（この手順の後で説明）。
  - デバイス コネクタを使用して証明書を管理する場合は、ステップ 14 （9 ページ） に進みます。
  - DNS またはプロキシ構成を設定する場合は、ステップ 17 （10 ページ） に進みます。

ステップ 8　DNS設定を構成または確認する場合は、**[設定（Settings）]**をクリック後、**[DNS構成（DNS Configuration）]** をクリックします。

[DNS 構成（DNS Configuration）] ページが表示されます。



ステップ 9　**[DNS 構成（DNS Configuration）]** ページで、DNS 設定を構成または確認します。

このページで DNS サーバーを設定することもできますが、Cisco APIC 全般設定を利用して DNS サービスポリシーを設定し、DNS プロバイダーに接続することをお勧めします。これを行うには、**[ファブリック（Fabric）]**> > **[ファブリック ポリシー（Fabric Policies）]**> > **[ポリシー（Policies）]**> > **[グローバル（Global）]**> > **[DNS プロファイル（DNS Profiles）]** に移動し、**[DNS プロファイル（DNS Profiles）]** を右クリックして **[DNS プロファイルの作成（Create DNS Profile）]** を選択します。DNS サービス ポリシーの構成の詳細については、「*Cisco APIC* 基本構成ガイド」を参照してください。

上記のように、一般的な Cisco APIC 設定を使用して DNS サービス ポリシーを構成して DNS プロバイダーに接続する場合、この **[DNS 構成（DNS Configuration）]** ページにすでに入力されている DNS 構成情報が表示されます。そうでない場合、またはこのページで DNS サーバーを構成する場合は、次の手順に従います。

a) **[ドメイン名（Domain Name）]** フィールドで、DNS ドメイン名を追加します。
b) **[DNS サーバー（DNS Server）]** フィールドで、DNS 名前解決を有効にするように少なくとも 1 つの DNS サーバーを構成します。Intersight デバイス コネクタは、DNS レコードを正常に解決できるはずです。

デバイス コネクタは 2 分ごとに DNS の変更について Cisco APIC にクエリを実行するため、この時点で「APIC DNS の変更が有効になるまでに最大 2 分かかる可能性があります」という警告メッセージが表示される場合があります。

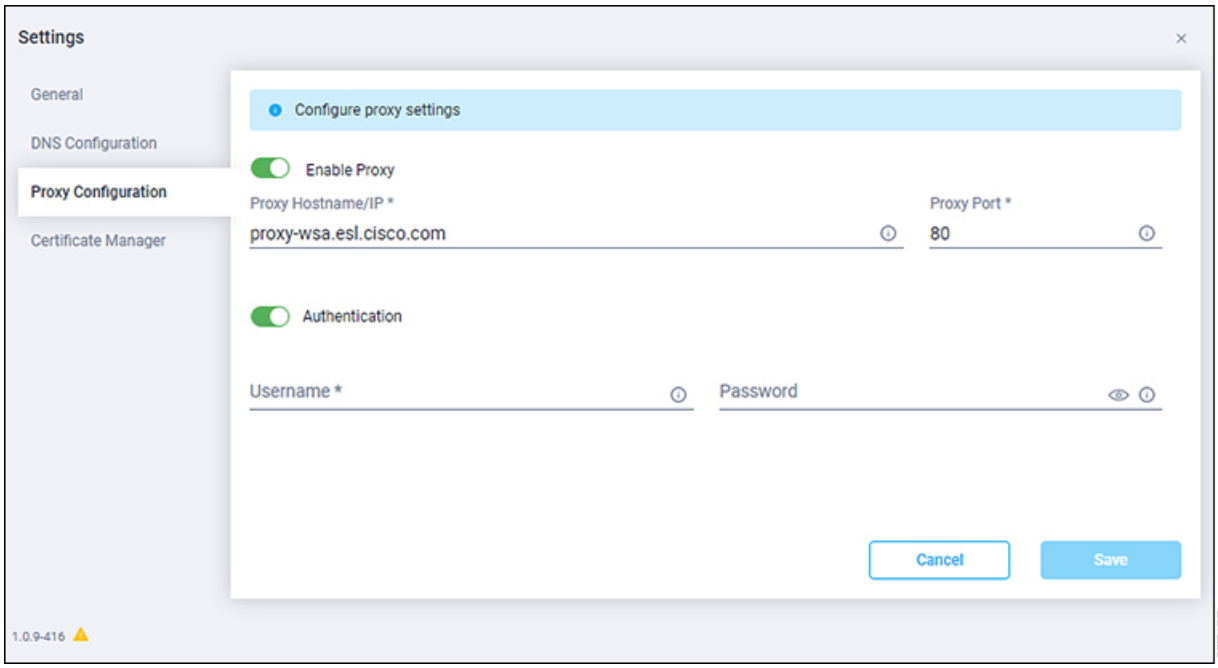
ステップ 10 構成が完了したら、**[DNS 構成（DNS Configuration）]** ページで **[保存（Save）]** をクリックします。

[Intersight - デバイス コネクタ] の概要ページが再度表示されます。この時点で、Intersight デバイス コネクタのいくつかの構成設定を行うか、確認できます。

- デバイス コネクタが Intersight クラウドとの通信に使用するプロキシを設定する場合は、ステップ 11 （8 ページ） に進みます。
- デバイス コネクタを使用して証明書を管理する場合は、ステップ 14 （9 ページ） に進みます。

ステップ 11 デバイス コネクタが Intersight クラウドとの通信に使用するプロキシを設定する場合は、**[設定（Settings）]** をクリックし、**[プロキシ設定（Proxy Configuration）]** をクリックします。

[プロキシ設定（Proxy Configuration）] ページが表示されます。



ステップ 12 **[プロキシ設定（Proxy Configuration）]** ページで、次の設定を行います。

このページでは、デバイス コネクタが Intersight クラウドとの通信に使用するプロキシを設定できます。

（注） デバイス コネクタで必須となるログイン情報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ー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。

a) **[プロキシの有効化（Enable Proxy）]** フィールドで、オプションを [オン（ON）] に切り替えてプロキシ設定を行います。
b) **[プロキシホスト名/IP（Proxy Hostname/IP）]** フィールドに、プロキシホスト名または IP アドレスを入力します。
c) **[プロキシポート（Proxy Port）]** フィールドで、プロキシポートを入力します。
d) **[認証（Authentication）]** フィールドで、**[認証（Authentication）]** オプションを [オン（ON）] に切り替えてプロキシ認証設定を行い、認証用のプロキシ ユーザー名とパスワードを入力します。

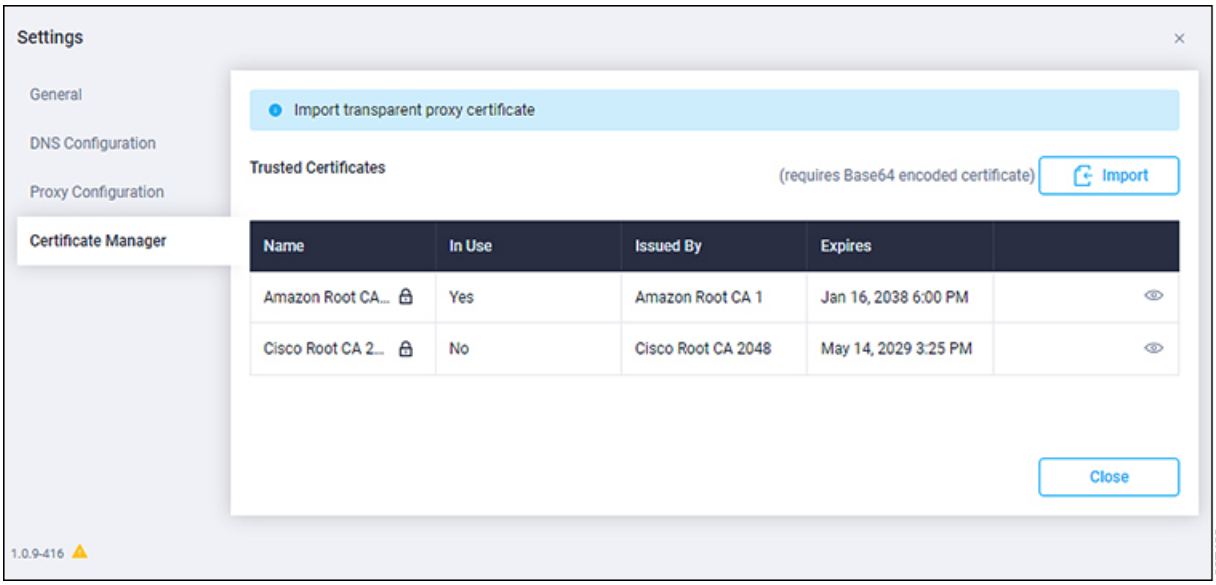
ステップ 13 **[プロキシ設定（Proxy Configuration）]** ページで設定が完了したら、**[保存（Save）]** をクリックします。

[Intersight - デバイス コネクタ] の概要ページが再度表示されます。

デバイス コネクタで証明書を管理する場合は、次の手順に進みます。

ステップ 14 デバイス コネクタを使用して証明書を管理する場合は、**[設定（Settings）]** をクリックし、**[証明書マネージャ（Certificate Manager）]** をクリックします。

[証明書マネージャ（Certificate Manager）] ページが表示されます。



ステップ 15 **[証明書マネージャ（Certificate Manager）]** ページで、次の設定を行います。

デフォルトでは、デバイス コネクタが信頼するのは組み込まれている svc.ucs-connect.com のみです。デバイス コネクタが TLS 接続を確立し、サーバが組み込まれている svc.ucs-connect.com 証明書に一致しない証明書を送信すると、デバイス コネクタはそのサーバが信頼できるデバイスかどうかを判断できないため、TLS 接続を終了します。

[インポート（Import）] をクリックして、CA 署名付き証明書をインポートします。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。証明書が正常にインポートされると、信頼できる証明書のリストに記載され、証明書が正しければ [使用中（In-Use）] に表示されます。

svc.ucs-connect.com（intersight.com）への接続に使用する証明書のリストの次の詳細を表示します。

- **[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。

信頼できる証明書のリストから証明書を削除します。ただし、バンドルされている証明書（root+中間証明書）はリストから削除できません。ロック アイコンは、バンドルされた証明書を表します。

ステップ 16 **[証明書マネージャ（Certificate Manager）]** ページで設定が完了したら、**[閉じる（Close）]** をクリックします。

ステップ 17 リリース 5.2(1) 以降を実行している場合は、次の場所に移動して、APIC の一元管理されたエリアでプロキシ設定を構成します。

- DNS 設定を構成するには、次の場所に移動します。

  [ファブリック（Fabric）] > > **[ファブリック ポリシー（Fabric Policies）]** > > **[ポリシー（Policies）]** > > **[グローバル（Global）]** > > **[DNS プロファイル（DNS Profiles）]**

[DNS プロファイル（DNS Profiles）] を右クリックして **[DNS プロファイルの作成（Create DNS Profiles）]** を選択します。DNS サービス ポリシーの構成の詳細については、「*Cisco APIC* 基本構成ガイド」を参照してください。

- プロキシ設定を構成するには、次の場所に移動します。

  [システム（System）] > **[システム設定（System Settings）]** > **[プロキシ ポリシー（Proxy Policy）]**

  [プロキシ ポリシー（Proxy Policy）] ページで、HTTP または HTTPS プロトコルのプロキシ サーバーを構成するか、特定のホストへの直接接続を許可するように構成を設定します。プロキシ サーバーに認証が必要な場合は、次のフォーマットを使用します。

  ```
  http[s]://[username:password]@proxy-server[:proxyport]
  ```

  プロキシ設定の構成の詳細については、「*Cisco APIC* 基本構成ガイド」を参照してください。

初回セットアップウィザードを使用して、DNS とプロキシの両方の設定を構成することもできます。詳細については、「*Cisco APIC* 基本構成ガイド」の「初回セットアップウィザード」の章を参照してください。

次のタスク

GUI を使用したデバイスの要求 （11 ページ） に記載されている手順に従ってデバイスを要求します。

GUI を使用したデバイスの要求

始める前に

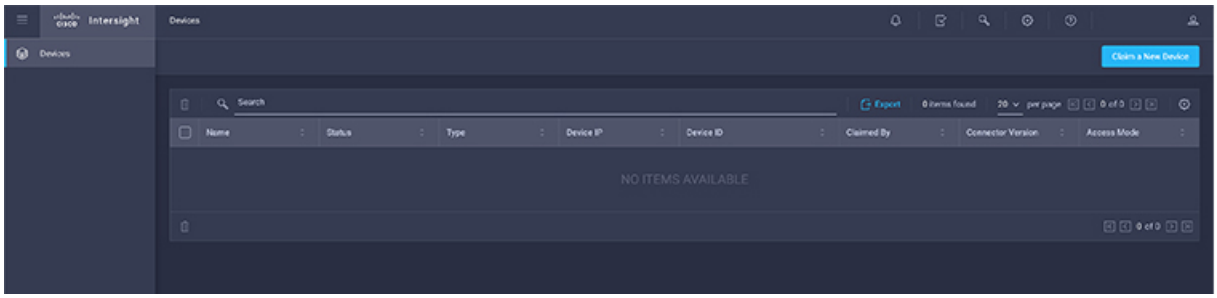
Intersight デバイス コネクタの設定 （4 ページ） で提供されている手順を使用して、Cisco Application Policy Infrastructure Controller（APIC）サイトから Cisco Intersight デバイス コネクタの情報を構成します。

手順

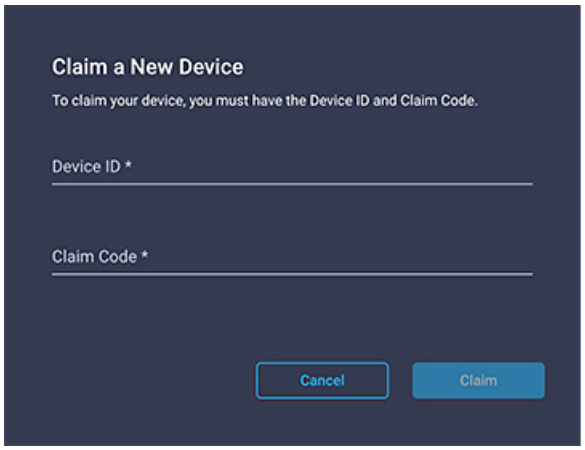
ステップ 1 Cisco Intersight クラウド サイトにログインします。

https://www.intersight.com

ステップ 2 Cisco Intersight クラウドサイトで、**[デバイス（Devices）]** タブをクリックし、**[新しいデバイスの要求（Claim a New Device）]** をクリックします。



[デバイス（Device）] ページが表示されます。



ステップ 3 Cisco APIC サイトに戻り、**[Intersight デバイス コネクタ（Intersight – Device Connector）]** ページに戻ります。

a) メニュー バーで、**[システム（System）]**> > **[システム設定（System Settings）]** を選択します。

b) **[ナビゲーション（Navigation）]** ペインで **[VM]** をクリックします。

ステップ 4 Cisco APICサイトから、**[デバイス ID（Device ID）]** および**[要求コード（Claim Code）]** をコピーし、Cisco Intersight クラウド サイトの **[新しいデバイスを要求（Claim a New Device）]** ページの適切なフィールドにペーストします。

Cisco APICサイトのフィールドの横にあるクリップボードをクリックして、フィールド情報をクリップボードにコピーします。

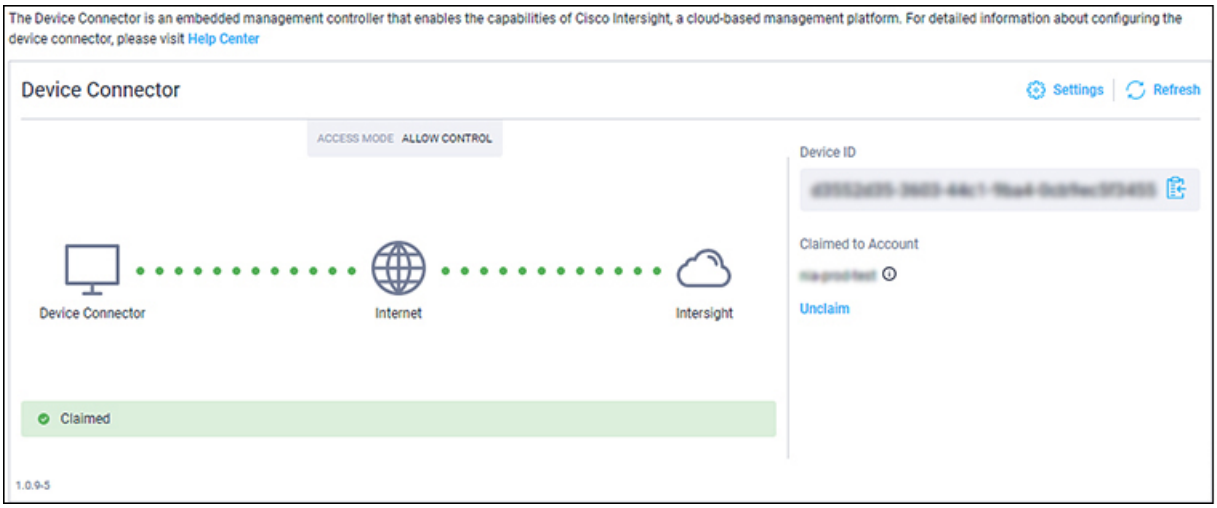
ステップ 5 Cisco Intersight クラウド サイトで、**[新しいデバイスの要求（Claim a New Device）]** ページで、**[要求する（Claim）]** をクリックします。

[新しいデバイスの要求（Claim a New Device）] ページに「デバイスが正常に申請されました」というメッセージが表示されます。また、メインページの [Status] 列に［接続済み（Connected）］と表示された Cisco APIC が表示されます。

6.0(1) リリース以降、Cisco APIC を要求すると、ファブリック内のすべてのスイッチも Cisco Intersight で自動的に要求されます。

ステップ 6 Cisco APIC GUIの **[Intersight デバイス コネクタ（Intersight - Device Connector）]** ページに戻り、Cisco Intersight がシステムに正常に要求したことを確認します。

[デバイス コネクタ（Device Connector）] の図に **[インターネット（Internet）]** と **[Intersight]** を接続する緑色の点線が描かれ、図の下に **[要求済み（Claimed）]** という文字が表示されます。



（注） ページの情報を現在の状態に更新するには、**[Intersight デバイス コネクタ（Intersight-Device Connector）]** ページで **[更新（Refresh）]** をクリックしなければならない場合があります。 z

何らかの理由でこのデバイスの要求を取り消す場合は、**[Intersight デバイス コネクタ（Intersight Device Connector）]** ページで **[要求解除（Unclaim）]** リンクを見つけて、そのリンクをクリックします。

Data Center HTTP または HTTPS プロキシ構成の自動入力について

4.2(4o) リリース以降、Cisco Application Policy Infrastructure Controller（APIC）は、スマート ライセンス HTTP または HTTPS プロキシ構成の値を使用して、データセンターのプロキシ構成を自動的に設定できます。この機能により、データセンター プロキシの構成プロセスが簡素化され、人的エラーの可能性が減少します。データセンターは、データセンターのブートストラップ時間中にのみ（Cisco APIC またはデータセンターのアップグレード時間中のいずれか）、プロキシ構成を読み取ります。Cisco APIC は、次の条件で構成を自動入力します。

- データセンターにプロキシが構成されていない場合、 Cisco APIC は、Cisco APIC または データセンターのアップグレードの結果として、データセンターのブートストラップ時間中にライセンス マネージャから読み取り、スマート ライセンス構成からプロキシ情報を入力します。
- データセンターは、Cisco APIC またはスマート ライセンスからの構成の変更をモニタしません。
- データセンターのブートストラップが完了した後にスマート ライセンス プロキシ構成に加えられた変更は、データセンターに反映されません。データセンターが Cisco Intersight と通信できない場合、GUI で適切なアラートが発生します。
- スマート ライセンスまたはユーザ構成から構成を事前入力した結果として構成がデータ センターに既に存在する場合、データセンターは次のブートストラップ時にスマート ライセンスからの構成を使用しません。

- プロキシ情報はデータセンターに事前に入力されていますが、Cisco APIC とのインベントリ共有は引き続き Cisco Network Insights Advisor から制御されます。
- プロキシサーバーが認証を必要とする場合、データセンターはプロキシ認証の構成（ユーザー名/パスワード）を事前に入力することはできません。これは、この情報がスマート ライセンスから入手できないためです。

データセンターは、licenseLicPolicy 管理対象オブジェクトからプロキシ構成を読み取り、モードが **proxy** に設定されている場合にのみ構成を入力します。

Data Center HTTP または HTTPS プロキシ構成の自動入力を無効にする

Cisco Application Policy Infrastructure Controller（APIC）インベントリを Cisco と共有したくない場合は、Cisco APICでプロキシ構成を無効にすることができます。これにより、プロキシ構成の自動入力機能も無効になります。

（注） これらの手順は、リリース 5.2(1) より前のリリースに適用されます。リリース 5.2(1) 以降の場合、プロキシ構成は、**[サイト間 - デバイス コネクタ（Intersight-Device Connector）]** ページでは構成されなくなりました。代わりに、これらの設定は APIC のこの集中エリアで構成されます。

[システム（System）] > **[システム設定（System Settings）]** > **[プロキシ ポリシー（Proxy Policy）]**

手順

ステップ 1 Cisco APIC で、メニュー バーで、**[システム（System）>]** > **[システム設定（System Settings）]** を選択します。

ステップ 2 ナビゲーションウィンドウで、**[サイト間（Intersight）]** を選択します。

ステップ 3 [作業（Work）] ペインで、**[設定（Settings）]**> > **[プロキシ構成（Proxy Configuration）]**をクリックします。

ステップ 4 **[プロキシの有効化（Enable Proxy）]** スライダーをクリックして無効にします。スライダーが左側に移動し、スライダーのバックグラウンドが灰色になります。

ステップ 5 [保存（Save）] をクリックします。

【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。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

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/

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。