Cisco Cloud APIC および Intersight デバイス コネクタ

改訂：2022 年 12 月 1 日

新機能と変更情報

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
25.0(4)	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 （2 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）]** オプションを有効のままにすることを推奨します。

[自動更新（Auto Update）] オプションが有効になっている場合、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 Cloud APIC がアップグレードされているかどうかを確認します。Cisco Cloud APIC 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、Cisco Cloud APIC が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。アップグレード中の Cisco Cloud 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 Cloud APICのアップグレードの事前検証プロセスは、Cisco Cloud 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、DC のアップグレードが進行中であり、DC のアップグレードが完了するまで待ってから Cloud APIC のアップグレードをトリガーすることを示すメッセージが表示されます。

Cisco Cloud 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 Cloud 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。

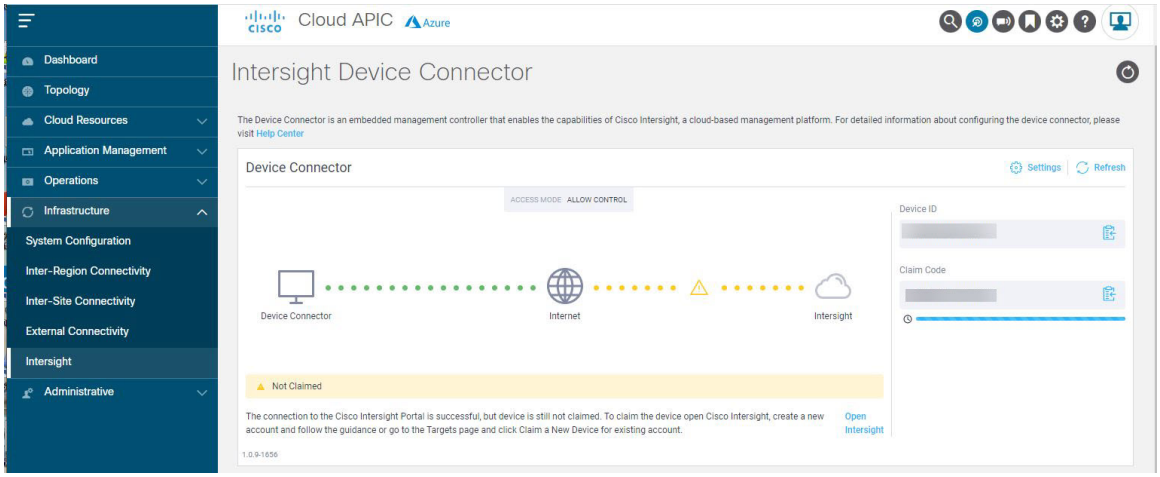
Intersight デバイス コネクタの設定

手順

ステップ 1 Cisco Cloud APIC GUI で、**[インフラストラクチャ（Infrastructure）]** > **[Intersight]**に移動します。

[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（Device Connector）]** から **[インターネット（Internet）]** へ接続する緑色の点線が表示されます。



- **[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]** に接続している赤い点線が表示されている場合は、ステップ 13 （8 ページ） に進んで接続を確認し、問題のトラブルシューティングを行ってください。

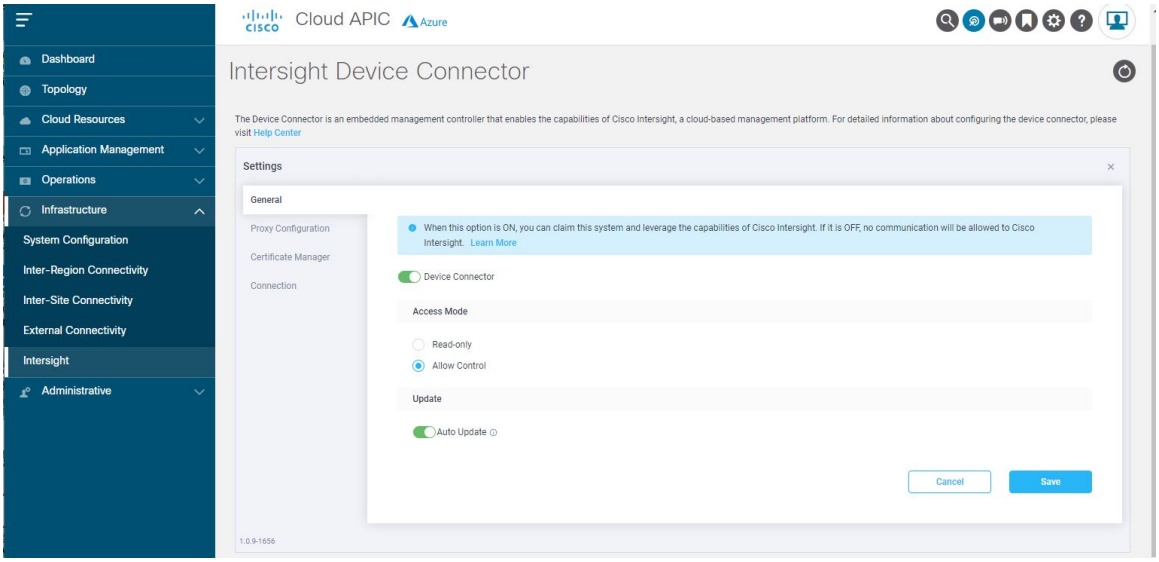
ステップ 2 使用可能な新しいデバイス コネクタ ソフトウェア バージョンがある場合は、この時点でソフトウェアを更新するかどうかを決定します。

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 3 （4 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 （2 ページ）」 を参照してください。

ステップ 3 **[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。



ステップ 4 **[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。無効になっている場合、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。

- [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。
- [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。

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 （2 ページ）」を参照してください。

ステップ 5 **[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。

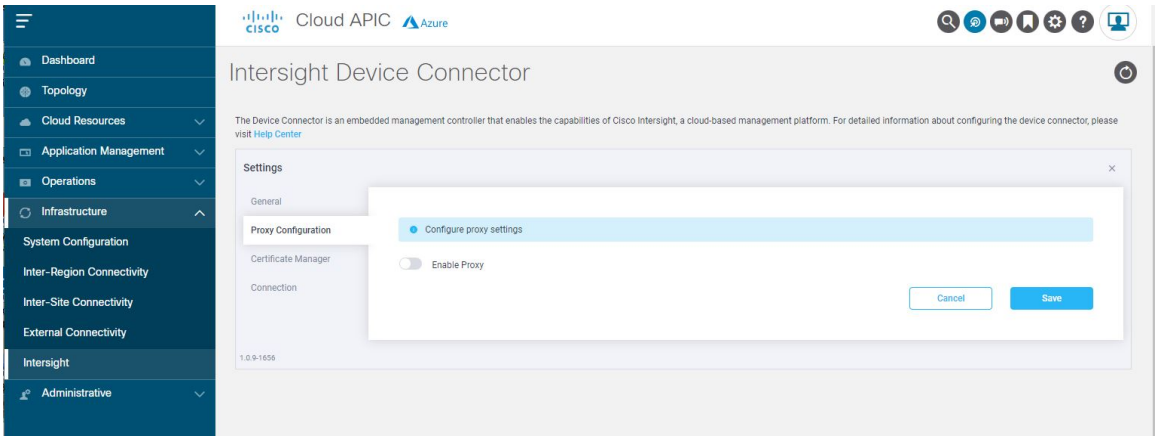
[Intersight デバイス コネクタ（Intersight Device Connector）] の概要ページが再度表示されます。

ステップ 6 必要に応じて、構成プロセスの次の手順に進みます。

- 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設定する場合は、ステップ 7 （5 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 10 （7 ページ） に進みます。
- 接続を確認する場合は、ステップ 13 （8 ページ） に進みます。

ステップ 7 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。



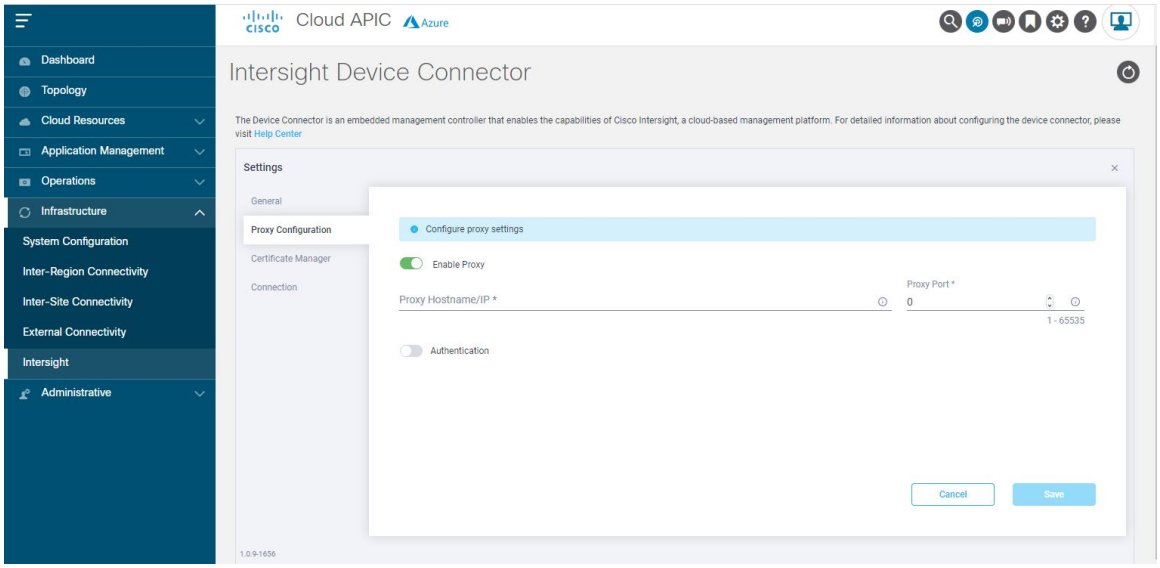
ステップ 8 **[プロキシ設定（Proxy Configuration）]** ページで、次の設定を行います。

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。

[プロキシホスト名/IP（Proxy Hostname/IP）] および **[プロキシポート（Proxy Port）]** フィールドが表示されます。

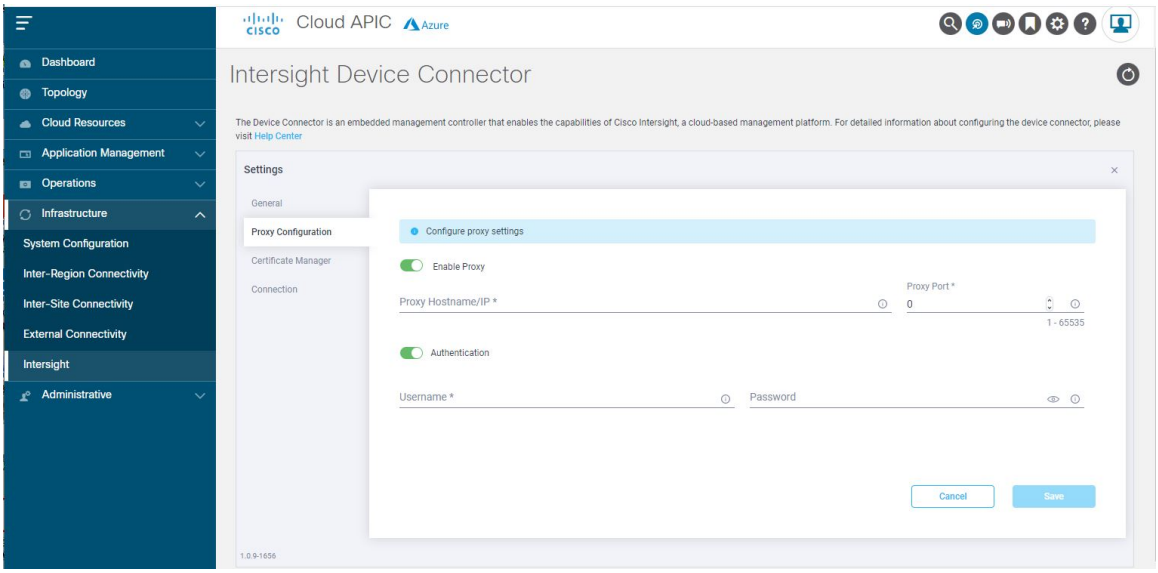


b) **[プロキシホスト名/IP（Proxy Hostname/IP）]** フィールドに、プロキシホスト名または IP アドレスを入力します。

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ます。

[ユーザー名（Username）] フィールドと **[パスワード（Password）]** フィールドが表示されます。



e) 認証用のプロキシのユーザー名とパスワードを入力します。

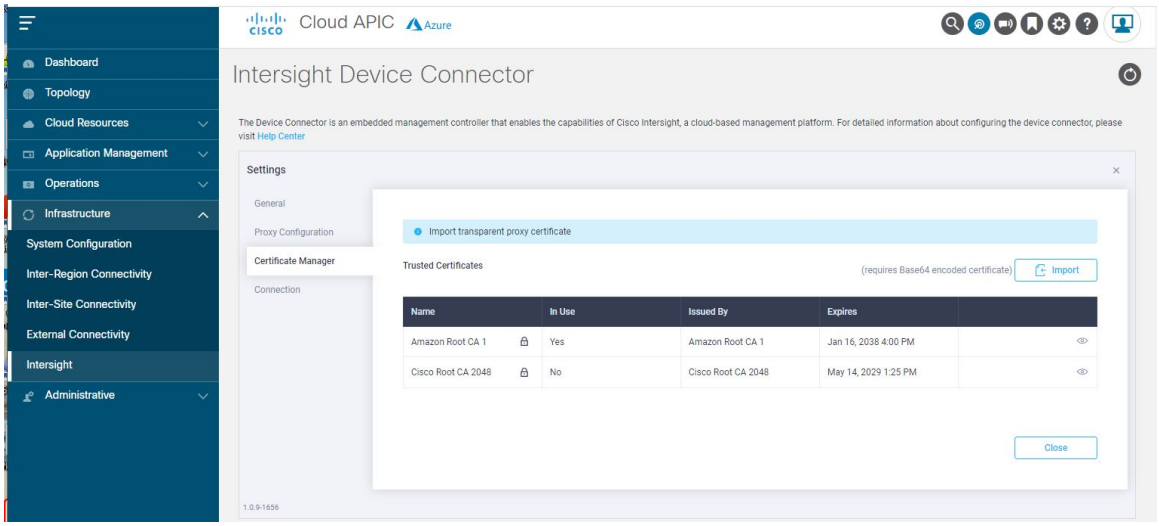
ステップ 9 **[プロキシ設定（Proxy Configuration）]** ページで設定が完了したら、**[保存（Save）]** をクリックします。

[Intersight デバイス コネクタ（Intersight Device Connector）] 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 10 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 11 **[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。

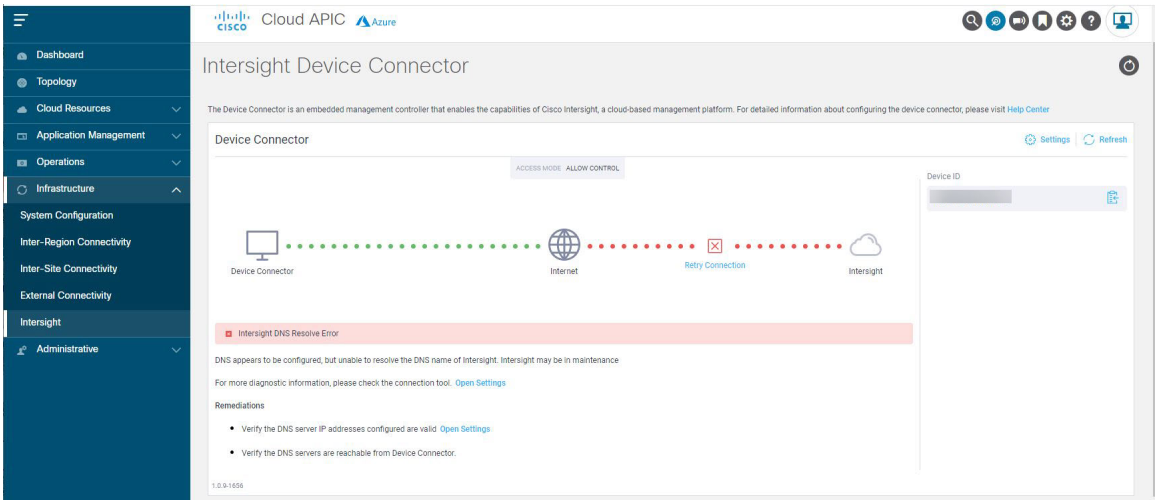
信頼できる証明書のリストから証明書を削除します。ただし、バンドルされている証明書（root+中間証明書）はリストから削除できません。ロック アイコンは、バンドルされた証明書を表します。

ステップ 12 **[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。

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

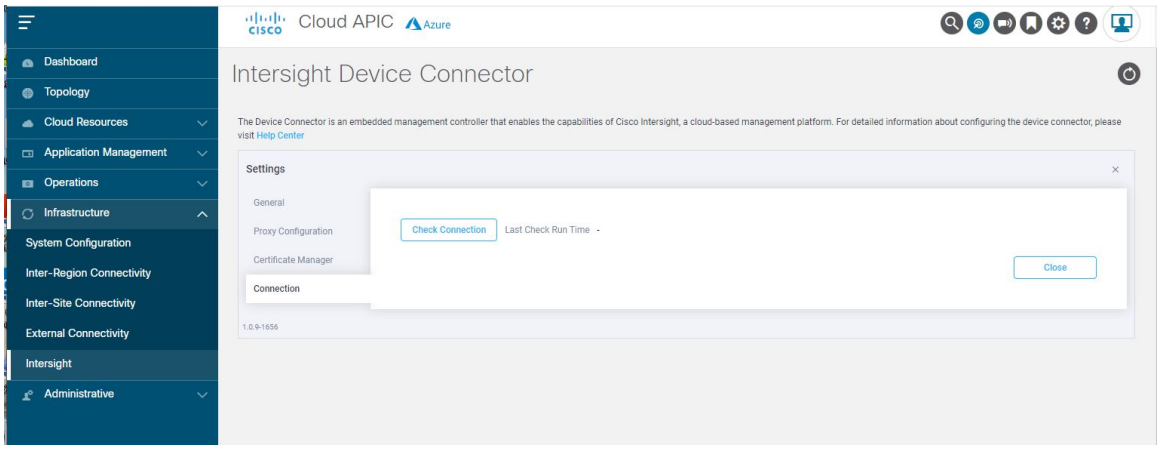
ステップ 13 接続を確認するかどうかを決定します。

次の図に示すように、**[デバイス コネクタ（Device Connector）]** の図で **[インターネット（Internet）]** から **[Intersight]** へ接続する赤色の点線が表示されている場合、**[接続（Connection）]** ページに移動して、接続の問題をトラブルシューティングする必要がある場合があります。

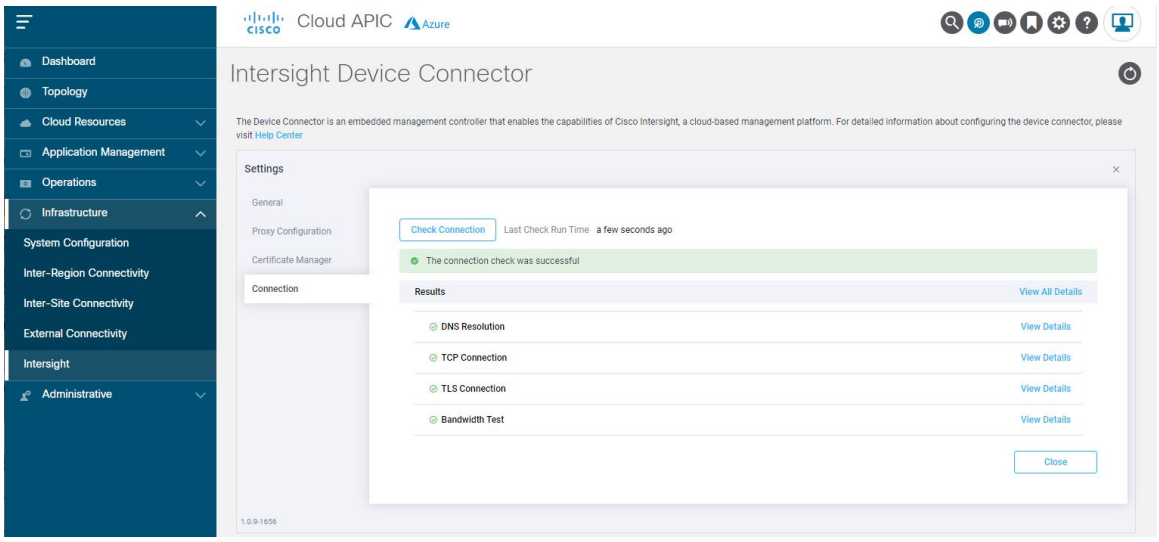


その場合は、**[デバイス コネクタ（Device Connector）]** の図で **[設定ページを開く（Open Settings）]** をクリックして **[接続（Connections）]** に移動するか、**[設定（Settings）]** をクリックしてから **[接続（Connections）]** に移動します。

[接続（Connection）] ページが表示されます。



[接続の確認（Check Connection）] をクリックして接続を確認し、ページに表示される情報を使用して、接続の問題に対処します。



このページでの作業が終了したら、**[閉じる（Close）]** をクリックします。

次のタスク

GUI を使用したデバイスの要求 （10 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 （3 ページ） で提供されている手順を使用して、Cisco Cloud 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 サイトに移動します。

https://www.intersight.com

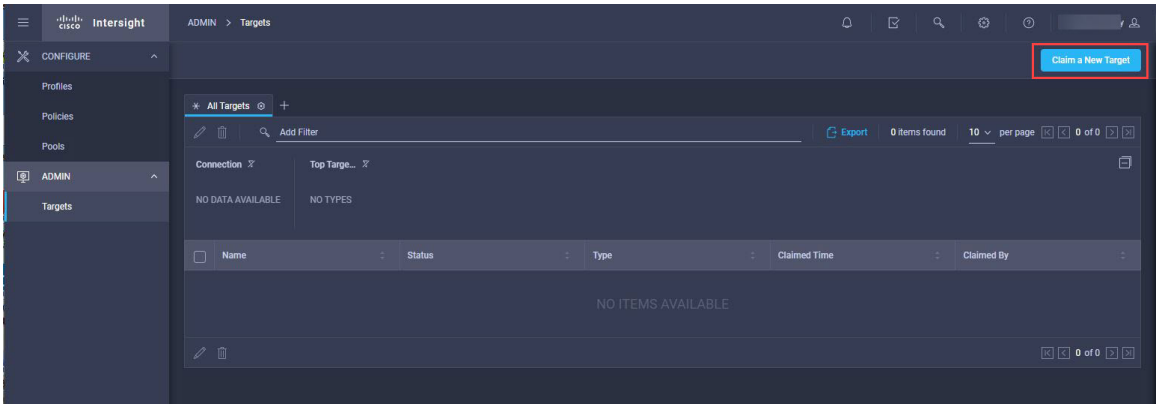
ステップ 2 Cisco Intersight クラウド サイトにログインするために必要な情報を入力します。

ステップ 3 必要に応じて、適切なアカウントとロールを選択します。

[プロファイル（Profiles）] ページが表示されます。

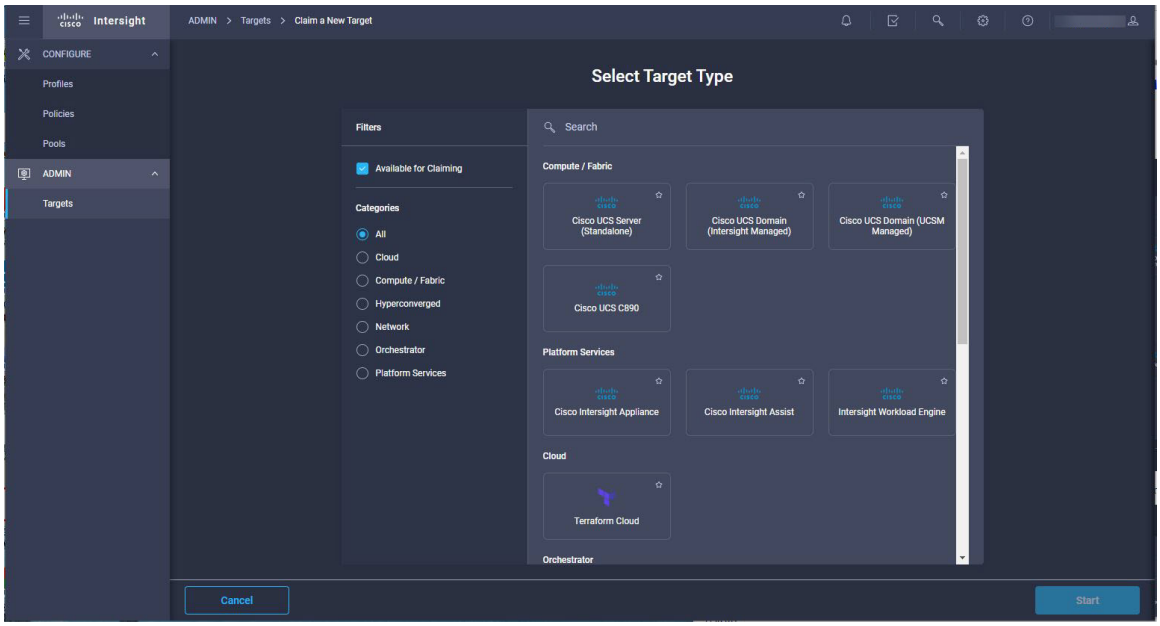
ステップ 4 **[管理（Admin）]** > **[ターゲット（Targets）]** に移動します。

[ターゲット（Targets）] ページが表示されます。

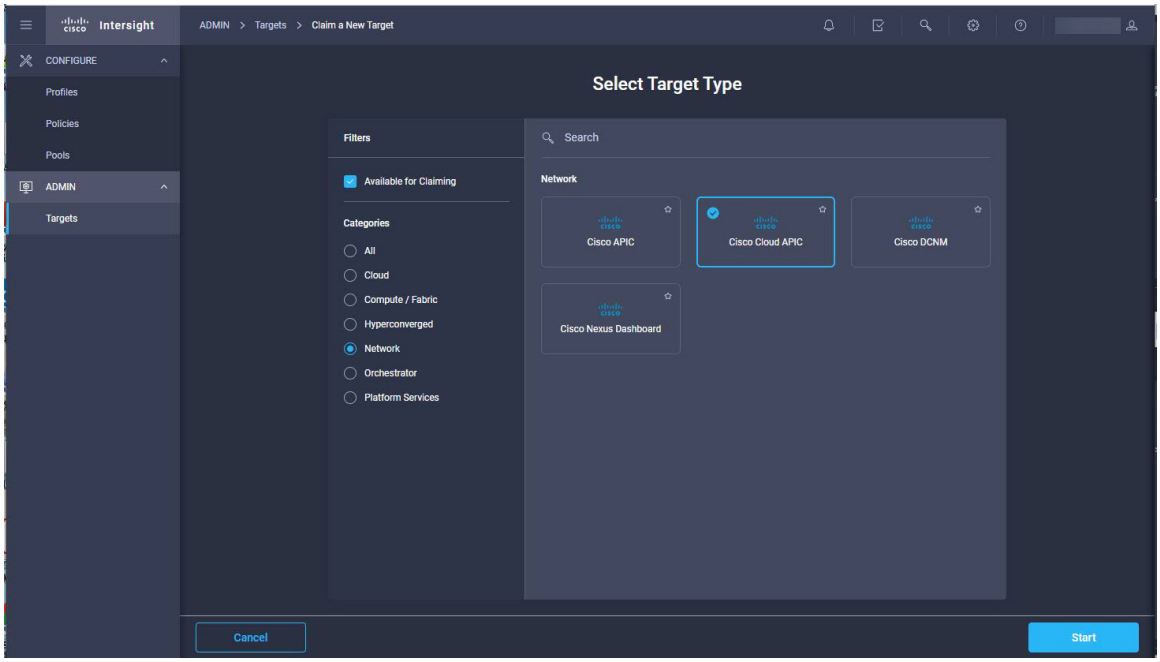


ステップ 5 **[新しいターゲットの要求（Claim a New Target）]** をクリックします。

[ターゲット タイプの選択（Select Target Type）] ページが表示されます。

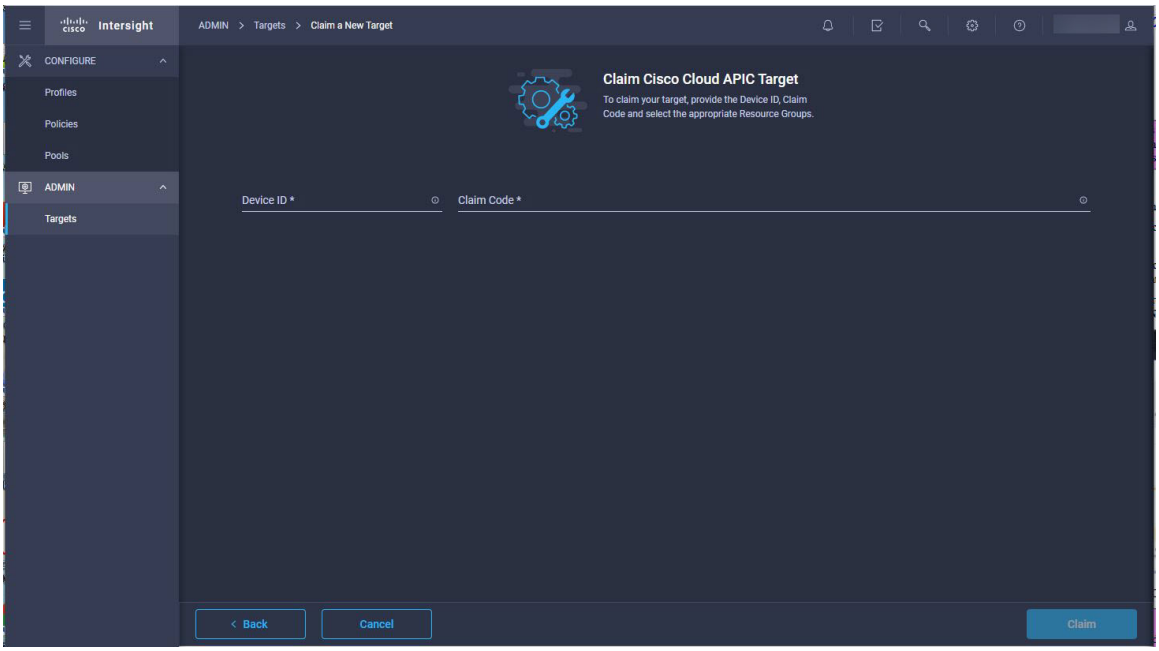


ステップ 6 左側の **[カテゴリ（Categories）]** エリアで、**[ネットワーク（Network）]** をクリックしてターゲットタイプをフィルタリングします。



ステップ 7 **[Cisco Cloud APIC]** ボタンをクリックし、**[開始（Start）]** をクリックします。

[Cisco Cloud APIC ターゲット（Claim Cisco Cloud APIC Target）] ページが表示されます。

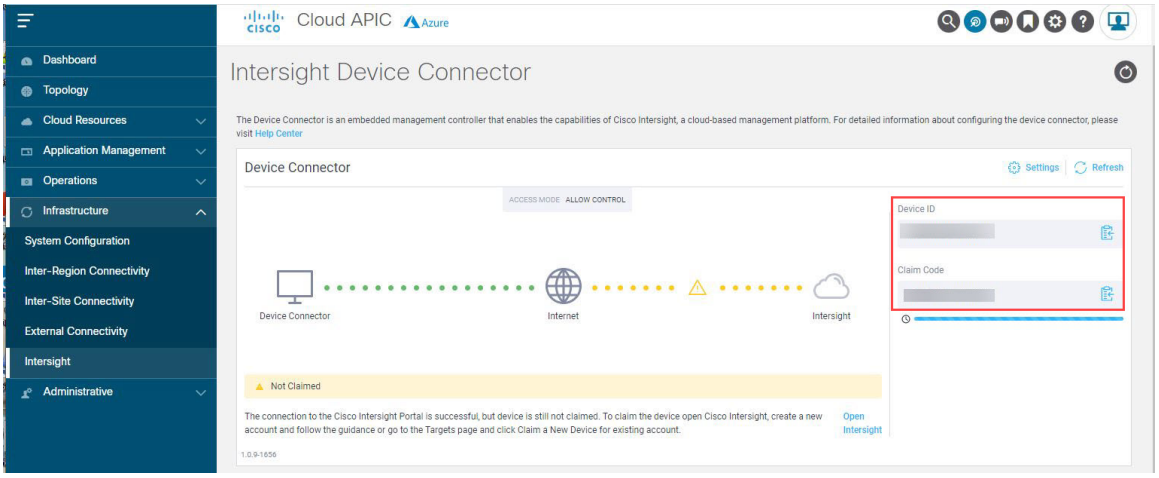


ステップ 8 Cisco Cloud APICサイトで、**[インフラストラクチャ（Infrastructure）]** > **[Intersight]**に戻ります。

[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。

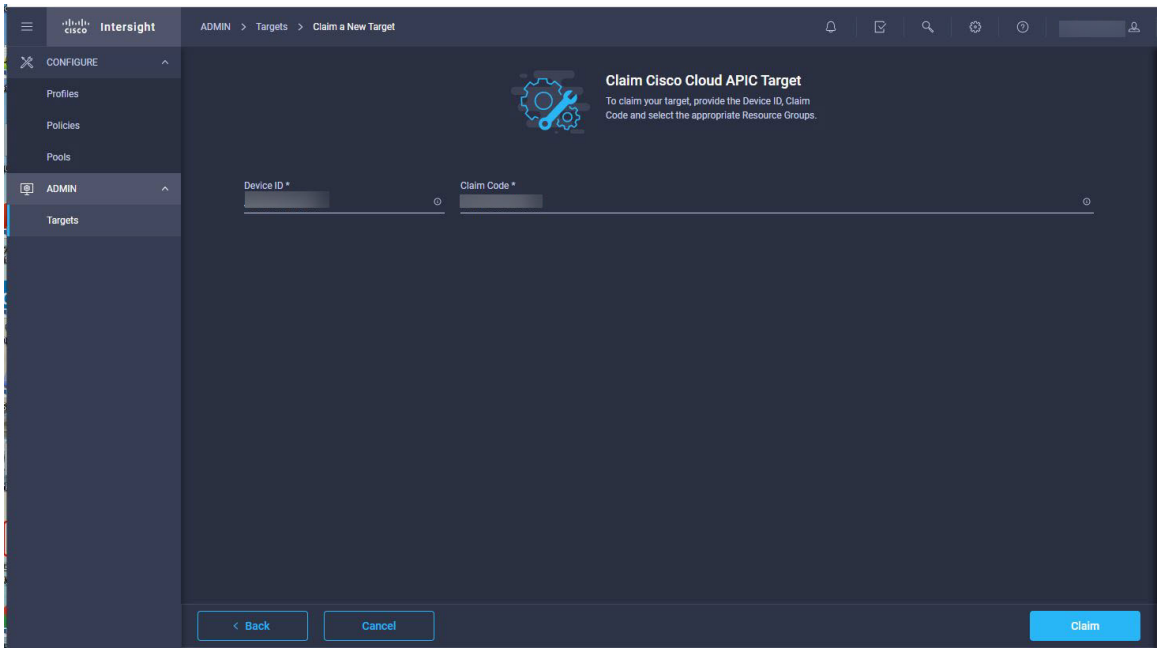
ステップ 9 Cisco Cloud APICサイトから、**[デバイス ID（Device ID）]** および **[要求コード（Claim Code）]** フィールドの値をコピーし、Cisco Intersight クラウド サイトの **[新しいデバイスを要求（Claim a New Device）]** ページの適切なフィールドにペーストします。

Cisco Cloud APIC サイトの各エリアについて、そ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情報をクリップボードにコピーしてから、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。

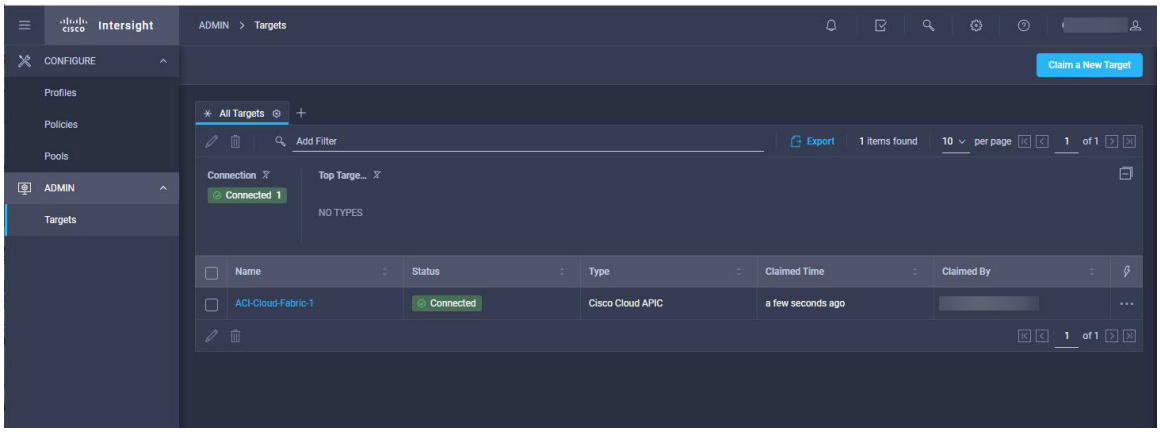


ステップ 10 Cisco Intersight クラウド サイトで、Cisco Cloud APIC ターゲットを要求します。

Cisco Intersight クラウドサイトの **[デバイス ID（Device ID）]** フィールドと **[要求コード（Claim Code）]** フィールドに Cisco Cloud APIC 値をペーストしたら、ページの右下のエリアにある **[要求（Claim）]** をクリックします。

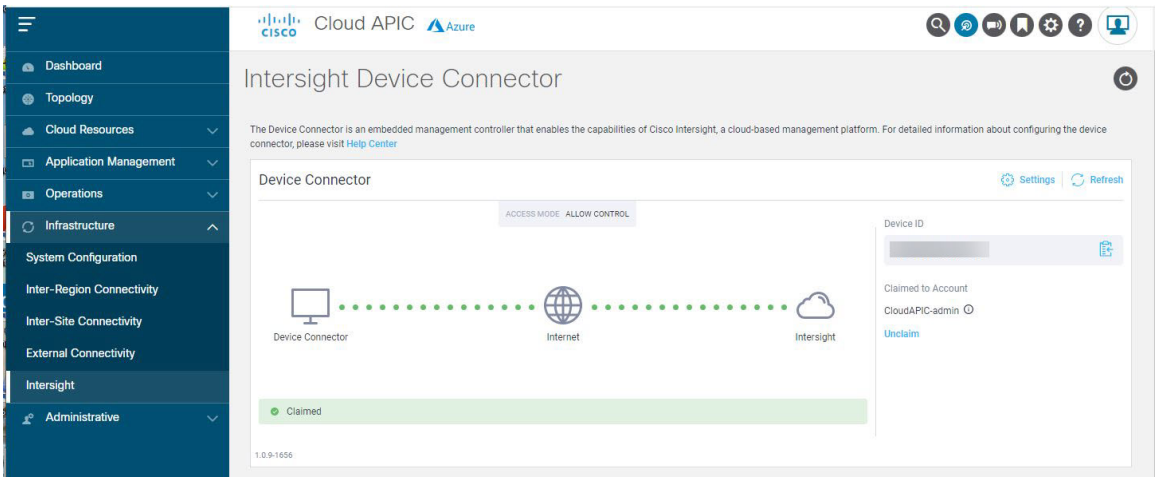


[ターゲット（Targets）] ページが再び表示され、表に Cisco Cloud APIC が表示され、ステータス列に **[接続済み（Connected）]** が表示されます。



ステップ 11 Cisco Cloud 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。

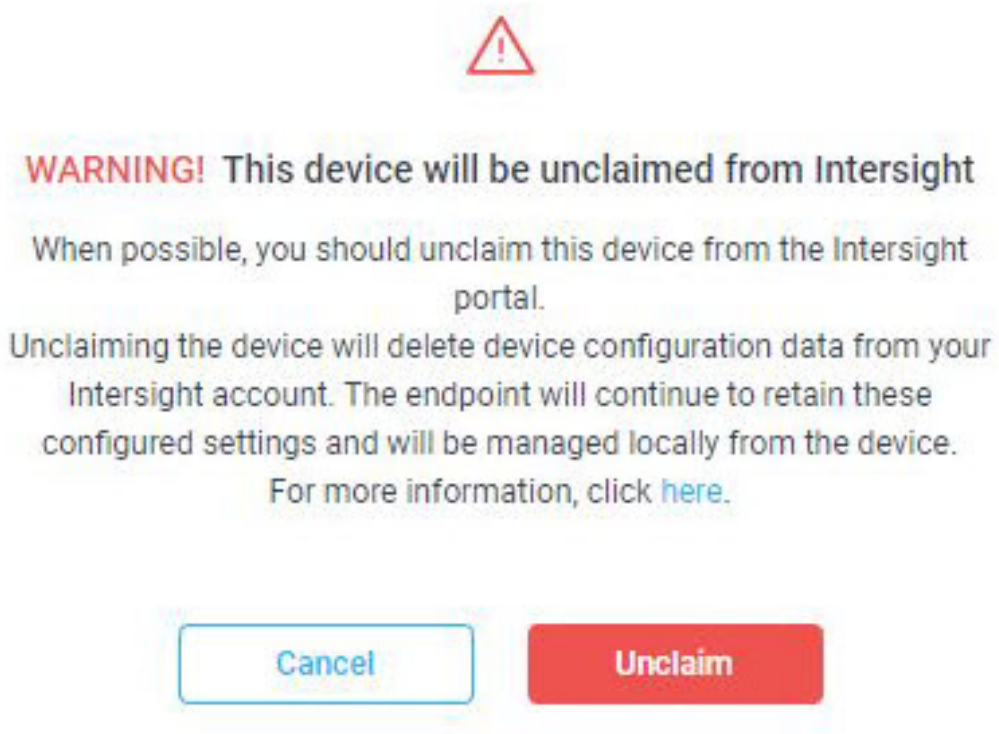
[デバイス コネクタ（Device Connector）] の図に **[インターネット（Internet）]** と **[Intersight]** を接続する緑色の点線が描かれ、図の下に **[要求済み（Claimed）]** という文字が表示されます。



（注） Cloud APIC GUI で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）]** をクリックします。

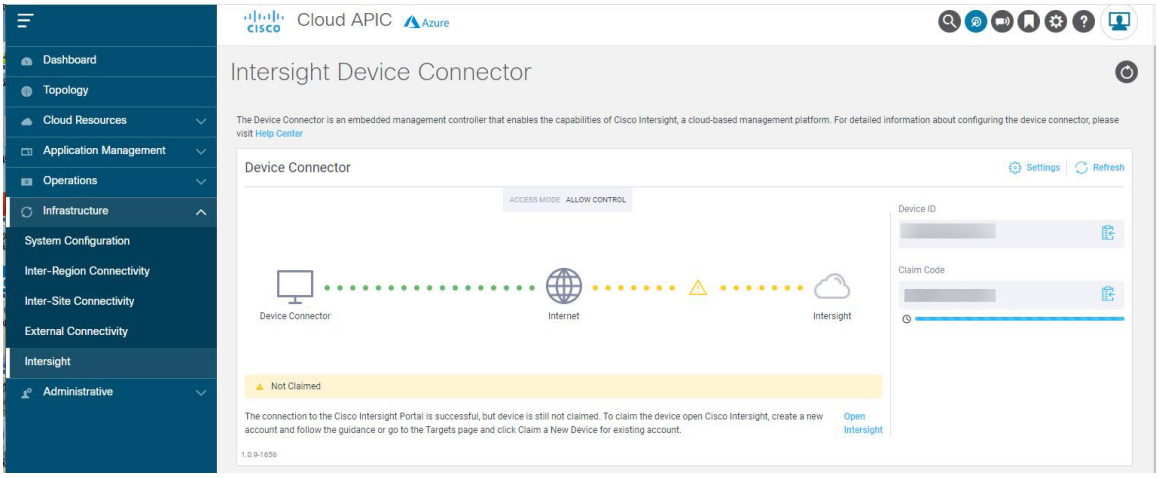
何らかの理由でこのデバイスの要求を取り消す場合は、Cisco Cloud APIC GUI の **[Intersight デバイス コネクタ（Intersight Device Connector）]** ページで **[要求解除（Unclaim）]** リンクを見つけて、そのリンクをクリックします。

デバイスの要求を取り消すかどうかを確認するポップアップ ページが表示されます。

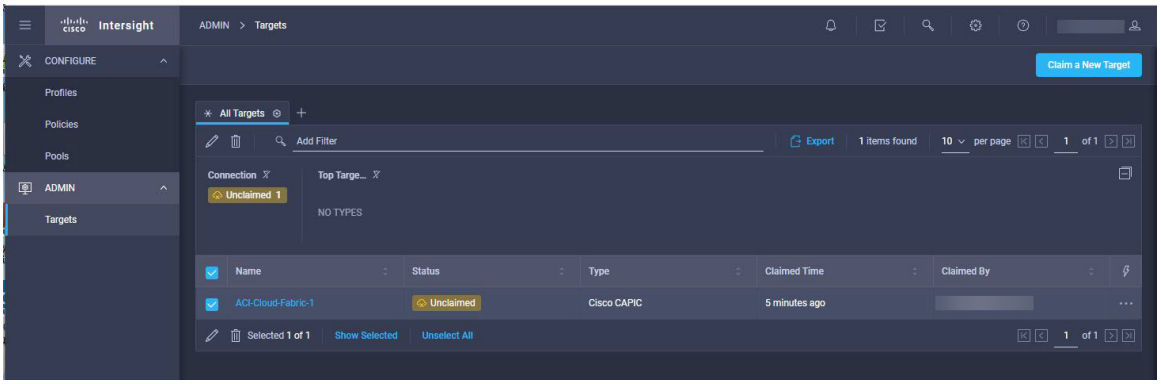


もう一度 **[要求解除（Unclaim）]** をクリックして、このデバイスの要求を取り消すことを確認します。

- Cisco Cloud APIC GUI の **[Intersight デバイス コネクタ（Intersight Device Connector）]** ページで、ステータスが **[要求しない（Not Claimed）]** に変わります。



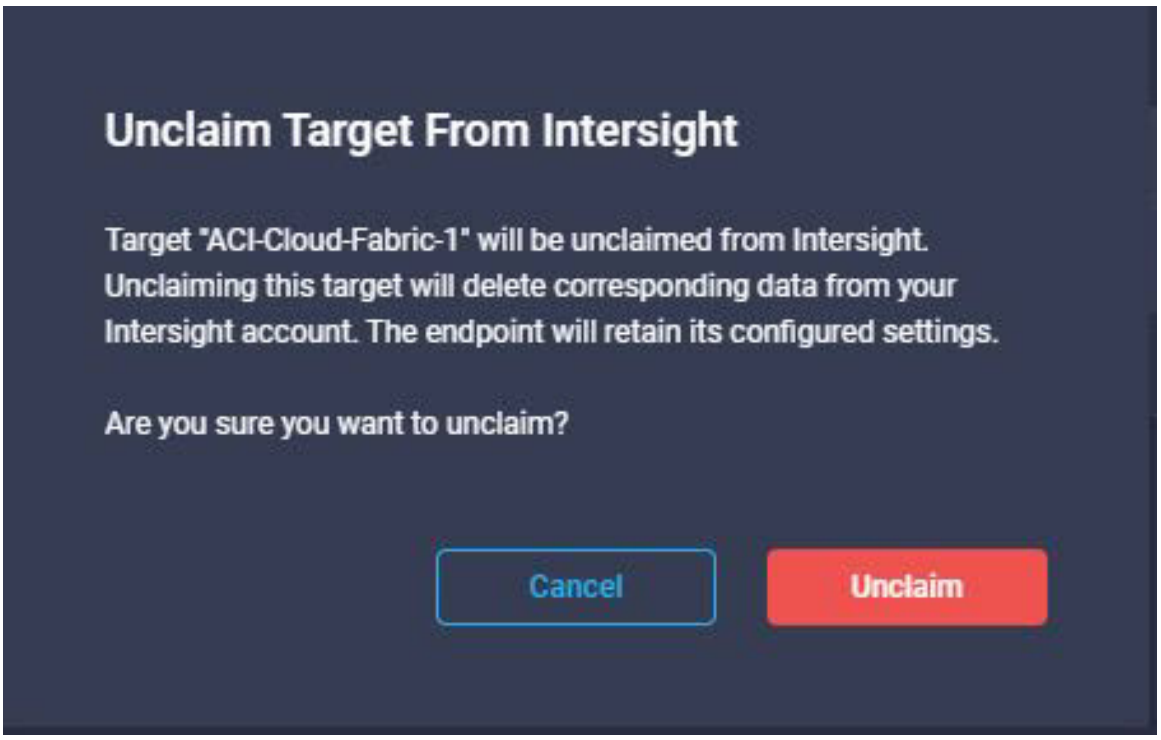
- Cisco Intersight クラウド サイトの **[ターゲット（Target）]** ページで、ステータスが **[未要求（Unclaimed）]** に変わります。



次に、必要に応じて、Cisco Intersight クラウド サイトの **[ターゲット（Target）]** Cisco Cloud APIC ページの横にあるボックスをクリックし、ゴミ箱アイコンをクリックしてそのターゲットを削除できます。

（注） また、Cisco Intersight クラウド サイトの **[ターゲット（Target）]** Cisco Cloud APIC ページにある の横にあるボックスをクリックしてからゴミ箱アイコンをクリックすることにより、Cisco Cloud APIC GUI でアクションを実行することなく、デバイスの要求を取り消してターゲットを 1 つのステップで削除することもできます。

デバイスの要求を取り消すかどうかを確認するポップアップ ページが表示されます。



もう一度 **[要求解除（Unclaim）]** をクリックして、このデバイスの要求を取り消すことを確認します。

【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。

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。