Cisco IWAN Application on APIC-EM ユーザ ガイド リリース 1.4.1

2017 年 3 月 17 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は
当社の Web サイト
www.cisco.com/go/offices

【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、米国シスコシステムズ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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2017Cisco Systems, Inc. All rights reserved.

CONTENTS

はじめに

この前書きは、次の項で構成されています。

製品情報

Cisco IWAN アプリケーション（IWAN アプリ）は、Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（APIC-EM）内で動作します。1.3.2 よりも前のリリースでは、IWAN アプリは APIC-EM にバンドルされていました。1.3.2 からは、APIC-EM とは別にリリースされ、APIC-EM に手動でインストールします。IWAN アプリは、これまでと同様に APIC-EM の必須部分です。

対象読者

このガイドは、次の 1 つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
1	新機能および変更された機能に関する情報	このマニュアルに記載されている Cisco IWAN アプリケーションのリリース固有の新規機能と変更された機能を要約して説明します。
2	概要	シスコ インテリジェント WANについて紹介し、シスコ インテリジェント WAN アプリケーションへのアクセス方法を説明します。
3	配置	Cisco APIC-EM 内での Cisco IWAN アプリケーションの導入について説明します。
4	ハブ サイトの管理	ハブ サイトを設定してセットアップするウィザードの手順を示します。
5	ブランチ サイトの管理	ブランチ サイトを追加してプロビジョニングする手順、およびサイトのステータス情報を表示する手順を示します。
6	デバイスの管理	各サイトには 1 つ以上のデバイスを関連付けることができます。IWAN アプリは、ネットワーク内のデバイスに対するバッチ CLI コマンドの実行を有効化するカスタム設定機能など、デバイスを個別に管理する手段を提供します。
7	アプリケーション ポリシーの管理	アプリケーション帯域幅に基づいてアプリケーション ポリシーを分類および定義する手順を示します。
8	サイトのモニタリングとトラブルシューティング	サイトをモニタおよびトラブルシューティングする手順を示します。
9	バックアップと復元、リカバリ、および削除	バックアップと復元の方法、シスコ インテリジェント WANの設定のリカバリ方法、およびハブ、中継ハブ、ブランチ サイトの削除方法を示します。
A	ブラウンフィールド検証メッセージの説明	ブランフィールド デバイス検証時に発生するエラー メッセージと警告メッセージの一覧が記載されています。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。

{x | y | z }	必ずいずれか 1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符(!)またはポンド記号(#)がある場合には、コメント行であることを示します。

(注) 「*注釈*」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「*問題解決に役立つ情報*」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス 「*時間の節約に役立つ操作*」です。記述されている操作を実行すると時間を節約できます。

警告 **安全上の重要事項**

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

警告 **このシンボルを使ったステートメントは、追加情報および規制要件または顧客要件に準拠するためのものです。**

関連資料

マニュアル	説明
Cisco IWAN Application on APIC-EM リリース 1.4.0 ユーザ ガイド	このマニュアル シスコ インテリジェント WANアプリケーションの導入方法、設定方法、使用方法が記載されています。
Cisco IWAN Application on APIC-EM Release Notes	Cisco APIC-EM 製品および シスコ インテリジェント WAN のすべてのリリース ノートの一覧が記載されています。
Cisco IWAN Technology Design Guides	Cisco Validated Designs for シスコ インテリジェント WANについて説明している設計ガイド。
Cisco APIC-EM Documentation Roadmap	すべての Cisco APIC-EM 製品のマニュアルの一覧が記載されています。このドキュメントは、コントローラとそのアプリケーションを最大限に活用できるようにすることを目的としています。You can find links to all of the documentation, including シスコ インテリジェント WANこちらのリンクから: http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html
Cisco Prime Infrastructure Release Notes	Cisco Prime Infrastructure 製品のすべてのリリース ノートの一覧が記載されています。
Cisco Prime Infrastructure 3.1 Documentation	導入ガイドおよびその他の Cisco Prime Infrastructure のドキュメントへのリンクです。
LiveAction	LiveAction IWAN のトレーニングとドキュメントがあります。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

新機能および変更された機能に関する情報

Cisco IWAN アプリ リリース 1.4.1 では、リリース 1.4.0 リリースでの未解決の問題が修正されます。

CSCvd43811：SiteID の不一致により、AR エラーでハブ プロビジョニングの障害が発生

リリース 1.4.0 の新機能

バグ修正を除けば、リリース 1.4.1 は 1.4.0 と同一です。次の表は、Cisco IWAN アプリケーション リリース1.4.0 の新規機能と変更された機能の概要を示しています。

表 1-1　リリース 1.4.0 の新機能および変更された機能に関する情報

機能	説明	参照先
0 日目と N 日目に QoS 帯域幅を変更	ハブまたはブランチ サイトのプロビジョニング時（0 日目）に、優先度が QoS クラスのモデルと他のクラスのモデルにユーザが定義した割合で帯域幅を割り当てる機能。	**ハブ** サイト： ウィザードの手順 4：サービス プロバイダーの設定（4-10 ページ） **ブランチ サイト（グリーンフィールド）**： 次の項で、[Configure WAN Cloud] ダイアログボックスの [Service Profile] フィールドを参照してください。 グリーンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング（5-5 ページ） **ブランチ サイト（ブラウンフィールド）**： 次の項で、[Configure WAN Cloud] ダイアログボックスの [Service Profile] フィールドを参照してください。 ブラウンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング（5-11 ページ）。
	ハブまたはブランチ サイトのプロビジョニング後（N 日目）に、優先度が QoS クラスのモデルと他のクラスのモデルに対するユーザ定義帯域幅の割合を変更する機能。	ハブ サイトの QoS 帯域幅の割合の変更（4-23 ページ） ブランチ サイトの QoS 帯域幅の割合の変更（5-27 ページ）
N 日目にハブまたはスポーク サイトの WAN 帯域幅を更新	ハブまたはスポーク（ブランチ）サイトのプロビジョニング後（「N 日目」）に、アップロードまたはダウンロードの WAN 帯域幅を変更する機能が導入されました。	プロビジョニング済みハブ サイトの WAN 帯域幅の更新（4-22 ページ） プロビジョニング済みブランチ サイトの WAN 帯域幅の更新（5-24 ページ）
N 日目にスポーク サイトの WAN IP を更新	サイトのプロビジョニング後（「N 日目」）に、スポーク（ブランチ）サイトに設定されている WAN IP、マスク、またはネクスト ホップを変更する機能が導入されました。	プロビジョニング済みブランチ サイトの WAN IP パラメータの更新（5-25 ページ）
ハブ サイトで複数の DHCP サーバをサポート	ハブ サイトに最大 5 つの DHCP サーバを追加する機能。	ウィザードの手順 1：システム設定項目の設定（4-2 ページ）

表 1-1　リリース 1.4.0 の新機能および変更された機能に関する情報（続き）

機能	説明	参照先
Cisco ISR4000 シリーズ ルータに対する 4G のサポート	ブランチ サイトの Cisco ISR4000 シリーズ ルータに対してセルラー/4G インターフェイスをサポート。	グリーンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング（5-5 ページ） ブラウンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング（5-11 ページ）
カスタム アプリケーションの削除	ユーザによって NBAR2 カスタム アプリケーションを削除する機能。	NBAR2 カスタム アプリケーションの削除（7-4 ページ）
NAT の背後のスポーク	NAT の背後のスポーク サイトをサポート。	ブランチ サイトの管理
NAT の背後の APIC-EM	NAT の背後の APIC-EM コントローラをサポート。この機能は、以前はグリーンフィールド サイトに対してサポートされていましたが、本バージョンではブラウンフィールド サイトに対してもサポートされるようになりました。	NAT による IWAN アプリの動作（5-2 ページ）
NBAR2 Protocol Pack 27.0.0 のサポート	IWAN アプリ 1.4.0 では NBAR2 Protocol Pack 27.0.0 が使用されます。このアップグレードにより、新しいアプリケーション プロトコルが提供され、既存のプロトコルが改善されています。 旧バージョンの IWAN アプリで定義された NBAR2 カスタム アプリケーションがルータにあり、カスタム アプリケーションの名前が Protocol Pack 27.0.0 で提供される新しいプロトコルと競合する場合は、カスタム アプリケーションの名前が次のように変更されます。 c_<元のカスタム アプリケーションの名前>	アプリケーション ポリシーの管理
カスタム設定	IWAN ネットワーク内のデバイスで CLI 設定コマンドを実行するメカニズムを提供します。	デバイスの管理
スポーク サイトでの ASR1000 シリーズ ルータのサポート	スポーク サイトにおける複数の Cisco ASR 1000 シリーズ ルータのサポートが追加されました。詳細については、リリース ノートを参照してください。	Cisco IWAN Application on APIC-EM Release Notes, Release 1.4.0
Cisco IOS XE Denali 16.x のサポート	Cisco IOS XE Denali 16.3.3 を実行するルータをサポート。すべてのソフトウェア要件については、リリース ノートを参照してください。	Cisco IWAN Application on APIC-EM Release Notes, Release 1.4.0

CHAPTER 2

概要

この章の内容は、次のとおりです。

Cisco IWAN アプリケーションについて

Cisco Intelligent WAN アプリケーション（IWAN アプリ）は、Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（APIC-EM）で動作します。

シスコ インテリジェント WANは、ビジネス ポリシーとアプリケーション規則に基づくアプリケーション中心のアプローチにより、Software Defined Networking（SDN）をブランチ サイトに拡張します。ネットワーク全体に渡って一元管理し分散的に適用するためのツールを IT 部門に提供します。

シスコ インテリジェント WANは、直感的なブラウザベースのユーザ インターフェイスによって導入を自動化します。ルータ CLI コマンドを使用することなく、新しいルータをより迅速にプロビジョニングできます。

ビジネス プライオリティは、シスコのベスト プラクティスと検証済みの設計に基づいてネットワーク ポリシーに変換されます。シスコ インテリジェント WANは、自動化とシンプルな事前定義済みワークフローによって、DMVPN、PKI、AVC、QoS、PfR などの高度なネットワーク サービスの設定に要する時間を短縮します。

アプリケーション中心のアプローチには次のような利点があります。

- 運用コストの削減：シスコ インテリジェント WANを使用することで、運用コストを削減しながら、あらゆる接続で IT による比類のないユーザ エクスペリエンスを実現できます。
- IT 運用のシンプル化：シスコ インテリジェント WANはソフトウェア ベースのコントローラ モデルを使用して、管理タスクを自動化および一元化し、より迅速かつ正常な展開を実現します。
- ネットワークの複雑さの軽減：シスコ インテリジェント WANは Cisco APIC-EM を活用してネットワーク デバイスを 1 つのシステムに抽象化することにより、ネットワークの複雑さを軽減してインフラストラクチャの集中プロビジョニングを実現し、アプリケーションやサービスの展開を高速化します。

シスコ インテリジェント WANアプリケーションにアクセスするためのワークフロー

表 2-1　　シスコ インテリジェント WANにアクセスするための基本的ワークフロー

いいえ。	Action	参照先
1	Cisco APIC-EM を導入する。	Cisco APIC-EM の導入（3-2 ページ）
2	IWAN アプリケーションの最新バージョンをインストールする。	Cisco IWAN アプリケーションのインストールまたはアップグレード（3-2 ページ）
3	Cisco APIC-EM にログインして シスコ インテリジェント WANアプリケーションにアクセスする。	Cisco IWAN アプリケーションへのアクセス（2-2 ページ）
4	シスコ インテリジェント WANアプリケーション ツールを使用する。	• ハブ サイトの管理 • ブランチ サイトの管理 • アプリケーション ポリシーの管理 • サイトのモニタリングとトラブルシューティング

Cisco IWAN アプリケーションへのアクセス

Cisco APIC-EM の GUI から シスコ インテリジェント WANアプリケーションにアクセスします。

手順

ステップ 1　Google Chrome または Mozilla Firefox を使用して、Cisco APIC-EM の IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

ステップ 2　ユーザ名とパスワードを入力して、[Log In]をクリックします。

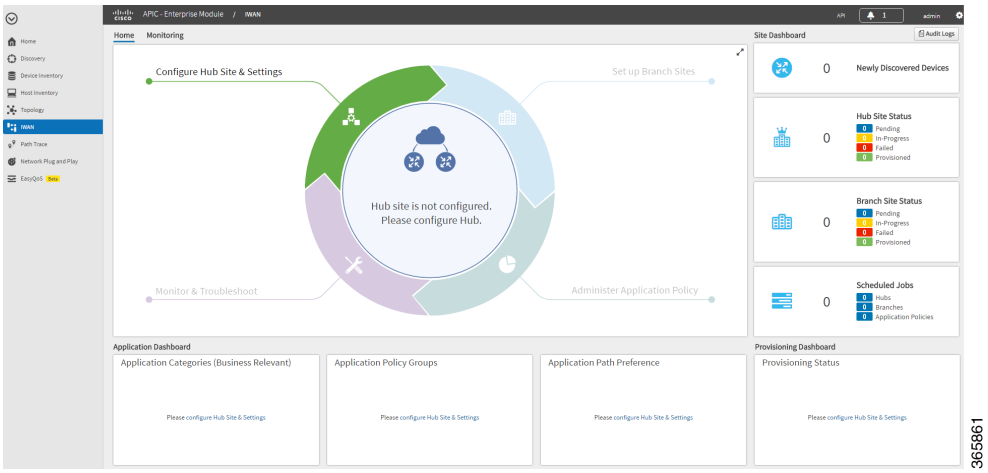
ステップ 3　（初めてログインした場合）テレメトリ情報の開示について確認し、[Confirm]をクリックします。Cisco APIC-EM GUI が表示されます。

ステップ 4　Cisco APIC-EM GUI の左ナビゲーション ペインで、[IWAN]をクリックします。シスコ インテリジェント WANアプリケーションのホームページが表示されます。シスコ インテリジェント WANアプリケーションのホームページ（2-2 ページ）を参照してください。

シスコ インテリジェント WANアプリケーションのホームページ

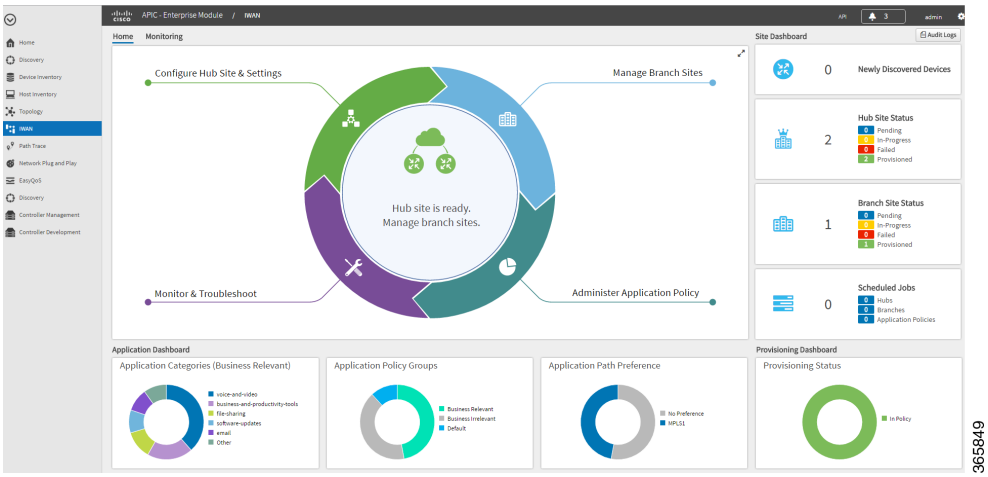
初めてログインした場合は、シスコ インテリジェント WANアプリケーションのホームページに、ワークフローをシンプルにするためのウィザード ベースの設定方法が示されます。自動ウィザードのわかりやすい手順に従って、セットアップと設定のプロセスを実行できます。

図 2-1　Cisco IWAN アプリのホーム ページ:新しいシステムへの最初のログイン



シスコ インテリジェント WANを設定してプロビジョニングすると、ホームページに追加情報が表示されます。たとえば、ハブとブランチのプロビジョニングのステータス、デバイスのステータス、アプリケーションのステータスなどが表示されます（次の図を参照）。

図 2-2　Cisco IWAN アプリのホームページ:プロビジョニング後



タスク エリア	機能	参照先
ハブ サイトの設定およびセットアップ（Configure Hub Site & Settings）	ウィザード:ハブ サイトの設定およびセットアップ。	ハブ サイトの管理（4-1 ページ）
ブランチ サイト管理（Manage Branch Sites）	ブランチ サイトの追加とプロビジョニング、およびサイトのステータスの表示。	ブランチ サイトの管理（5-1 ページ）
アプリケーション ポリシー管理	アプリケーションの帯域幅に基づき、アプリケーション ポリシーを分類して定義。	アプリケーション ポリシーの管理（7-1 ページ）

タスク エリア	機能	参照先
モニタとトラブルシューティング（Monitor & Troubleshoot ）	サイトのモニタとトラブルシューティング。	サイトのモニタリングとトラブルシューティング（8-1 ページ）
アプリケーション ダッシュボード（Application Dashboard）	以下に関する情報を一目でわかるように表示。 • Application Categories • アプリケーション ポリシー グループ（Application Policy Groups） • アプリケーション パスのプリファレンス（[Application Path Preference]）	—
プロビジョニング ダッシュボード（Provisioning Dashboard）	サイトのプロビジョニングのステータス	—
サイト ダッシュボード（Site Dashboard）	以下に関する情報を一目でわかるように表示。 • 新たに検出されたデバイス（[Newly Discovered Devices]） • ハブ サイトのステータス（[Hub Site Status]） • ブランチ サイトのステータス（[Branch Site Status]） • スケジュール済みジョブ（[Scheduled Jobs]）	—

CHAPTER 3

導入

この章の内容は、次のとおりです。

Cisco IWAN Application on APIC-EM

概要で説明しているように、Cisco IWAN アプリケーション（IWAN アプリ）は、Cisco APIC-EM を介して、APIC-EM ブラウザベースのインターフェイス内でツールとして動作します。

APIC-EM のリリース スケジュールからの分離

Cisco IWAN アプリ リリース 1.3.2 では、IWAN アプリのリリースに関する新たなアプローチが導入されました。本リリースから以下のようになります。

- IWAN アプリは APIC-EM のリリース スケジュールから切り離され、APIC-EM のインストールやアップグレードのプロセスからも切り離されました。
- IWAN アプリのリリース番号は、APIC-EM のリリース番号とは関係がなくなりました。
- IWAN アプリを APIC-EM とは別にダウンロードし、APIC-EM の [App Management] ページを使用してインストールしたりアップグレードしたりします。Cisco IWAN アプリケーションのインストールまたはアップグレード（3-2 ページ）を参照してください。

APIC-EM の必須部分

リリース スケジュールおよびインストールは APIC-EM から独立して扱われることになりましたが、IWAN アプリは引き続き APIC-EM の必須部分であり、これまでと同様に APIC-EM GUI に表示されます。

システム要件

APIC-EM のシステム要件は、引き続き IWAN アプリに適用されます。

リリース ノートには、APIC-EM および Cisco Prime Infrastructure のバージョンを含めて、IWAN アプリのリリースと互換性があるソフトウェアが記載されています。

Cisco APIC-EM の導入

シスコ インテリジェント WANアプリケーションには Cisco APIC-EM のグラフィカル ユーザ インターフェイス（GUI）からアクセスします。IWAN アプリを使用するには、まず Cisco APIC-EM を導入する必要があります。

Cisco APIC-EM は、サーバ（ベアメタル ハードウェア）または VMware vSphere 環境の仮想マシンに導入できます。Cisco APIC-EM はシングル ホストとして導入することも、複数ホスト環境に導入することもできます。

APIC-EM の導入ガイドの手順に従って Cisco APIC-EM を導入してください。導入ガイドは APIC-EM の [Install and Upgrade Guides] ページで入手できます。

Cisco IWAN アプリケーションのインストールまたはアップグレード

IWAN アプリケーションをインストールまたはアップグレードする前に

IWAN アプリをインストールする前に、以下を実行してください。

- （APIC-EM をまだインストールしていない場合）APIC-EM の導入ガイドの手順に従って Cisco APIC-EM をインストールします。導入ガイドは APIC-EM の [Install and Upgrade Guides] ページで入手できます。必要に応じて、必要なパッチをインストールして APIC-EM を適切なリリースにアップグレードします。

  APIC-EM インストール パッケージの一部のバージョンには、IWAN アプリの旧バージョンが含まれていることがあります。

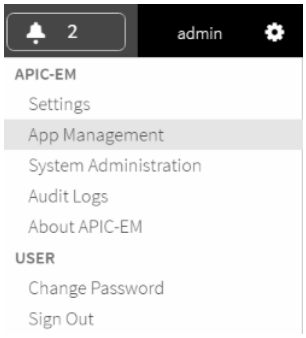
- Cisco APIC-EM のリリース（リリース1.4.1 以降が必要）およびネットワーク内の他の要素のソフトウェア バージョンが、インストールする IWAN アプリのバージョンと互換性があることを確認します。詳細については、リリース ノートを参照してください。

- **注**：IWAN アプリの以前のリリースからアップグレードする場合、アップグレード後、以前のリリースで実行した操作のログは引き継がれません。

推奨事項

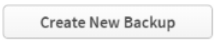
- 現在の APIC-EM 設定のバックアップを作成してください。バックアップおよび復元の詳細については、APIC-EM のマニュアルを参照してください。基本的な手順は以下のとおりです。

  1. APIC-EM で、[Settings]（歯車ボタン）>[App Management] を選択します。



  2. [Backup & Restore]タブを選択します。

  3. [Create New Backup]ボタンをクリックします。



- 以前のリリースの IWAN アプリからアップグレードする場合は、アップグレードする前に IWAN の設定のバックアップを実行します。バックアップと復元、リカバリ、および削除を参照してください。

手順

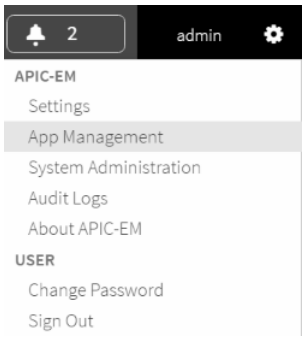
ステップ 1　シスコの [Download Software] ツールを使用して [Policy and Automation Controllers] に移動し、APIC-EM を選択するか、または次の直接リンクを使用します。

https://software.cisco.com/download/type.html?mdfid=286208072&flowid=77162

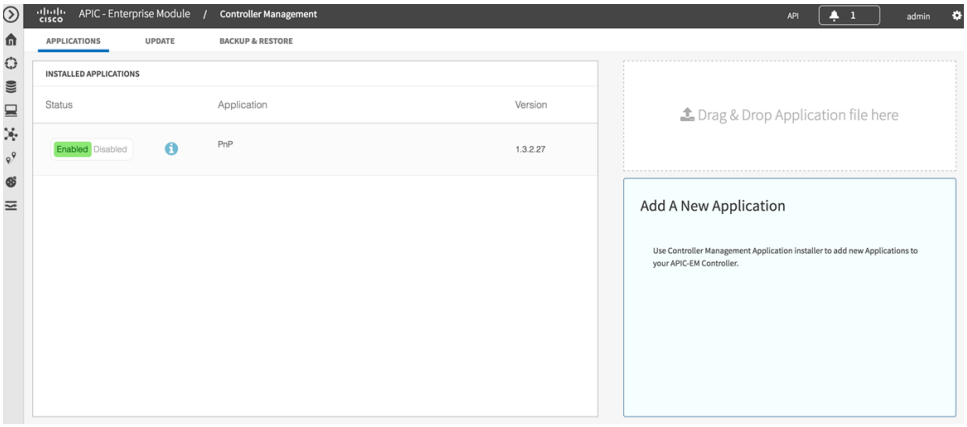
ステップ 2　[IWAN Application Software]オプションを探します。IWAN アプリケーションをダウンロードします。ダウンロードしたファイルの場所をメモします。

ステップ 3　APIC-EM を起動し、[APIC-EM Applications] ページを開きます。

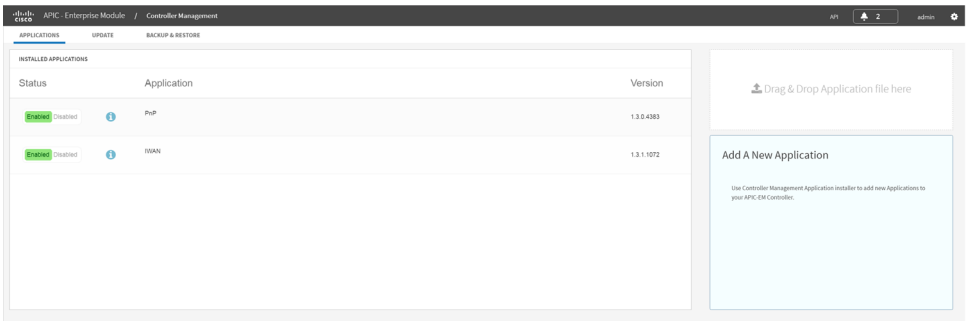
a.　[Settings]（歯車ボタン）>[App Management] を選択します。



b.　[Applications] タブが表示されることを確認します。
（下記の例に示されているのは、IWAN アプリの旧リリースで使用されていた PnP のバージョン番号です）。

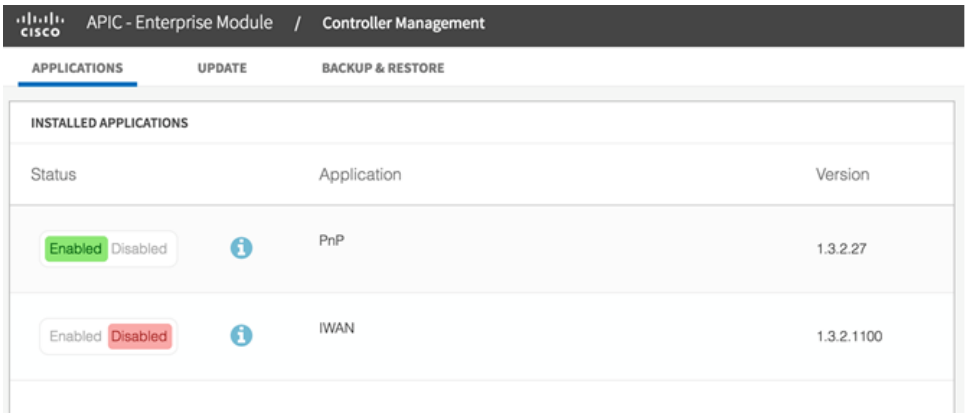


IWAN アプリがインストールされている場合は、そのバージョンが [Installed Applications] リストに表示されます。
（下記の例に示されているのは、IWAN アプリケーションの旧リリースです）。

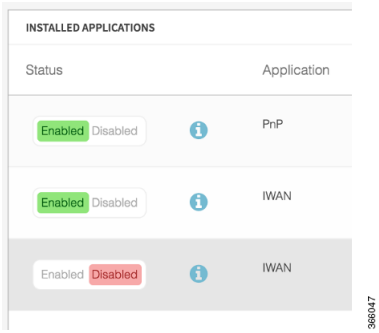


c. [APIC-EM Applications] ページの右側にある [Drag&Drop Application file here]ボックスに注目してください。

ステップ 4　ダウンロードした IWAN アプリ インストール ファイルを [Drag&Drop Application file here]ボックスにドラッグアンドドロップします。新しい IWAN アプリがアプリケーションのリストに示され、[Disabled] と表示されます。
（下記の例に示されているのは、IWAN アプリケーションの旧リリースです）。

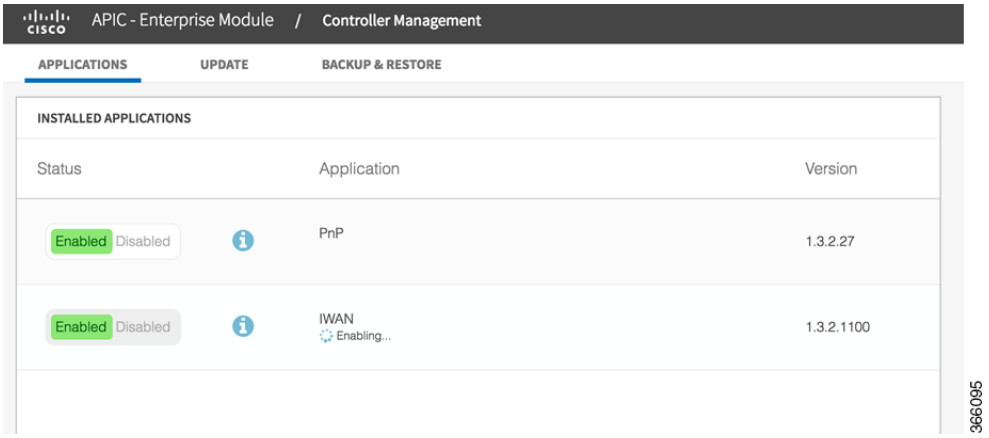


IWAN アプリの以前のバージョンからアップグレードする場合、インストールのこの時点では、IWAN の以前のバージョンが引き続きリストに表示されます。

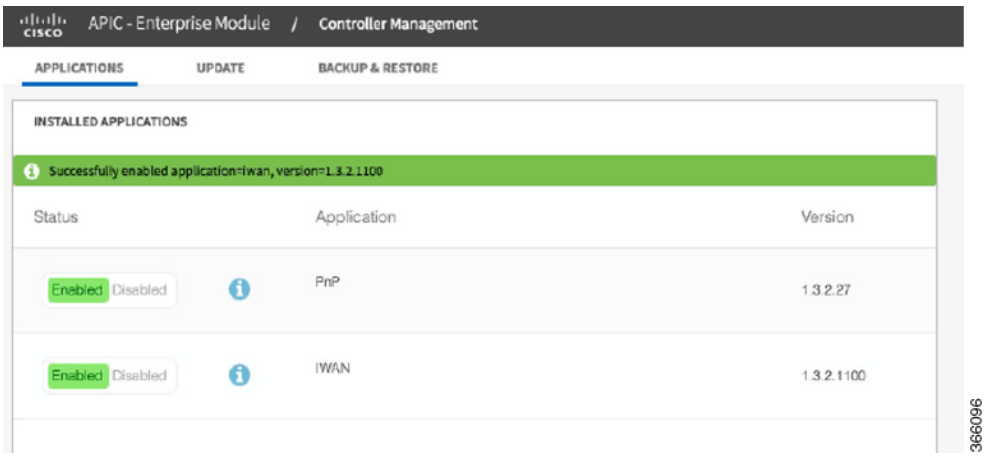


ステップ 5　新しい IWAN アプリケーションの [Enabled]をクリックします。APIC-EM で新しいバージョンが有効になります。IWAN アプリの以前のバージョンからアップグレードする場合、APIC-EM は IWAN の既存の設定を保持します。

ページには、有効化プロセスが進行中であることが示されます。処理が完了するまで待ちます。インストールの所要時間は、クラスタ サイズや他の要因に応じて異なります。
（下記の例に示されているのは、IWAN アプリケーションの旧リリースです）。



ステップ 6　インストールと有効化が完了したら、ブラウザのキャッシュをクリアして [APIC-EM Applications] ページを更新します。[Status] 列に新しい IWAN アプリが有効であることが示され、[Version] 列に新しい IWAN アプリのバージョンが示されます。IWAN アプリの以前のバージョンはすべて、リストから削除されます。
（下記の例に示されているのは、IWAN アプリケーションの旧リリースです）。



CHAPTER 4

ハブ サイトの管理

この章の内容は、次のとおりです。

ハブ サイトの設定およびセットアップの基本的ワークフロー

ハブ サイトを設定およびセットアップするには、Cisco IWAN アプリケーション（IWAN アプリ）に付属するウィザードを使用します。

表 4-1　ハブ サイトの設定およびセットアップの基本的ワークフロー

いいえ。	タスク	参照先
1	システム設定項目を設定する。	ウィザードの手順 1：システム設定項目の設定（4-2 ページ）
2	認定された Cisco IOS ソフトウェア イメージをアップロードする。 (注)　このウィザードの手順は、グリーンフィールド ブランチ デバイスに対してのみ表示されます。	ウィザードの手順 2：ブランチ デバイスの認定 Cisco IOS ソフトウェア イメージのアップロード（4-6 ページ）

表 4-1　ハブ サイトの設定およびセットアップの基本的ワークフロー(続き)

いいえ。	タスク	参照先
3	IP アドレス プールを設定する。	ウィザードの手順 3:IP アドレス プールの設定(4-7 ページ)
4	サービス プロバイダーを設定する。	ウィザードの手順 4:サービス プロバイダーの設定(4-10 ページ)
5	IWAN 集約サイトを設定する。	ウィザードの手順 5:IWAN 集約サイトの設定(4-12 ページ)

ウィザードの手順 1:システム設定項目の設定

Netflow Collector、DNS、AAA、Syslog、SNMP、DHCP などのシステム設定項目を設定するには、次の手順を実行します。

一部のシステム設定項目が表示されないことがあります。必要に応じて [Show More]または [Show Less] ボタンをクリックし、設定を表示または非表示にしてください。

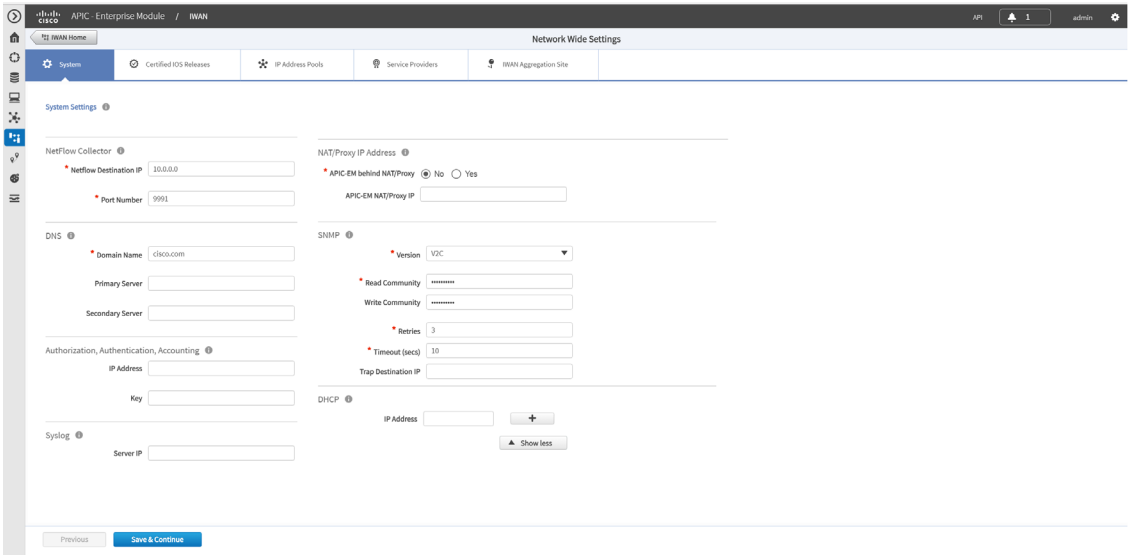
手順

ステップ 1　初めてログインする場合は、[CLI Credentials]ダイアログボックスでグローバル設定を指定するように指示されます。ユーザ名とパスワードを入力し、[Add]をクリックします。

ステップ 2　左側のナビゲーション パネルで、[IWAN]をクリックします。Cisco IWAN のホームページが開きます。

ステップ 3　シスコ インテリジェント WANのホームページで、[Configure Hub Site & Settings]をクリックします。デフォルトで [Settings] タブが開き、[System Settings] ページが表示されます(次の図を参照)。

図 4-1　[Systems Settings] タブ



ステップ 4　[Netflow Collector]領域で、次のプロパティを入力します。

フィールド	説明
Netflow Destination IP	NetFlow コレクタ(サーバ)の IP アドレス。 トラフィック統計情報がネットワーク デバイスから NetFlow コレクタに送信されます。
Port Number	NetFlow コレクタ(サーバ)のポート番号。

ステップ 5　[DNS]領域で、次のプロパティを入力します。

フィールド	説明
ドメイン名	DNS ドメイン名。
プライマリ サーバ	(任意)プライマリ DNS サーバの IP アドレス。
Secondary Server	(任意)セカンダリ DNS サーバの IP アドレス。

ステップ 6　[Authorization, Authentication, Accounting]領域で、次のプロパティを入力します。

フィールド	説明
I[P Address]	(任意)認証、許可、アカウンティング(AAA)サーバの IP アドレス。 Cisco IWAN でサポートされる集中管理型 AAA サービスは、TACACS だけです。TACACS サーバを指定すると、デバイスはスポーク デバイスへの管理アクセス(SSH および HTTPS)に TACACS を使用します。TACACS を指定するかどうかに関わらず、スポーク デバイス上にローカル AAA ユーザ データベースが作成されるので、TACACS サーバを使用できない場合に対応できます。 次のデフォルト値のいずれかがローカル AAA ユーザ クレデンシャルに使用されます。 • Cisco APIC-EM グローバル クレデンシャル • ブランチ ルータのグローバル デバイス クレデンシャルで指定されたユーザ名とパスワード • ハブのプロビジョニング時に入力されたユーザ名とパスワード
Key	(任意)AAA サーバにアクセスするためのキー。

ステップ 7　[Syslog]領域で、次の情報を入力します。

フィールド	説明
Server IP	(任意)Syslog サーバの宛先 IP アドレス。 すべてのルータからの syslog メッセージがこのサーバに送信されます。

ステップ 8　[NAT/Proxy IP Address]領域で、以下を設定します。

フィールド	説明
APIC-EM Behind NAT/Proxy	APIC-EM コントローラが NAT ルータの背後にある場合は、[Yes]を選択します。
APIC-EM NAT/Proxy IP	APIC-EM コントローラのパブリック NAT パブリック IP アドレス。

ステップ 9　[SNMP]領域の [Version] フィールドでバージョン番号を選択します。選択した SNMP バージョン番号（V2C または V3）に応じて、異なるプロパティが表示されます。

- SNMP バージョン V2C の場合は、次のプロパティを入力します。

フィールド	説明
Version	SNMP ソフトウェアのバージョン。値:V2C。
Read Community	SNMP V2C read コミュニティ ストリング。
Write Community	（任意）SNMP V2C write コミュニティ ストリング。
Retries	再試行数デフォルト:3
Timeout (secs)	SNMP V2C に対してのみ表示されます。 タイムアウトの期間を指定します。デフォルト:10
Trap Destination IP	（任意）SNMP サーバの IP アドレス。 **（注）** IP アドレスを入力しない場合は、SNMP サーバとして Cisco IWAN アプリが使用されます。 APIC-EM コントローラを管理対象ネットワーク デバイスの SNMP マネージャとして動作させるか、別の SNMP サーバを指定して SNMP トラップを処理させることができます。SNMP の設定によってハブとリモート サイトのデバイスからのインベントリが決まります。これらの値は設定に反映されます。

- SNMP バージョン V3 の場合は、次のプロパティを入力します。

フィールド	説明
Version	SNMP ソフトウェアのバージョン。値:V3。
モード	ドロップダウン リストからモードを選択します。次のオプションがあります。 • 認証および暗号化 • No Authentication and No Encryption • Authentication and No Encryption
Auth.タイプ	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合に表示されます。 ドロップダウンリストから認証タイプを選択します。次のオプションがあります。 • HMAC-SHA • HMAC-MDS
Username	認証ユーザ名

フィールド	説明
Auth.Password]	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合に表示されます。 認証ユーザ名のパスワード。
Encryption Type	[Mode] フィールドで [Authentication and Encryption] を選択した場合に表示されます。 暗号化ユーザ名。
Encryption Password	[Mode] フィールドで [Authentication and Encryption] を選択した場合に表示されます。 暗号化ユーザ名のパスワード。
Retries	再試行数デフォルト:3
Timeout (secs)	SNMP V2C に対してのみ表示されます。 タイムアウトの期間を指定します。デフォルト:10
Trap Destination IP	(任意)SNMP サーバの IP アドレス。 (注)　IP アドレスを入力しない場合は、SNMP サーバとして Cisco IWAN アプリが使用されます。 APIC-EM コントローラを管理対象ネットワーク デバイスの SNMP マネージャとして動作させるか、別の SNMP サーバを指定して SNMP トラップを処理させることができます。SNMP の設定によってハブとリモート サイトのデバイスからのインベントリが決まります。これらの値は設定に反映されます。

ステップ 10　[DHCP]領域で、次のプロパティを入力します。

フィールド	説明
External DHCP IP	(任意)DHCP サーバの宛先 IP アドレス。 クライアント コンピュータや他の TCP/IP ベースのネットワーク デバイスに有効な IP アドレスを提供する、DHCP サーバを入力します。 DHCP サーバを追加するには、[IP Address] フィールドの横にある [+]アイコンをクリックして IP アドレスを入力します。 (注)　最大 5 つの DHCP サーバを追加できます。 DHCP サーバを削除するには、削除する [IP Address] フィールドの横にある [-]アイコンをクリックします。

ステップ 11　[保存して続行(Save and Continue)]をクリックします。[Certified IOS Releases] タブが開きます。ウィザードの手順 2:ブランチ デバイスの認定 Cisco IOS ソフトウェア イメージのアップロード (4-6 ページ)を参照してください。

[Systems] タブの既存の値を更新すると、[Network Wide Settings Summary] ダイアログボックスが開き、変更内容が表示されます。次のいずれかを実行します。

- [Apply Now] オプション ボタンをクリックして、[Continue] をクリックします。
- [Schedule]オプション ボタンをクリックして、変更を適用する日時を指定し、[Submit] をクリックします。

ウィザードの手順 2:ブランチ デバイスの認定 Cisco IOS ソフトウェア イメージのアップロード

(注)　このウィザードの手順は、グリーンフィールド ブランチ デバイスに対してのみ表示されます。

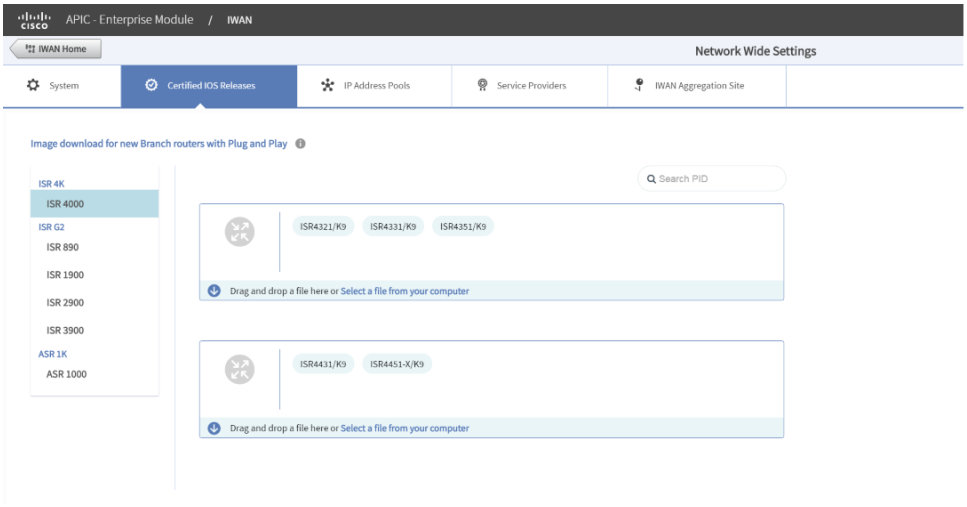
認定された Cisco IOS イメージをコンピュータからシスコ インテリジェント WANアプリケーションにアップロードできます。グリーンフィールド デバイスが出現すると、Plug-n-Play エージェントは Cisco APIC-EM 内の Plug-n-Play サーバとやり取りして、適切な Cisco IOS ソフトウェア イメージをデバイスにダウンロードし、そのイメージとともにデバイスをリロードします。

(注)　適切なソフトウェア イメージがすでにルータにインストールされている場合は、この手順をスキップできます。

手順

ステップ 1　[Certified IOS Releases]タブをクリックします。[Cisco IOS Releases for Sites] ページが開きます(次の図を参照)。

図 4-2　[Certified IOS Releases] タブ



ステップ 2　左ペインで、Cisco IOS イメージをアップロードするルータのタイプを選択します。

ステップ 3　次のいずれかを実行します。

- Cisco IOS ソフトウェア イメージ ファイルをコンピュータから GUI にドラッグアンドドロップします。
- Cisco IOS ソフトウェア イメージ ファイルが保存されている場所を参照して、ファイルをシステムにアップロードします。

ステップ 4　[Continue]をクリックします。[IP Address Pools] ページが開きます。ウィザードの手順 3:IP アドレス プールの設定(4-7 ページ)を参照してください。

ウィザードの手順 3:IP アドレス プールの設定

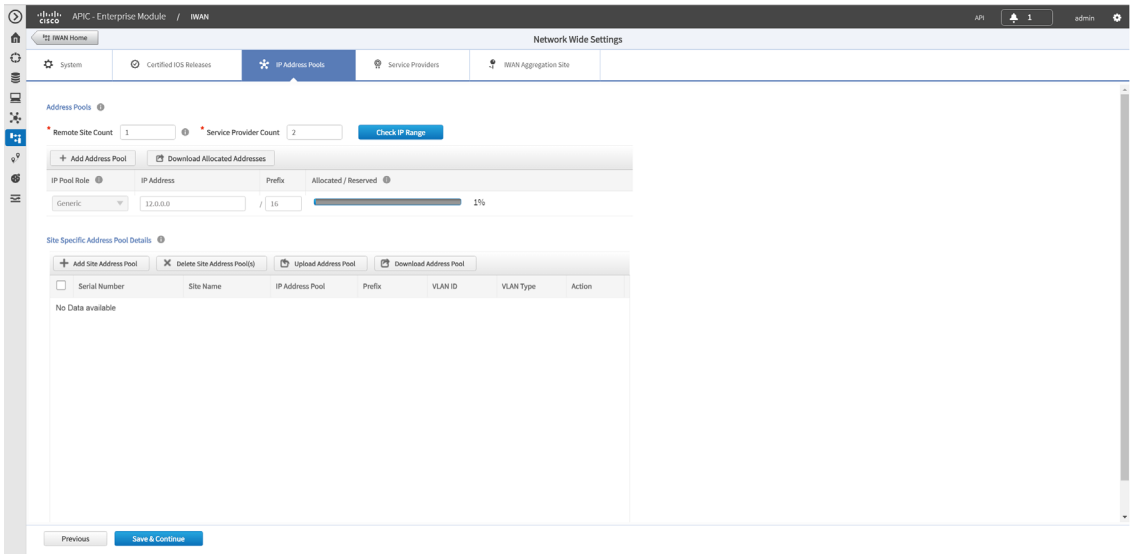
（注）　汎用 IP プールはオーバーレイ アドレスやループバック アドレスに使用されます。汎用 IP アドレス プールは、[IP Address Pools] タブで指定したリモート サイトとサービス プロバイダーの数に従って分割されます。将来の要件を把握して計画を立て、導入するサービス プロバイダーとリモート サイトの最大数を指定してください。IP アドレス プールの設定を指定した後は、それらを変更できません。

IP アドレス プールを定義するには、[IP Address Pools]タブを使用します。IP アドレス プールの詳細については、IP アドレス プールについて（4-21 ページ）を参照してください。

手順

ステップ 1　[IP Address Pool]タブを選択します。[Address Pools] ページが開きます（次の図を参照）。

図 4-3　[IP Address Pool] タブ



ステップ 2　[Remote Site Count]フィールドで、導入するリモート サイトの最大数を入力します。

Cisco IWAN リリース 1.2.x を使用している既存のお客様の場合は、Cisco IWAN リリース 1.3.x にアップグレードすることによりリモート サイトの数を増加できます。（初期プロビジョニング時に作成される）事前予約済みサブネットの内部 IP アドレスの可用性に基づいて、より大きいリモート サイト数を指定できます。

ステップ 3　[Service Provider Count]フィールドで、必要なサービス プロバイダーの最大数を入力します。

Cisco IWAN リリース 1.2.x を使用している既存のお客様の場合は、Cisco IWAN リリース 1.3.x にアップグレードすることによりサービス プロバイダーの数を増加できます。最大 4 つのサービス プロバイダーを指定できます。

ステップ 4　[Check IP Range]ボタンをクリックします。[Proposed IP Range] が開きます。

入力したリモート サイトとサービス プロバイダーの数に基づいて、[Proposed IP Range] ページに、汎用 IP アドレス プールに使用可能な最小推奨プレフィックス長、LAN インターフェイス プールのプレフィックス長、VLAN ごとの IP アドレスの数、および VLAN の数に関する情報が表示されます。[OK]または [Get IP Range] をクリックします。

ステップ 5　次のいずれかを実行します。

- 手動で IP アドレスを入力するには、[+ Add Address Pool]をクリックします。次のプロパティを入力します。

フィールド	説明
ロール	次のいずれかです。 • [Generic]:最初の範囲は常に、デフォルトで汎用IP プールになります。 • [LANGreenfield]:新しいグリーンフィールド ブランチ デバイスの LAN IP アドレス プールを定義するには、このオプションを選択します。任意の数の LAN グリーンフィールド IP アドレス プールを指定できます。 • [LANBrownfield]:ブラウンフィールド ブランチ デバイス(既存の設定があるデバイス)の LAN IP アドレス プールを定義するには、このオプションを選択します。任意の数の LAN ブラウンフィールド IP アドレス プールを指定できます。
IP Address	IP アドレス プールの IP アドレス。
Prefix	CIDR プレフィックス。
Allocated	プール内の使用されているアドレスの割合を表示します。

- 多数の IP アドレスをアップロードするには、[Upload Address Pool]をクリックして、コンピュータから .csv ファイルをアップロードします。

  .csv ファイルに含める必要がある情報の種類については、[Download Address Pool]タブをクリックしてください。テンプレートの詳細を含む Controller_Profile_DD-MM-YYYY.csv ファイルがシステムにダウンロードされます。

ステップ 6　[+ Add Site Address Pool]をクリックして、サイト固有の LAN IP アドレス プールの情報を入力します。[Add Site Address Pool] ダイアログボックスが開きます。下記の表に示すプロパティを入力し、[OK]をクリックします。

デフォルトでは、グリーンフィールド ブランチ サイトは LAN グリーンフィールド IP アドレス プールが存在する場合はその IP アドレスを使用し、存在しない場合は汎用 IP アドレス プールの IP アドレスを使用します。(たとえば、VLAN に LAN グリーンフィールド IP アドレス プールや汎用 IP アドレス プールの IP アドレスを使用したくない場合などに)VLAN に特定の IP アドレス プールを使用する新しいグリーンフィールド ブランチ サイトをプロビジョニングする場合は、サイトをプロビジョニングする前に VLAN とそれぞれの IP アドレス プールを定義できます。

(注)　サイトをプロビジョニングした後は、VLAN があるサイト固有の IP アドレス プールと VLAN がないサイト固有の IP アドレス プールとの間を移動できません。したがって、サイトをプロビジョニングする前に、必ず明確なビジョンを確立しておく必要があります。

フィールド	説明
Serial Number	サイト デバイスのシリアル番号。 サイトに複数のデバイスがある場合は、すべてのシリアル番号をセミコロンで区切って指定します。
Site Name	サイト名。
IP Address Pool	この VLAN 上のホストに使用する IP アドレス プール。
Prefix	CIDR プレフィックス。
VLAN ID	値の範囲:1 ～ 4094。 (注)　VLAN ID 99 は中継 VLAN 用に予約されているため、この ID を別の VLAN に使用することはできません。
VLAN Type	VLAN のタイプを入力するか、ドロップダウン リストから選択します。 値:Data、Guest、Voice and Video、Wireless (注)　VLAN タイプを入力する場合は、次の制限が適用されます。 – VLAN タイプの値は 200 文字以下でなければなりません。 – VLAN タイプには「?」記号を使用できません。 – サイト固有のアドレス プールの場合は、サイトごとに最大 20 エントリを入力できます。

ステップ 7　必要に応じてステップ 6 を繰り返し、さらにサイト アドレス プールを追加します。

ステップ 8　[保存して続行(Save and Continue)]をクリックします。[Service Providers] タブが開きます。ウィザードの手順 4:サービス プロバイダーの設定(4-10 ページ)を参照してください。

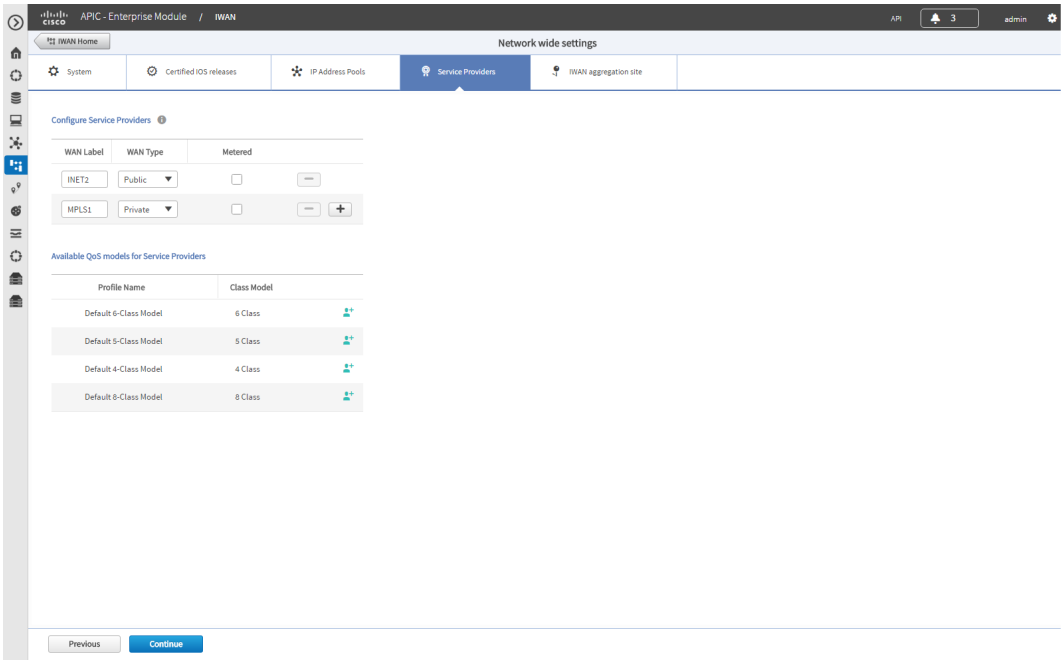
ウィザードの手順 4:サービス プロバイダーの設定

リンクのタイプとサービス プロバイダーの数を指定するには、[Service Providers] タブを使用します。

手順

ステップ 1　[Service Providers]タブを選択します。[Configure Service Providers] ページが開きます(次の図を参照)。

図 4-4　[Service Providers] タブ



ステップ 2　[Configure Service Providers]領域で、[+] アイコンをクリックして次のプロパティを定義します。

(注)　最大 4 つのサービス プロバイダーを指定できます。

フィールド	説明
WAN Label	WAN トランスポート タイプ。最大 7 文字まで指定できます。
WAN Type	次のいずれかです。 • プライベート • パブリック

フィールド	説明
Metered	WAN が従量制の場合はこのオプションを選択します。 (注)　サービス プロバイダーの数が 3 つ以上の場合にのみ、[Metered] オプションを選択できます。サービス プロバイダーが 2 つしかない場合に一方のリンクを従量制リンクとして選択することはできません。 (注)　パブリック クラウドでは、1 つのリンクだけが従量制リンクとして許可されます。
Available QoS Models for Service Providers	
Profile Name	すべての使用可能なサービス プロファイルの名前が一覧表示されます。
Class Model	それぞれのサービス プロファイルに対応するクラス モデルが一覧表示されます。 • 4 Class • 5 Class • 6 Class • 8 Class

ステップ 3　(任意)提供されているデフォルト クラスではなくカスタムのクラス モデルが必要な場合は、[Available QoS Models for Service Providers]領域をクリックし、サービス プロバイダーのサービス レベル契約(SLA)に最も合致するプロファイルの横にある [+]アイコンをクリックします。[Add Service Profile] ダイアログボックスが開きます(次の図を参照)。

図 4-5　[Add Service Profile] ダイアログボックス

ステップ 4　次のプロファイル情報を入力し、[Save]をクリックします。

(注)　プライベート WAN インターフェイスの場合は、一連の定義済みサービス プロバイダーのプロファイルを使用できます。サービス プロバイダーの SLA を満たすために、出力 QoS キューイングが WAN 出力に適用されます。

フィールド	説明
Profile Name	新しいサービス プロファイルの名前
Class Model	クラス モデルのタイプが表示されます。次のいずれかです。 • 4 Class • 5 Class • 6 Class • 8 Class
Class Name	データ クラス名が表示されます。
DSCP	各クラスの DiffServ コード ポイント(DSCP)値が表示されます。保存すると、新しいプロファイルとして表示されます。保存後は、この値を変更できません。
Priority Bandwidth (%)	プライオリティ クラスに割り当てる帯域幅の割合。例:Voice。
残りの帯域幅(%)	ストリーミング ビデオや重要なクラスなど、他のクラスに割り当てる帯域幅の割合。 (注)　0 よりも大きい値を入力する必要があります。[Remaining Bandwidth] 列のすべてのデータ クラスの合計値が 100 % を超えることはできません。

(注)　プロファイル情報を追加すると、[Available QoS Models for Service Providers] 領域にプロファイルの詳細情報が表示されます。

ステップ 5　[Continue]をクリックします。[IWAN Aggregation Site] タブが開きます。ウィザードの手順 5:IWAN 集約サイトの設定(4-12 ページ)を参照してください。

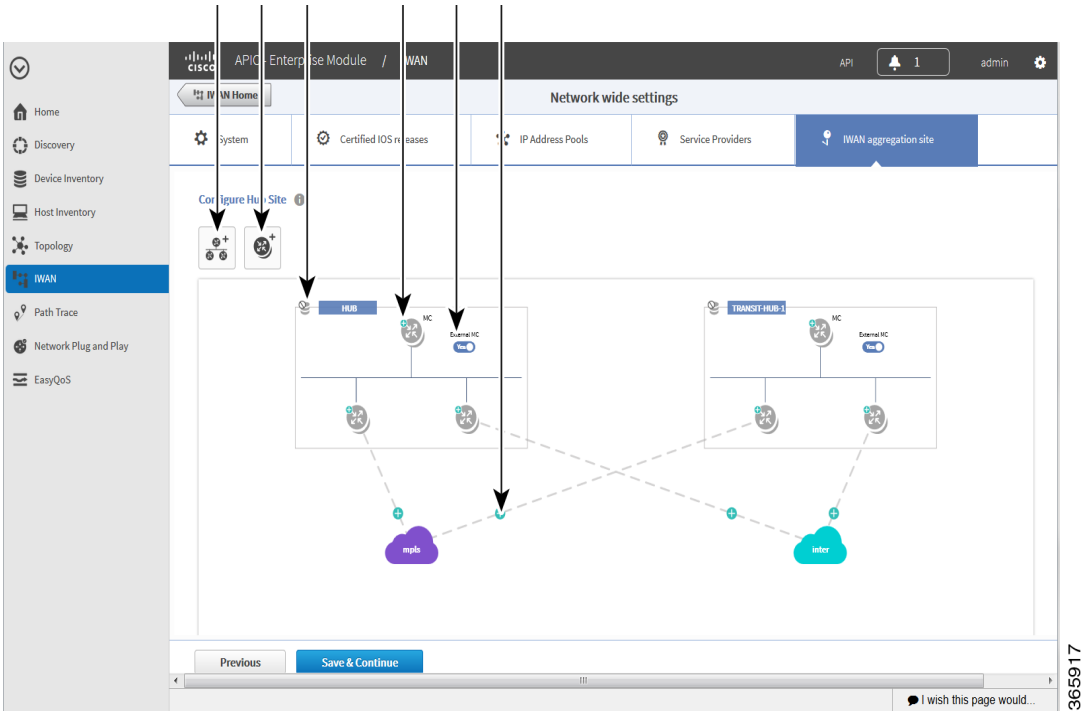
ウィザードの手順 5:IWAN 集約サイトの設定

この手順を使用して、以下を実行します。

1. ハブ デバイスの検出。
2. LAN の設定。
3. WAN の設定。
4. 外部マスター コントローラの設定。

次の図を参照して、実行する手順を把握してください。

図 4-6　[IWAN Aggregation Site] タブ



1	[Add POP] アイコン	4	[Configure External MC Router +] アイコン
2	[Add Border Router] アイコン	5	[External MC] 切り替えボタン
3	[Configure LAN] アイコン	6	[Configure WAN Link +] アイコン

手順

ステップ 1　ハブ デバイスの検出。次の手順を実行します。

a. [IWAN Aggregation Site]タブを選択します。[Configure Hub Site] ページが開き、ウィザードの手順 4 で定義したすべてのサービス プロバイダーとそれぞれのハブ境界ルータが表示されます。

b. 次のいずれかを実行します。

- (推奨)[External MC]ボタン(図 4-6 の 5)をクリックして [Yes]に切り替えます。新しいルータがスタンドアロン マスター コントローラ(MC)として追加されます。
- [External MC]ボタンをクリックして [No]に切り替えます。境界ルータの 1 つが MC として指定されます。

c. さらにハブを追加するには、[Add POP]アイコン(図 4-6 の 1)をクリックします。プライマリ ハブの横に中継ハブが追加されます(上の図の TRANSIT-HUB-1 を参照)。

(注)　プロビジョニング時には最大 2 つのハブ サイトを指定できます。ハブのプロビジョニング後に、ルータを追加または削除できます。

d. (任意)新しい TRANSIT-HUB-1 を別の名前に変更するには、ハブの名前をクリックして別の名前を追加します。

(注)　ハブの名前は初期設定時(ハブにルータを追加する前)にのみ変更できます。

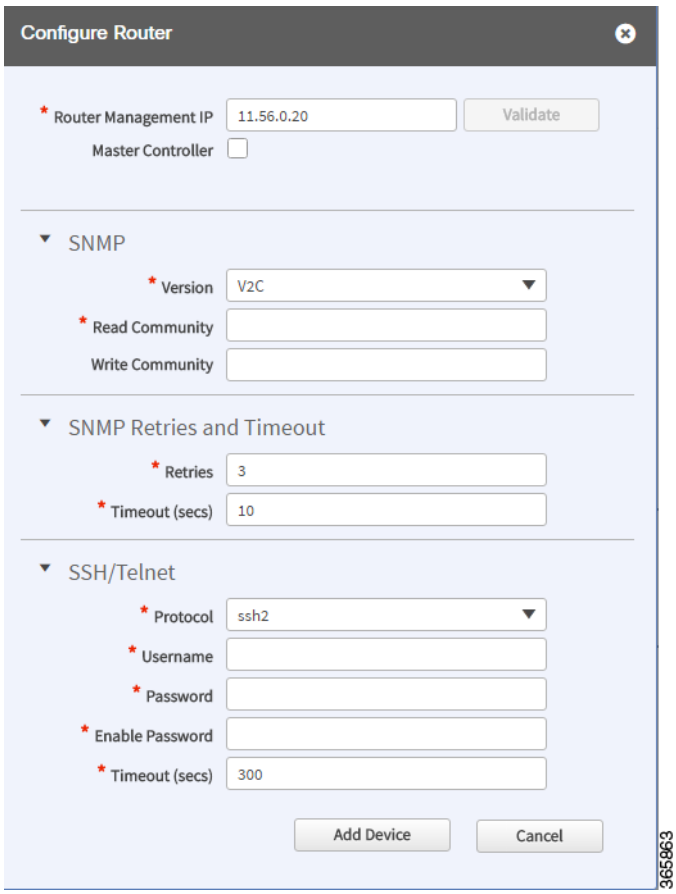
e. 境界ルータをハブに追加する場合は、[Add Border Router]アイコン(図 4-6 の 2)の上にカーソルを移動すると、[Add to POP]オプションが表示されます。2 つの使用可能なハブのいずれかを選択します。新しい境界ルータが当該ハブに追加されます。

(注)　1 つのハブ サイトに最大 4 つの境界ルータを指定できます。

f. 新たに追加した境界ルータを設定するには、ルータ上部の [+]アイコンをクリックして、[Configure Router] ダイアログボックスを開きます。

g. [Configure Router] ダイアログボックスで、次の手順を実行します。

- [Router Management IP]フィールドに、ハブ ルータの管理 IP アドレスを入力します。
- [Validate]をクリックします。[Configure Router]ダイアログボックスが再び開き、追加のフィールドが表示されます(次の図を参照)。



フィールド	説明
Router Management IP	ハブ ルータの管理 IP アドレス。
マスター コントローラ	デバイスをマスター コントローラとして選択するには、このオプションをオンにします。
SNMP	
Version	SNMP のバージョン番号。 選択したバージョン番号に応じて異なるプロパティが表示されます。
Read Community （SNMP V2C を選択した場合に表示）	SNMP V2C read コミュニティ ストリング。
Write Community （SNMP V2C を選択した場合に表示）	（任意）SNMP V2C write コミュニティ ストリング。
モード （SNMP V3 を選択した場合に表示）	ドロップダウン リストからモードを選択します。次のオプションがあります。 • 認証および暗号化 • [No Authentication and No Encryption] • [Authentication and No Encryption]
Auth.タイプ （SNMP V3 を選択した場合に表示）	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合に表示されます。 ドロップダウン リストから、認証タイプを選択します。次のオプションがあります。 • HMAC-SHA • HMAC-MDS
Username （SNMP V3 を選択した場合に表示）	SNMP V3 を選択した場合に表示されます。 認証ユーザ名
Auth.Password] （SNMP V3 を選択した場合に表示）	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合に表示されます。 認証ユーザ名のパスワード。
Encryption Type （SNMP V3 を選択した場合に表示）	[Mode] フィールドで [Authentication and Encryption] を選択した場合に表示されます。 暗号化ユーザ名。
Encryption Password （SNMP V3 を選択した場合に表示）	[Mode] フィールドで [Authentication and Encryption] を選択した場合に表示されます。 暗号化ユーザ名のパスワード。
SNMP の再試行回数およびタイムアウト	
Retries	SNMP の再試行回数。デフォルト:3
Timeout (secs)	SNMP 要求がタイム アウトしたと見なされるまでの待機秒数。デフォルト:10

フィールド	説明
SSH/Telnet	
Protocol	ホストとの通信に使用されるプロトコル（Telnet または SSH）。
Username	SSH または Telnet のユーザ名。
Password	SSH または Telnet のパスワード。
Enable Password	ユーザ名のイネーブルパスワード。
Timeout (secs)	SSH または Telnet 要求がタイム アウトしたと見なされるまでの待機秒数。

– 上記の表の説明に従って、プロパティを入力します。

（注）　これらのクレデンシャルは 1 回だけ入力できます。これらの値は、システム内の残りのハブ デバイスに自動的に入力されます。

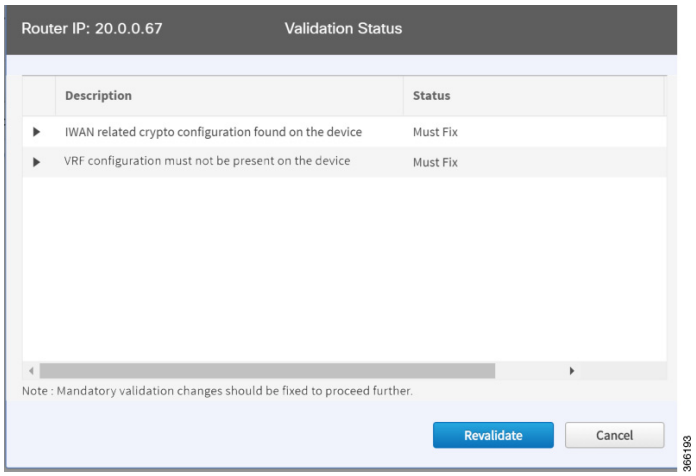
– [Add Device]をクリックします。

デバイスがバックグラウンドで検証され、プロビジョニングに適しているかどうかが判断されます。以下が実行されます。

Cisco IWAN アプリはルータにアクセスしてその設定をチェックし、Cisco IWAN アプリと競合する可能性がある設定が含まれているかどうかを確認します。これはブラウンフィールド検証と呼ばれます。

ルータに競合する設定がない場合は、デバイスの上部にオレンジ色のアイコンが表示され、[Configure Router] ダイアログが開きます。

ルータに競合する設定がある場合は、[Validation Status] ダイアログが開き、すべての検証エラーが一覧表示されます（次の図を参照）。



h. 検証ステータスは [Warning] または [Must Fix] のいずれかになります。次の手順を実行します。

– 検証ステータスが [Warning] の場合は、エラーを修正または無視することができます。

– 検証ステータスが [Must Fix] の場合は、説明で示された設定を削除し、[Revalidate]をクリックします。

[Validation Status] ダイアログボックスに表示されるメッセージの詳細については、付録 A「ブラウンフィールド検証メッセージ」を参照してください。

ルータの検証に成功した場合（[Must Fix] エラーがない場合）は、[Configure Router]ダイアログボックスが開きます。

i. [Configure Router] ダイアログボックスで、適切な [LAN IP-Interface]チェックボックスをオンにして、[Save] をクリックします。

（注）　複数の LAN IP インターフェイスを選択できます。

j. 境界ルータをクラウドに接続するには、ルータをクリックしてクラウドにドラッグします。

k. 上記の手順を使用して、他の境界ルータを設定します。

ステップ 2　LAN の設定。次の手順を実行します。

a. プライマリ ハブの左上隅にあるアイコン（図 4-6の 3）をクリックします。[Configure LAN] ダイアログボックスが開き、次の表に示すフィールドが表示されます。

[Routing Protocol]、[AS Number]、[Datacenter Prefix]は、設定しやすいように、デバイスから収集されて自動的に入力されます。各ルーティング プロトコルに対してデバイス間の共通（一致）AS 番号が表示されます。デバイスの AS 番号は変更できますが、お勧めしません。

フィールド	説明
Routing Protocol	ハブ ルータで実行するデフォルトのルーティング プロトコル。 例：EIGRP、OSPF、BGP
AS Number	ルーティング プロトコルに応じて、AS 番号またはエリア番号。 （注）　LAN ルーティング プロトコルが BGP で、もう一方のハブ デバイスからの照合 AS 番号がない場合、このフィールドはグレー表示されます。デバイスの LAN 側ルーティングを手動で変更する必要があります。 （注）　異なる AS 番号の BGP はサポートされません。
Datacenter Prefix	プレフィックスとして指定したハブ サイトの IP アドレス。

b. [Save（保存）] をクリックします。

ステップ 3　WAN の設定。次の手順を実行します。

a. ルータとクラウドを接続しているリンク上の [+]アイコン（図 4-6 の 6）をクリックします。[Configure Link]ダイアログボックスが開きます。

表示されるダイアログボックスは、[Service Provider]の設定時に指定した WAN のタイプ（[Private] または [Public] など）に応じて異なります。

b. [Public]WAN を指定した場合は、[Configure Link] ダイアログボックスが開きます。ネットワークのリンクごとに次の情報を入力します。

表 4-2　[Configure Link] ダイアログボックス：Public WAN

フィールド	説明
WAN IP-Address	WAN インターフェイスの IP アドレス。
デフォルト ゲートウェイ	デフォルト ゲートウェイの IP アドレス。

表 4-2　[Configure Link] ダイアログボックス:Public WAN（続き）

フィールド	説明
NAT Enabled	NAT IP アドレスを使用する場合は、このオプションをオンにします。
NAT IP Address	パブリック IP アドレス
帯域幅（Mbps）	アップロードとダウンロードの対称帯域幅。
サービス プロファイル	ドロップダウン リストからサービス プロファイルを選択します。 ドロップダウン リストには、デフォルトのサービス プロファイルと、[Service Providers] タブで設定したカスタムの 8 Class サービス プロファイルが含まれています。

c. [Private]WAN を指定した場合は、[Configure Link] ダイアログボックスが開きます。ネットワークのリンクごとに次の情報を入力します。

表 4-3　[Configure Link] ダイアログボックス:Private WAN

フィールド	説明
WAN IP-Address	WAN インターフェイスの IP アドレス。
デフォルト ゲートウェイ	デフォルト ゲートウェイの IP アドレス。
Enable Non IWAN Sites	ネットワークの段階的移行に向けて、非 IWAN サイトと新たに有効になった IWAN POP（ハブ）およびスポーク サイトとの通信を有効にするには、このオプションをオンにします。IWAN サイトと非 IWAN サイトの共存について（4-19 ページ）を参照してください。
Loopback IP-Interface	ドロップダウン リストからプロビジョニング済みのループバック IP アドレスを選択します。これにより、シスコ インテリジェント WANアプリケーションで既存サイトと新規 IWAN サイト間のルートを形成できるようになります。 （注）　ループバック インターフェイスはプライベート（MPLS）ルータに設定する必要があります。ループバック インターフェイスは、IWAN サイトと非 IWAN サイトの共存をサポートする必要があり、デバイスを Cisco APIC-EM に追加する前に設定しておく必要があります。ループバック IP アドレスは WAN インターフェイスと同じサブネット内に指定することをお勧めします。
帯域幅（Mbps）	アップロードとダウンロードの対称帯域幅。
サービス プロファイル	ドロップダウン リストからサービス プロファイルを選択します。 ドロップダウン リストには、デフォルトのサービス プロファイルと、[Service Providers] タブで設定されたカスタム サービス プロファイル（4 Class、5 Class、6 Class、8 Class）がすべて含まれています。

d. [Save]をクリックします。

ステップ 4　外部マスター コントローラの設定。

ハブおよびルータの初期設定時に、[External MC]ボタンをクリックして [Yes]に切り替えた場合は、新しいルータがスタンドアロン MC として追加されています。次の手順を実行します。

a. External MC ルータの上部にある [+]アイコン（図 4-6 の 4）をクリックします。[Configure Router] ダイアログボックスが開きます。

専用のマスター コントローラを使用する場合は、デバイスをグリーンフィールド検証する必要があります。IWAN やダイナミック ルーティング プロトコルと競合する設定は、LAN および WAN でサポートされません。

b. [Router Management IP]フィールドに、ハブ ルータの管理 IP アドレスを入力します。

c. [Validate]をクリックします。[Configure Router] ダイアログボックスが開きます。

d. [Router Management IP] のアドレス、[SNMP]、[SSH/Telnet] のプロトコル情報を入力し、[Save] をクリックします。

ハブ サイトの設定の変更

[Hub Site and Settings] 領域でウィザード手順をすべて完了すると、後から戻ってプロパティを変更できます。グレー表示のフィールドは変更できません。

IWAN サイトと非 IWAN サイトの共存について

IWAN サイトと非 IWAN サイトの共存機能を使用すると、ネットワークの段階的移行に向けて、新たに有効になった IWAN POP（ハブ）およびスポークサイトと非 IWAN サイトとの間で通信できるようになります。この機能の利点は次のとおりです。

- 全面的な導入に先立ち、少数のサイトに シスコ インテリジェント WANを導入できる。
- 非 IWAN サイトは、IWAN 対応のハブおよびスポーク ルータとの通信を継続できる（逆も同様）。

IWAN ソリューションと非 IWAN サイトの同時サポートを有効にするための前提条件

APIC-EM ワークフローで Cisco IWAN アプリを起動する前に、次の設定を完了しておく必要があります。

- Cisco IWAN ハブ プライベート（MPLS）境界ルータを定義する。
- ハブ ルータで以下を実行する。
  - 境界ルータでループバック インターフェイスを有効にする必要があります。ループバック IP アドレスは WAN インターフェイスと同じサブネット内に指定することをお勧めします。
  - （シスコ インテリジェント WANアプリケーション ワークフローに従ってハブをプロビジョニングする前に）既存の MPLS-CE をデフォルト ゲートウェイとしてスタティック ルートを追加する必要があります。

- 既存の MPLS-CE ルータで以下を実行する。
  - IWAN MPLS 境界ルータ上のループバック IP アドレスを、MPLS-CE ルータ上の BGP（または MPLS プロバイダーとのピアリングに使用される他のルーティング プロトコル）によってアドバタイズする必要があります。ループバック IP は、すべてのリモート サイトからアクセスできる必要があります。

Cisco IWAN リリース 1.1.0 以降、2 つのハブと 2 つのクラウドを指定して、より多くのデバイスをクラウドに追加できるようになったので、マルチリンク ネットワークが可能になりました。つまり、マルチリンク ネットワークに 2 つのデータセンターを配置して、各データセンターに 4 つのリンクを持つ 4 つのデバイスを含めることができます。

異種 WAN サイトの例

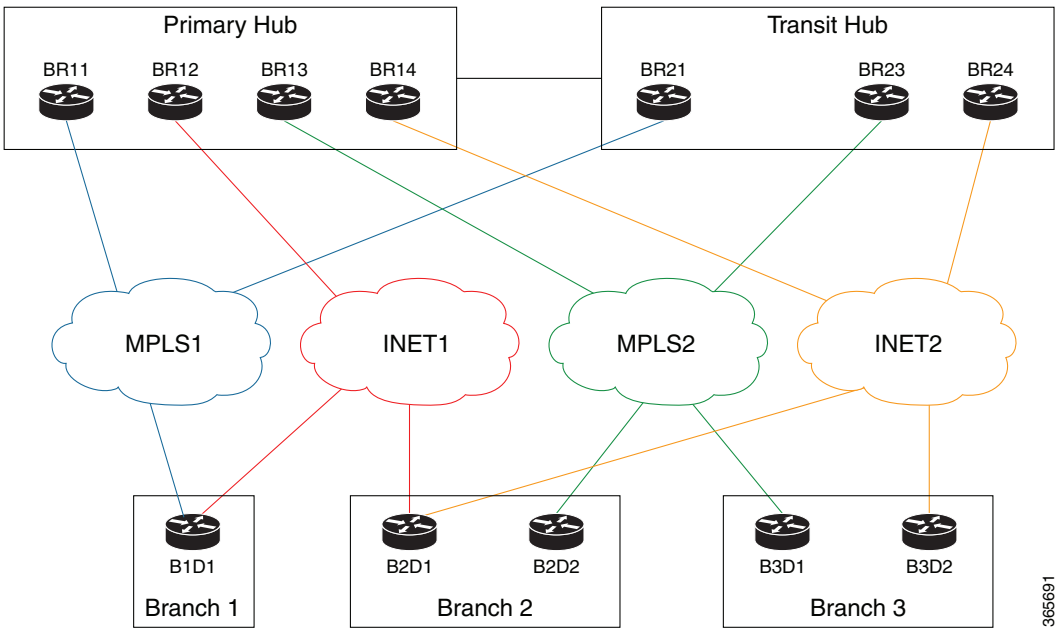
Cisco IWAN リリース 2.0 以降では、プロビジョニング済みのサイトで以下を実行できます。

- WAN クラウドとサービス プロバイダーを追加する。
- 任意のタイプ（Private または Public）のリンクを最大 2 つ追加する。新しいリンクによって既存のデバイスの優先度が影響を受けたり、パス プリファレンスが変更されることはありません。
- 異なるハブ サイトを異なるサービス プロバイダーに接続する（サービス プロバイダーの最大数は 4）。

（注）　上記の変更点はサイトのプロビジョニング時には実行できません。

次の図は異種トポロジの例を示しています。この例では、プライマリ ハブが 4 つのサービス プロバイダーに接続され、中継ハブが 3 つのサービス プロバイダーに接続されています。この例は、両方のハブ サイトが同数のサービス プロバイダーを持つ必要がないことを示しています。

図 4-7　MPLS リンクに接続されている中継ハブ



IP アドレス プールについて

シスコ インテリジェント WANアプリケーションは、グローバル エンタープライズ IP アドレス プール スペースから切り分けられた IP アドレスを自動的に使用します。この機能をサポートするには、シスコ インテリジェント WANアプリケーション用に 1 つの汎用グローバル IP アドレス プールを定義する必要があります。ハブとスポーク デバイスをプロビジョニングするために、この汎用 IP アドレス プールから IP アドレスが割り当てられます。これにはインターフェイス、LAN、VPN オーバーレイ、およびルーティングの IP アドレスが含まれます。

必要に応じて、1 つ以上の LAN グリーンフィールド IP アドレス プールを定義して、ブランチ LAN 側の IP アドレス空間をさらに調整できます。すべての LAN グリーンフィールド IP アドレス プールが使い尽くされると、汎用 IP アドレス プールが使用されます。

IWAN サイトの長期的なニーズに対応できるように、汎用 IP アドレス プールのサイズを適切に設定することが重要です。VPN 要件では、サイトをプロビジョニングする前に、内部でサブネットを定義して割り当てることが指示されています。Cisco IWAN リリース 1.3 では、初期プロビジョニングの後にサイトやサービス プロバイダーの数を増加できますが、指定済みの汎用 IP アドレス プールを変更することはできません。したがって、サービス プロバイダーやサイトの将来の規模を念頭に置いて、汎用 IP アドレス プールを定義することを推奨します。汎用 IP プールはオーバーレイ アドレスやループバック アドレスに使用されます。汎用 IP プールは、[IP Address Pools] タブで指定されたリモート サイトとサービス プロバイダーの数に従って分割されます。

固有の IP アドレスが必要な場合は、サイト固有の LAN 要件や VLAN 要件を定義し、汎用グローバル IP アドレス プールよりも優先させることができます。

サイト固有のプロファイル

サイト固有のプロファイルはオプションであり、各サイトの LAN IP アドレスを事前プロビジョニングする場合にのみ必要です。事前プロビジョニングにより、要求されていないデバイスのリストにデバイスが追加される前に、サイト名とデバイスの組み合わせを使用してサイトを定義することができます。これは、デバイスのシリアル番号とサイト名を照合することで遂行されます。各サイトの VLAN 定義によって、IP アドレス プールの範囲を指定できます。指定しない場合は、LAN グリーンフィールド IP アドレス プールまたは汎用 IP アドレス プールから必要な LAN IP アドレスが提供されます。

ブランチ サイト固有のプロファイル

ブランチ サイトの仕様を事前プロビジョニングできます。デバイスのシリアル番号とサイト名をサイトの VLAN とともに使用して、シングルまたはデュアル ルータ サイトを定義できます。

シングル ルータ ブランチの場合は、デバイスのシリアル番号を指定する必要があります。デュアル ルータ ブランチの場合は、両方のデバイスのシリアル番号をセミコロンで区切って指定する必要があります。Cisco IWAN アプリによって、サイト名とデバイスのシリアル番号が自動的に照合され、事前に定義した VLAN と IP アドレス プールが使用されます。したがって、当該デバイスが要求されていないデバイスとしてサイト プロビジョニング ワークフローに表示される前に、ブランチ サイトを使用できるようになります。

サイトと VLAN を定義すると、サイト プロビジョニング ワークフローでデバイスがプロビジョニングされる際に、デバイスを簡単に設定できます。デバイスが要求されてプロビジョニングされる際に、サイト プロビジョニング ワークフローは既存のサイト設定やサイト名と競合しません。

IP アドレス プールは保存後に変更できません。

LAN ブラウンフィールド IP アドレス プール

Cisco IWAN リリース 1.3 では、ブラウンフィールド ブランチ デバイスの LAN IP アドレスを定義するために、LAN ブラウンフィールド ロールが導入されました。

ブラウンフィールド ブランチがプロビジョニングされる際に、その VLAN サブネットが予約されます。

VLAN サブネットが LAN ブラウンフィールド IP アドレス プールのサブネットである場合、VLAN サブネットは LAN ブラウンフィールド IP アドレス プールから予約されます。

VLAN サブネットの LAN ブラウンフィールド サブネットがない場合は、サイト固有の IP アドレス プールとして予約されます。

追加、削除、更新の操作は、ブラウンフィールド サイト固有の IP アドレス プールでは許可されません。

プロビジョニング済みハブ サイトの WAN 帯域幅の更新

ハブ サイトがプロビジョニングされた後（「N 日目」）、アップロードまたはダウンロードの WAN 帯域幅を変更できます。プロビジョニング済みブランチ サイトの WAN 帯域幅の更新（5-24 ページ）も参照してください。

有効な帯域幅値はインターフェイスのタイプに応じて異なります。

- 10 ギガビット インターフェイス：0.1 ～ 10000 Mbps
- ギガビット インターフェイス：0.1 ～ 1000 Mbps
- セルラー インターフェイス：0.1 ～ 300 Mbps

帯域幅の設定を更新するには、次の手順を実行します。

手順

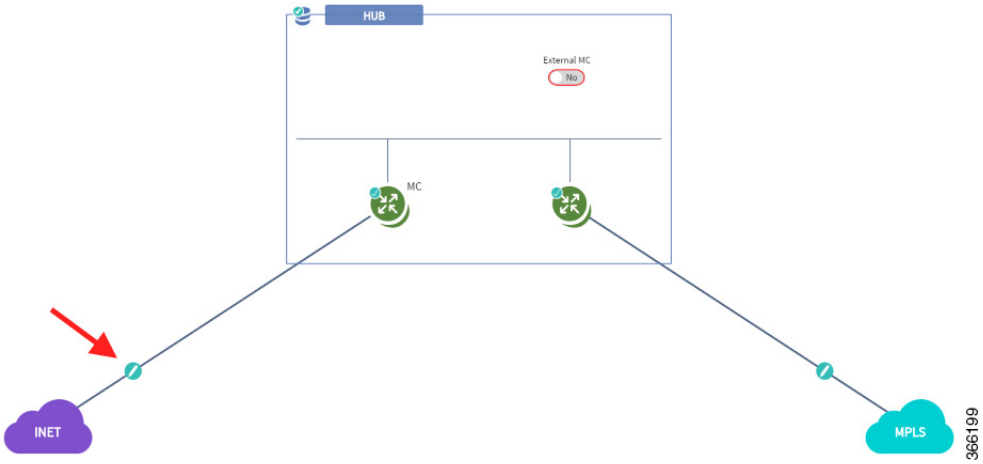
ステップ 1　IWAN アプリのホームページで、[Set up Branch Sites]をクリックします。

ステップ 2　[Sites]タブをクリックします。

ステップ 3　ハブ サイトの鉛筆アイコン（[Edit Site]）をクリックします。[IWAN Aggregation Site] ページが開きます。

（注）　IWAN のフロントページで [Configure Hub Site & Settings]をクリックし、[IWAN Aggregation Site] タブをクリックすることによっても、このページに移動できます。

ステップ 4　WAN リンクの鉛筆アイコンをクリックします。[Configure Link] ダイアログボックスが開きます。



ステップ 5　[Bandwidth] フィールドに新しい値を入力します。

ステップ 6　ダイアログ ボックスで [Save]をクリックします。

ステップ 7　ページの左下にある [Save & Continue]ボタンをクリックします。[Hub Site summary] ダイアログ ボックスが開きます。

ステップ 8　[Continue]をクリックしてサマリーを終了します。

ハブ サイトの QoS 帯域幅の割合の変更

ハブ サイトがプロビジョニングされた後（N 日目）、ハブ サイトの QoS 帯域幅の割合を変更できます。

手順

ステップ 1　IWAN アプリのホームページで、[Set up Branch Sites]をクリックします。[Sites] ページが開きます。

ステップ 2　[Sites]タブをクリックします。

ステップ 3　ハブ サイトの鉛筆アイコン（[Edit Site]）をクリックします。

（注）　IWAN のフロントページで [Configure Hub Site & Settings]をクリックし、[IWAN Aggregation Site] タブをクリックすることによっても、このページに移動できます。

ステップ 4　WAN リンク（ルータとクラウド間のリンク）上にある鉛筆アイコンをクリックします。[Configure Link] ダイアログボックスが開きます。

ステップ 5　[Service Provider] フィールドの横にある[Edit]（鉛筆）アイコンをクリックして、モデルの説明があるダイアログボックスを開きます。

ステップ 6　必要に応じて QoS 帯域幅の割合を変更します。

ステップ 7　[Update]をクリックします。変更した帯域幅の割合が WAN リンクに適用されます。

CHAPTER 5

ブランチ サイトの管理

この章の内容は、次のとおりです。

概要

ハブ サイトを設定してセットアップした後、デバイスを シスコ インテリジェント WANに追加してサイト向けにプロビジョニングします。

次の 2 種類のデバイスを追加してプロビジョニングできます。

- グリーンフィールド デバイス
  - グリーンフィールド デバイスは、購入後すぐに使用できる最新ルータです。
  - これらは Cisco Plug-n-Play（Cisco PnP）アプリケーションによって検出されます。
  - IWAN ベースの設定と同期化する既存の設定はなく、解決すべき設定の競合もありません。
- ブラウンフィールド デバイス
  - ブラウンフィールド デバイスは、シスコ インテリジェント WANに追加されている既存のサイトに属しています。
  - Cisco APIC-EM アプリケーションによって検出されます。

- IWAN ベースの設定と同期化する既存の設定が含まれている可能性があります。
- ブラウンフィールド デバイスのプロビジョニング時に、IWAN アプリは検証手順を実行し、設定の競合があるかどうかを確認します。警告またはエラーが報告された場合は、デバイスの問題を修正して再び検証します。ブラウンフィールド検証メッセージを参照してください。

NAT による IWAN アプリの動作

NAT の背後のスポーク

ネットワーク アドレス変換（NAT）は、パブリック インターネット クラウドに接続している WAN リンク上ですべてのトポロジをサポートします。つまり、グリーンフィールド デバイス（PnP ディスカバリを使用）とブラウンフィールド ブランチ デバイス（APIC-EM により検出）の両方をサポートします。

グリーンフィールド デバイスの場合は、PnP アプリケーションがパブリック NAT IP アドレスを使用して、NAT ルータを自動的に Cisco APIC-EM に追加します。

ブラウンフィールド デバイスの場合は、外部 IP アドレスまたはパブリック IP アドレスを使用してデバイスを検出します。

プロビジョニング時に Cisco APIC-EM から NAT ルータへの接続を有効にするには、次の標準ポートを使用します。

- SSH：ポート 22
- Telnet：ポート 23
- SNMP：ポート 161

プロビジョニングが完了し、ブランチ デバイスがループバック インターフェイスを介して Cisco APIC-EM により管理されるようになると、必要に応じてこれらの設定を削除できます。

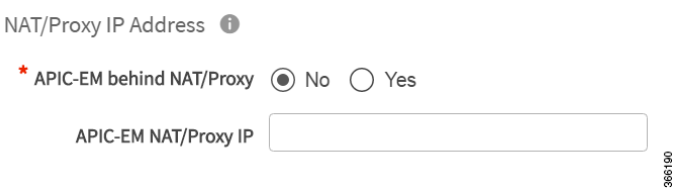
（注）　NAT ルータは Cisco IWAN によって管理されません。NAT ルータは手動で設定します。

NAT の背後の APIC-EM

IWAN アプリがサポートしているネットワーク トポロジは、APIC-EM コントローラがネットワーク アドレス変換（NAT）を介してスポーク（ブランチ）サイトと接続するトポロジです。

NAT ネットワークの背後の APIC-EM を設定する場合は、スポーク サイトをプロビジョニングする前に、APIC-EM コントローラの NAT パブリック IP アドレスを設定します。次の場所でアドレスを設定します。

IWAN アプリのホームページ > [Configure Hub Site & Settings]> [System] タブ > [NAT/Proxy IP Address] セクション



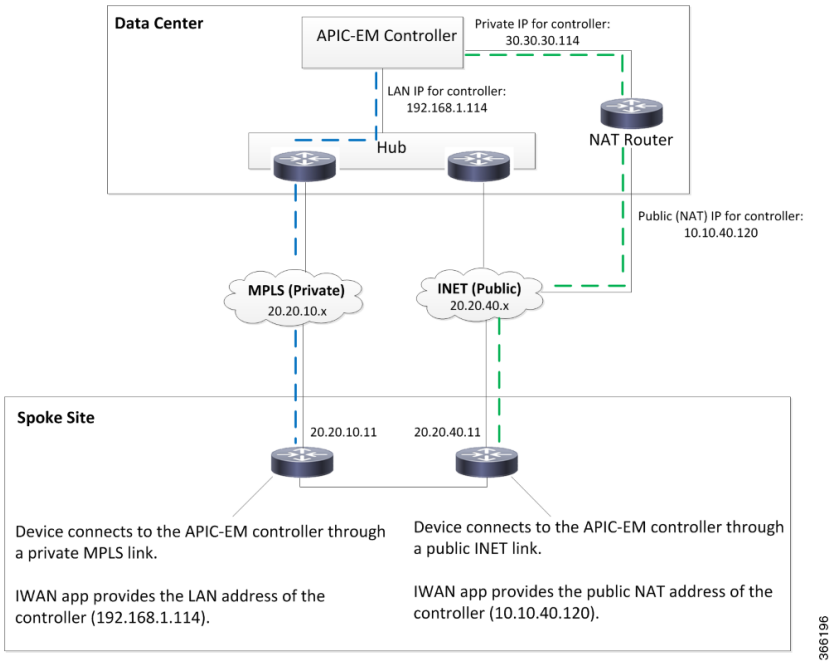
これは、「0 日目」（スポーク サイトをプロビジョニングする前）の要件です。「N 日目」（スポーク サイトがプロビジョニングされた後）のオプションではありません。

IWAN アプリによるスポーク デバイスへの NAT パブリック IP アドレスの提供

パブリック リンク（INET など）を介して APIC-EM コントローラに接続するスポーク デバイスには、コントローラの NAT パブリック アドレスが必要です。

- **グリーンフィールド サイト**：PnP アプリケーションは、自動的に APIC-EM のパブリック NAT IP アドレスを取得します。プロビジョニング時、IWAN アプリは、このアドレスをパブリック リンクで接続するスポーク デバイスに提供します。
- **ブラウンフィールド サイト**：プロビジョニング時、IWAN アプリは、APIC-EM コントローラの手動設定された NAT パブリック IP アドレスをパブリック リンクで接続するスポーク デバイスに提供します。

  注：プロビジョニング時に、ブラウンフィールド スポーク サイトのパブリック リンク インターフェイス IP アドレスまたは NAT パブリック IP アドレス（NAT の背後のスポークの場合）を使用して、ブラウンフィールド スポーク サイトを追加します。



制限事項

APIC-EM NAT IP は、スポーク サイトが設定されていない場合にのみ N 日目に変更できます。スポーク サイトが設定されているときに、APIC-EM NAT IP を変更する必要がある場合は、スポーク サイトを削除してから APIC-EM NAT IP を変更します。

ブランチ サイトの管理ワークフロー

表 5-1　ブランチ サイトの管理の基本的ワークフロー

番号	タスク	参照先
1	Cisco PnP アプリケーションによって検出されたデバイスをブートストラップする。	グリーンフィールド デバイスのブートストラップ（5-4 ページ）
2	デバイスを シスコ インテリジェント WAN に追加してサイト向けにプロビジョニングする。	グリーンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング（5-5 ページ） ブラウンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング（5-11 ページ）
3	サイトのステータスを確認する。	サイト ステータス情報の表示（5-21 ページ）

グリーンフィールド デバイスのブートストラップ

Cisco PnP アプリケーションによって検出されたデバイスをブートストラップできます。これらはグリーンフィールド デバイスです。

ブートストラップ ファイルをダウンロードするには、次の手順を実行します。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Manage Branch Sites]をクリックします。[Sites] ページが開きます。

ステップ 2　[Bootstrap]タブをクリックします。ダウンロード可能なブートストラップ ファイルが表示されます。

ステップ 3　[Download] 列で、[Download Bootstrap] アイコンをクリックし、コンピュータのローカル ディレクトリにブートストラップ ファイルをダウンロードします。このファイルは PnP call-home のテンプレートとして使用できます。

サイトに対してグリーンフィールド デバイスがプロビジョニングされた後、適切なブートストラップ ファイルが自動的にデバイスにアップロードされます。

詳細については、『*Cisco Open Plug-n-Play Agent Configuration Guide*』（http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pnp/configuration/xe-3e/pnp-xe-3e-book.html）を参照してください。

グリーンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング

Cisco PnP アプリケーションによって検出されたグリーンフィールド デバイスを追加し、ブランチ サイトに対してプロビジョニングするには、次の手順を実行します。

(注)

- 設定の保存

  サイトのプロビジョニングにデバイスを使用する前に、必要に応じて復元できるように、実行中の設定を IWAN_RECOVERY.cfg ファイルとしてフラッシュまたはブートフラッシュに保存することを推奨します。

- VTY ライン

  少なくとも 16 行のVTY ラインが設定されている必要があります。

- 4G/セルラー インターフェイスのサポート

  IWAN アプリは、ブランチ サイトの Cisco ISR4000 シリーズ ルータで 4G/セルラー インターフェイスの設定をサポートするようになりました。

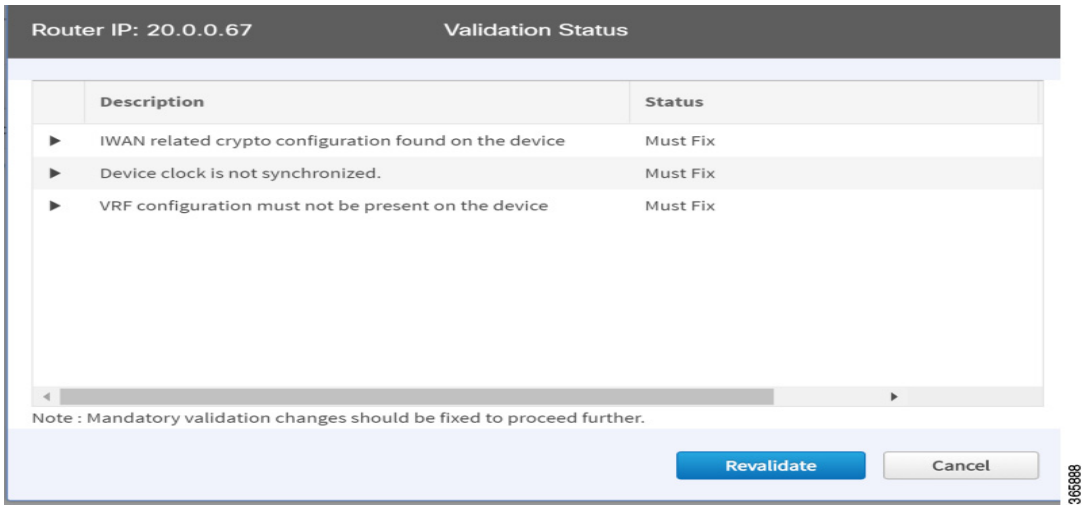
IWAN アプリは、ブランチ サイトのさまざまなタイプのルーティング デバイスとスイッチング デバイスをサポートしていますが、一部の機能は特定タイプのデバイスのみサポートします。次の表は、サポートされる接続タイプを示しています。

WAN 接続タイプ	接続タイプをサポートしているデバイス
インターネット（T1、E1、イーサネットなど）	すべて（All）
MPLS	すべて（All）
4G/セルラー インターフェイス	Cisco ISR 4000 シリーズ ルータ

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Manage Branch Sites]をクリックします。[Sites] ページが開きます。

ステップ 2　[Device(s)]タブをクリックします。要求されていないデバイスのリストが表示されます（次の図を参照）。



フィールド	説明
チェックボックス	要求されていないデバイスをプロビジョニング用に選択するには、このチェックボックスをオンにします。
Serial Number	デバイスのシリアル番号
IP アドレス	デバイスの IP アドレス。 (注)　NAT ルータがある場合は、NAT IP アドレスがこの列に表示されます。
タイプ	デバイスのタイプ。
Site Name	デバイスが属しているサイトの名前。サイト名を編集するには、サイト名をダブルクリックし、新しい名前を追加します。
Host Name	デバイスのホスト名
Discovered By	次のいずれかです。 • [PNP]：Cisco PnP アプリケーションによって検出。これはグリーンフィールド デバイスを示しています。 • [APIC]：Cisco APIC-EM アプリケーションによって検出。これはブラウンフィールド デバイスを示しています。

検証ステータス	グリーンフィールド デバイスに関する次の情報が表示されます。 • [N/A]：Cisco PnP アプリケーションによって検出されたデバイス。 ブラウンフィールド デバイスの場合は、次のいずれかです。 • [Success]：検証に成功し、ブランチ サイトに対してプロビジョニング可能なデバイス。これらのデバイスは、Cisco APIC-EM アプリケーションによって検出されるか、または [Add Device]タブをクリックして手動で追加します。 • [Failure]：修理が必要なデバイス。これらのデバイスは、Cisco APIC-EM アプリケーションによって検出されるか、または [Add Device]タブをクリックして手動で追加します。 • [Warning]：エラーを無視するか修理するかを選択できます。これらのデバイスは、Cisco APIC-EM アプリケーションによって検出されるか、または [Add Device]タブをクリックして手動で追加します。

ステップ 3　使用するグリーンフィールド デバイスの横にあるチェックボックスをオンにして、[Provision Site]タブをクリックします。[Select Topology]タブが開き、使用可能なトポロジが表示されます。

使用可能なトポロジのオプションは、IWAN アプリの [Network wide settings] ページで設定したハブ サイトのネットワーク設定に応じて異なります。ウィザードの手順 3：IP アドレス プールの設定（4-7 ページ）のサービス プロバイダー数の設定、およびウィザードの手順 4：サービス プロバイダーの設定（4-10 ページ）のトポロジを参照してください。

トポロジのオプションには以下が含まれていることがあります。

- 1 リンク オプション：1 つの WAN クラウドに接続しているハブ ルータが必要です。
- 2 リンク オプション：2 つの WAN クラウドに接続しているハブ ルータが必要です。
- 3 リンク オプション：3 つの WAN クラウドに接続しているハブ ルータが必要です。

（注）　デバイスがブラウンフィールドかグリーンフィールドかを確認するには、[Add Devices] ページの [Discovered By]列を調べます。[PNP] は、グリーンフィールド デバイスであることを示しています。[APIC] は、ブラウンフィールド デバイスであることを示しています。

（注）　最大 2 つのデバイスを選択できます。

（注）　グリーンフィールド デバイスとブラウンフィールド デバイスは、同じサイトに属することができません。

ステップ 4　ネットワークに適したトポロジをクリックします。L2/L3 オプションが表示されます。

（注）　表示されるトポロジ オプションは、ステップ 3 で選択したデバイスの数に応じて異なります。

ステップ 5　[L2]オプションをクリックします。[Configure Topology] ページが表示されます。

（注）　L3 は、グリーンフィールド デバイスではサポートされません。

ステップ 6　[Configure Topology]ページで、次のプロパティを指定します。

フィールド	説明
Site Name	サイト名。必要に応じて変更できます。
サイトの場所（Site Location）	地図上のサイトの場所を指定するには、[Set Geo]をクリックします。地図が表示されます。サイトをクリックすると、[Site Location] フィールドに入力されます。地図を終了するには、地図の外側のいずれかの場所をクリックします。
POP to Connect	ドロップダウン リストからこのブランチ サイトの優先ハブ サイトを選択します。
Select WAN	ドロップダウン リストから WAN を選択します。

ステップ 7　ブランチ デバイスの WAN 設定を行います。次の手順を実行します。

a. WAN クラウドの横にある [+]アイコンをクリックします。[Configure WAN Cloud]ダイアログボックスが表示されます。[Configure WAN Cloud]ダイアログボックスに表示されるフィールドは、ステップ 6 で選択した WAN のタイプに応じて異なります。

b. パブリック WAN の場合は、[Configure WAN Cloud]ダイアログボックスに次のフィールドが表示されます。必要なプロパティを入力して、[Save]をクリックします。

フィールド	説明
WAN Type	パブリック
Interface Type	インターフェイスのタイプ。値：T1、E1、Ethernet、Cellular
インターフェイス	WAN クラウドに接続するインターフェイスをドロップダウン リストから選択します。
Connect to WAN	接続方法。
NAT Enabled	NAT IP アドレスを使用する場合は、このオプションをオンにします。
NAT IP Address	パブリック IP アドレス
Enable	必要に応じて、次の 2 つのオプション ボタンのいずれかを選択します。 • [Static IP]：オンにすると、追加のフィールド（[WAN IP Address]、[WAN IP Mask]、[WAN Gateway IP Address]）が表示されます。 • DHCP
アップロード（Mbps）	アップロード帯域幅（Mbps 単位）。

ダウンロード（Mbps）	E1 インターフェイス：事前設定された帯域幅値 3。 T1 インターフェイス：事前設定された帯域幅値 1.5。 GigabitEthernet インターフェイス：ドロップダウン リストから帯域幅を選択するか、0.1 ～ 1000 の値を入力します。 TenGigabitEthernet インターフェイス：ドロップダウン リストから帯域幅を選択するか、0.1 ～ 9000 の値を入力します。 E1、T1、GigabitEthernet、TenGigabitEthernet 以外のタイプのインターフェイスの場合、デフォルトの範囲は 0.1 ～ 9000 Mbps です。
サービス プロファイル	ドロップダウン リストからサービス プロファイルを選択します。 ドロップダウン リストには、デフォルトのサービス プロファイルと、[Service Providers] タブで設定したカスタムの 8 Class サービス プロファイルが含まれています。

c. プライベート WAN の場合は、[Configure WAN Cloud]ダイアログボックスに次のフィールドが表示されます。必要なプロパティを入力して、[Save]をクリックします。

フィールド	説明
WAN Type	プライベート
Interface Type	インターフェイスのタイプ。値：T1、E1、または Ethernet。
インターフェイス	ドロップダウン リストからインターフェイスを選択します。
Connect to WAN	接続方法。
CE IP Address	カスタマー エッジ サーバの IP アドレス。インターフェイスに静的 IP アドレスが設定済みの場合、このフィールドは自動的に入力されます。 （注）　[IWAN Aggregation Site] でハブ サイトを設定するときに作成したリンクの数によっては、CE デバイスに追加の IP アドレスを指定する必要があります。
CE IP Mask	CE IP アドレスのマスク。
PE IP Address	プロバイダー エッジ サーバの IP アドレス。インターフェイスに IP アドレスとデフォルト ゲートウェイがある場合、このフィールドは自動的に入力されます。
ダウンロード（Mbps）	E1 インターフェイス：事前設定された帯域幅値 3。 T1 インターフェイス：事前設定された帯域幅値 1.5。 GigabitEthernet インターフェイス：ドロップダウン リストから帯域幅を選択するか、0.1 ～ 1000 の値を入力します。 TenGigabitEthernet インターフェイス：ドロップダウン リストから帯域幅を選択するか、0.1 ～ 9000 の値を入力します。 E1、T1、GigabitEthernet、TenGigabitEthernet 以外のタイプのインターフェイスの場合、デフォルトの範囲は 0.1 ～ 9000 Mbps です。
サービス プロファイル	ドロップダウン リストからサービス プロファイルを選択します。 ドロップダウン リストには、デフォルトのサービス プロファイルと、[Service Providers] タブで設定されたカスタム サービス プロファイル（4 Class、5 Class、6 Class、8 Class）がすべて含まれています。

ステップ 8　LAN の設定を行います。次の手順を実行します。

グリーンフィールド デバイスに関する次の情報が表示されます。

（注）　LAN グリーンフィールド IP アドレス プールは、ハブのプロビジョニング時に作成するか、グリーンフィールドの導入のためにハブをプロビジョニングした後に追加できます。LAN グリーンフィールド IP アドレス プールがない場合は、汎用プールの IP アドレスが自動的に使用されます。

a. LAN の横にある [+]アイコンをクリックします。サイトに対してサイト固有の IP アドレス プールが設定されている場合は、[Configure VLAN]ダイアログボックスが開きます。

b. 次のプロパティを入力して、[Save]をクリックします。

フィールド	説明
LAN インターフェイス	
サイト名 Interface	LAN インターフェイスを入力するか、ドロップダウン リストから選択します。
VLAN	
VLAN Type	VLAN のタイプを入力するか、ドロップダウン リストから選択します。 デフォルト値：Data、Guest、Voice & Video、Wireless。 カスタム VLAN を作成するには、最後の VLAN の [+]アイコンをクリックし、VLAN の名前を入力します。
VLAN ID	数値の範囲：1 ～ 98、100 ～ 1001、1006 ～ 4094。 VLAN ID は複製できません。
Total IPs	VLAN 内のホスト数。

ステップ 9　[Provisioning Sites] ページで、[Apply Changes]をクリックします。[Provisioning Site Summary]ダイアログボックスが開き、設定の概要が表示されます。

ステップ 10　情報を確認し、次のいずれかを実行します。

- [Apply Now] オプション ボタンをクリックして、[Submit] をクリックします。
- [Schedule] オプション ボタンをクリックして、プロビジョニングを適用する日時を指定し、[Submit] をクリックします。

（注）　[Apply Now]オプションを選択した場合、スケジュール済みのワークフローとの競合は検証されません。変更に基づいてスケジュール済みのジョブを再評価し、必要に応じてジョブを更新する必要があります。スケジュール済みジョブがアクティブなときに競合が発生すると、サイトのプロビジョニングに失敗する可能性があります。

ブラウンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング

Cisco APIC-EM アプリケーションによって検出されたブラウンフィールド デバイスを追加し、ブランチ サイトに対してプロビジョニングするには、次の手順を実行します。

ブラウンフィールド デバイスは [Devices] タブに自動的に表示されません。最初にブラウンフィールド デバイスを Cisco IWAN に追加してから、ブランチ サイトに対してプロビジョニングする必要があります。

(注)

- 設定の保存

  サイトのプロビジョニングにデバイスを使用する前に、必要に応じて復元できるように、実行中の設定を IWAN_RECOVERY.cfg ファイルとしてブートフラッシュに保存することを推奨します。

- VTY ライン

  少なくとも 16 行のVTY ラインが設定されている必要があります。

- SNMP

  SNMP バージョン 2 またはバージョン 3 が設定されているデバイスは、ブランチ デバイスとして使用できます。

- 4G/セルラーのサポート

  IWAN アプリは、ブランチ サイトの Cisco ISR4000 シリーズ ルータで 4G/セルラー インターフェイスの設定をサポートするようになりました。

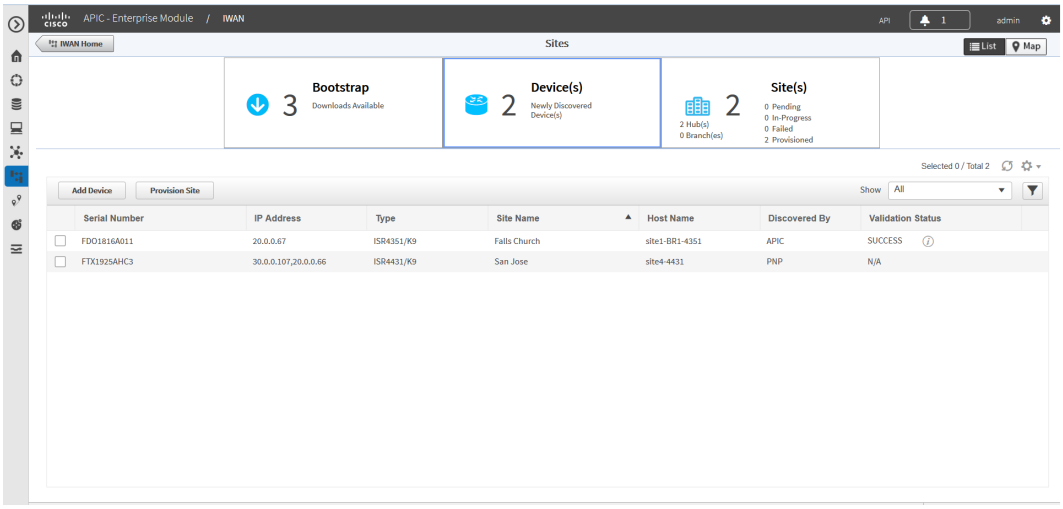
IWAN アプリは、ブランチ サイトのさまざまなタイプのルーティング デバイスとスイッチング デバイスをサポートしていますが、一部の機能は特定タイプのデバイスのみサポートします。次の表は、サポートされる接続タイプを示しています。

WAN 接続タイプ	接続タイプをサポートしているデバイス
インターネット（T1、E1、イーサネットなど）	すべて（All）
MPLS	すべて（All）
4G/セルラー	Cisco ISR 4000 シリーズ ルータ

手順

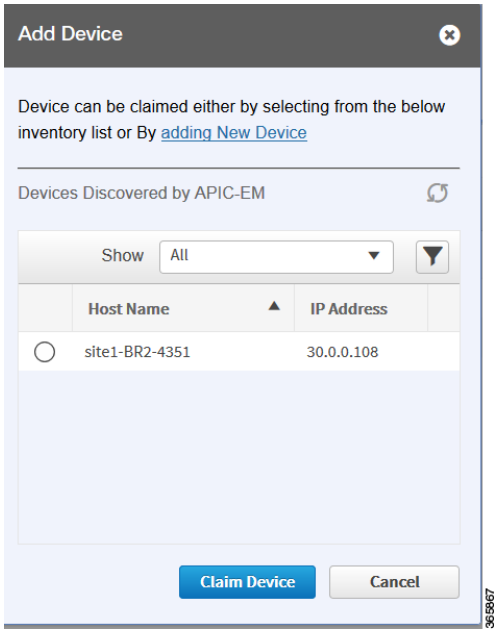
ステップ 1　シスコ インテリジェント WANのホームページで、[Manage Branch Sites]をクリックします。[Sites] ページが開きます。

ステップ 2　[Device(s)]タブをクリックします。次のページが表示されます。



ステップ 3　ブラウンフィールド デバイスを追加するには、[Add Device]タブをクリックします。[Add Device] ダイアログボックスが開き、Cisco APIC-EM アプリケーションによって検出されたデバイスのリストが表示されます（次の図を参照）。

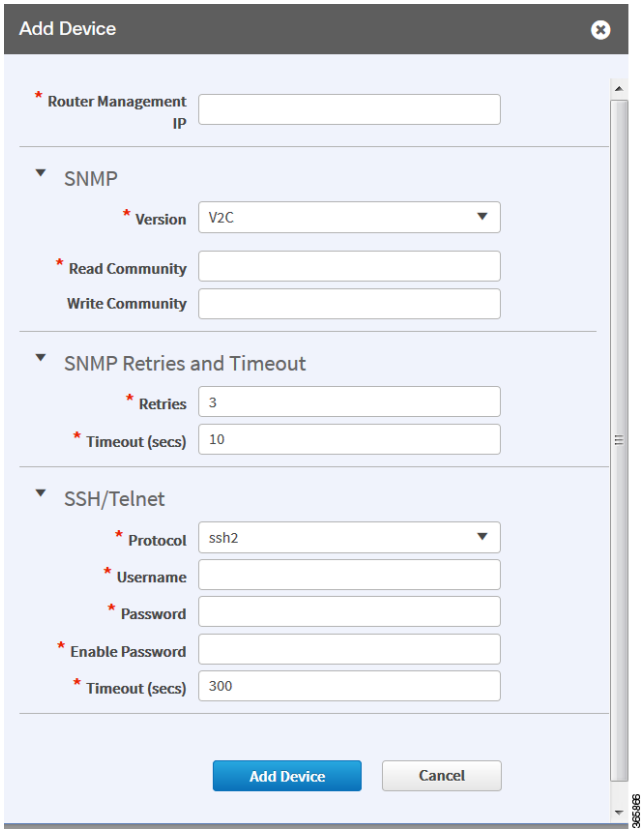
（注）　さらに、Cisco APIC EM の検出機能を使用してデバイスを追加できます。



ステップ 4　次のいずれかを実行します。

- Cisco APIC-EM によって検出された既存のデバイスを選択する場合：[Devices Discovered by APIC-EM] 領域で、シスコ インテリジェント WANに追加するデバイスの横にあるオプション ボタンをクリックし、[Claim Device]をクリックします（上の図を参照）。要求したデバイスが [Devices] ページに追加され、プロビジョニングできるようになります。

- 新しいデバイスを追加する場合：[Adding New Device]をクリックします（上の図を参照）。[Add Device] ダイアログボックスが開きます。このダイアログボックスで、新しいデバイスの IP アドレスやその他のプロパティを指定し、[Add Device]をクリックします（次の図を参照）。



フィールド	説明
Router Management IP	新しいデバイスの IP アドレス。 NAT ルータの背後にスポーク デバイスがあり、その NAT ルータを管理ルータにする場合は、このフィールドに NAT ルータの IP アドレスを入力します。
SNMP	
Version	SNMP のバージョン番号。 選択したバージョン番号に応じて異なるプロパティが表示されます。
Read Community （SNMP V2C を選択した場合に表示）	SNMP V2C read コミュニティ ストリング。
Write Community （SNMP V2C を選択した場合に表示）	（任意）SNMP V2C write コミュニティ ストリング。

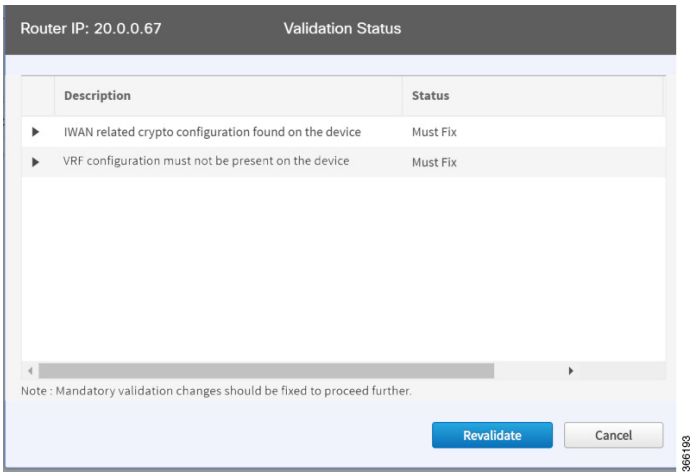
フィールド	説明
モード （SNMP V3 を選択した場合に表示）	ドロップダウン リストからモードを選択します。次のオプションがあります。 • 認証および暗号化 • [No Authentication and No Encryption] • [Authentication and No Encryption]
Auth.タイプ （SNMP V3 を選択した場合に表示）	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合に表示されます。 ドロップダウン リストから、認証タイプを選択します。次のオプションがあります。 • HMAC-SHA • HMAC-MDS
Username （SNMP V3 を選択した場合に表示）	SNMP V3 を選択した場合に表示されます。 認証ユーザ名
Auth.Password] （SNMP V3 を選択した場合に表示）	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合に表示されます。 認証ユーザ名のパスワード。
Encryption Type （SNMP V3 を選択した場合に表示）	[Mode] フィールドで [Authentication and Encryption] を選択した場合に表示されます。 暗号化ユーザ名。
Encryption Password （SNMP V3 を選択した場合に表示）	[Mode] フィールドで [Authentication and Encryption] を選択した場合に表示されます。 暗号化ユーザ名のパスワード。
SNMP の再試行回数およびタイムアウト	
Retries	SNMP の再試行回数。デフォルト:3
Timeout (secs)	SNMP 要求がタイム アウトしたと見なされるまでの待機秒数。 デフォルト:10
SSH/Telnet	
Protocol	ホストとの通信に使用されるプロトコル（Telnet または SSH）。
Username	SSH または Telnet のユーザ名。
Password	SSH または Telnet のパスワード。
Enable Password	ユーザ名のイネーブルパスワード。
Timeout (secs)	SSH または Telnet 要求がタイム アウトしたと見なされるまでの待機秒数。

デバイスがバックグラウンドで検証され、プロビジョニングに適しているかどうかが判断されます。以下が実行されます。

Cisco IWAN アプリはルータにアクセスしてその設定をチェックし、Cisco IWAN アプリと競合する可能性がある設定が含まれているかどうかを確認します。これはブラウンフィールド検証と呼ばれます。

ルータに競合する設定がない場合は、デバイスの上部にオレンジ色のアイコンが表示され、[Configure Router] ダイアログが開きます。

ルータに競合する設定がある場合は、[Validation Status] ダイアログが開き、すべての検証エラーが一覧表示されます（次の図を参照）。



c. 検証ステータスは [Warning] または [Must Fix] のいずれかになります。次の手順を実行します。

- 検証ステータスが [Warning] の場合は、エラーを修正または無視することができます。
- 検証ステータスが [Must Fix] の場合は、説明で示された設定を削除し、[Revalidate]をクリックします。

[Validation Status] ダイアログボックスに表示されるメッセージの詳細については、付録 A「ブラウンフィールド検証メッセージ」を参照してください。

ステップ 5　[Devices] ページで、サイトに対してプロビジョニングするブラウンフィールド デバイスの横にあるチェックボックスをオンにして、[Provision Site]タブをクリックします。[Select Topology]タブが開き、使用可能なトポロジが表示されます。

使用可能なトポロジのオプションは、IWAN アプリの [Network wide settings] ページで設定したハブ サイトのネットワーク設定に応じて異なります。ウィザードの手順 3：IP アドレス プールの設定（4-7 ページ）のサービス プロバイダー数の設定、およびウィザードの手順 4：サービス プロバイダーの設定（4-10 ページ）のトポロジを参照してください。

トポロジのオプションには以下が含まれていることがあります。

- 1 リンク オプション：1 つの WAN クラウドに接続しているハブ ルータが必要です。
- 2 リンク オプション：2 つの WAN クラウドに接続しているハブ ルータが必要です。
- 3 リンク オプション：3 つの WAN クラウドに接続しているハブ ルータが必要です。

(注)　デバイスがブラウンフィールドかグリーンフィールドかを確認するには、[Add Devices] ページの [Discovered By]列を調べます。[PNP] は、グリーンフィールド デバイスであることを示しています。[APIC] は、ブラウンフィールド デバイスであることを示しています。

(注)　最大 2 つのデバイスを選択できます。

ステップ 6　ネットワークに適したトポロジをクリックします。L2/L3 オプションが表示されます。

(注)　表示されるトポロジ オプションは、ステップ 5 で選択したデバイスの数に応じて異なります。

ステップ 7　LAN サイトの設定に応じて、適切な [L2] または [L3]オプションをクリックします。[Configure Topology] ページが表示されます。

(注)　ブランチ デバイスの VLAN が同じサブネット上にある場合は、[L2] を選択します。ブランチ デバイスの VLAN が異なるサブネット上にある場合は、[L3] を選択します。

ステップ 8　[Configure Topology]ページで、次のプロパティを指定します。

フィールド	説明
Site Name	サイト名。必要に応じて変更できます。
サイトの場所（Site Location）	地図上のサイトの場所を指定するには、[Set Geo]をクリックします。地図が表示されます。サイトをクリックすると、[Site Location] フィールドに入力されます。地図を終了するには、地図の外側のいずれかの場所をクリックします。
POP to Connect	[IWAN Aggregation Site]で指定したハブをドロップダウン リストから選択します。
Select WAN	ドロップダウン リストから WAN を選択します。

ステップ 9　ブランチ デバイスの WAN 設定を行います。次の手順を実行します。

a. WAN クラウドの横にある [+]アイコンをクリックします。[Configure WAN Cloud]ダイアログボックスが表示されます。[Configure WAN Cloud]ダイアログボックスに表示されるフィールドは、ステップ 8 で選択した WAN のタイプに応じて異なります。

b. パブリック WAN の場合は、[Configure WAN Cloud]ダイアログボックスに次のフィールドが表示されます。必要なプロパティを入力して、[Save]をクリックします。

フィールド	説明
WAN Type	パブリック
Interface Type	インターフェイスのタイプ。値:T1、E1、Ethernet、Cellular
インターフェイス	WAN クラウドに接続するインターフェイスをドロップダウン リストから選択します。

Connect to WAN	接続方法。
NAT Enabled	NAT IP アドレスを使用する場合は、このオプションをオンにします。
NAT IP Address	パブリック IP アドレス
Enable	必要に応じて、次の 2 つのオプション ボタンのいずれかを選択します。 • [Static IP]:オンにすると、追加のフィールド([WAN IP Address]、[WAN IP Mask]、[WAN Gateway IP Address])が表示されます。 • DHCP
アップロード（Mbps）	アップロード帯域幅(Mbps 単位)。
ダウンロード（Mbps）	E1 インターフェイス:事前設定された帯域幅値 3。 T1 インターフェイス:事前設定された帯域幅値 1.5。 GigabitEthernet インターフェイス:ドロップダウン リストから帯域幅を選択するか、0.1 ～ 1000 の値を入力します。 TenGigabitEthernet インターフェイス:ドロップダウン リストから帯域幅を選択するか、0.1 ～ 10000 の値を入力します。 E1、T1、GigabitEthernet、TenGigabitEthernet 以外のタイプのインターフェイスの場合、デフォルトの範囲は 0.1 ～ 10000 Mbps です。
サービス プロファイル	ドロップダウン リストからサービス プロファイルを選択します。 ドロップダウン リストには、デフォルトのサービス プロファイルと、[Service Providers] タブで設定したカスタムの 8 Class サービス プロファイルが含まれています。

c. プライベート WAN の場合は、[Configure WAN Cloud]ダイアログボックスに次のフィールドが表示されます。必要なプロパティを入力して、[Save]をクリックします。

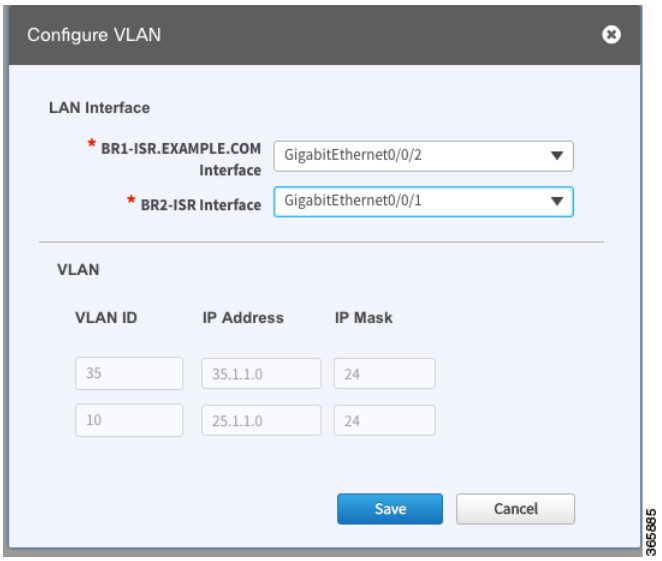
フィールド	説明
WAN Type	プライベート
Interface Type	インターフェイスのタイプ。値:T1、E1、または Ethernet。
インターフェイス	ドロップダウン リストからインターフェイスを選択します。
Connect to WAN	接続方法。
CE IP Address	カスタマー エッジ サーバの IP アドレス。インターフェイスに静的 IP アドレスが設定済みの場合、このフィールドは自動的に入力されます。 (注)　[IWAN Aggregation Site] でハブ サイトを設定するときに作成したリンクの数によっては、CE デバイスに追加の IP アドレスを指定する必要があります。
CE IP Mask	CE IP アドレスのマスク。
PE IP Address	プロバイダー エッジ サーバの IP アドレス。インターフェイスに IP アドレスとデフォルト ゲートウェイがある場合、このフィールドは自動的に入力されます。

ダウンロード（Mbps）	E1 インターフェイス：事前設定された帯域幅値 3。 T1 インターフェイス：事前設定された帯域幅値 1.5。 GigabitEthernet インターフェイス：ドロップダウン リストから帯域幅を選択するか、0.1 ～ 1000 の値を入力します。 TenGigabitEthernet インターフェイス：ドロップダウン リストから帯域幅を選択するか、0.1 ～ 10000 の値を入力します。 E1、T1、GigabitEthernet、TenGigabitEthernet 以外のタイプのインターフェイスの場合、デフォルトの範囲は 0.1 ～ 10000 Mbps です。
サービス プロファイル	ドロップダウン リストからサービス プロファイルを選択します。 ドロップダウン リストには、デフォルトのサービス プロファイルと、[Service Providers] タブで設定されたカスタム サービス プロファイル（4 Class、5 Class、6 Class、8 Class）がすべて含まれています。

ステップ 10　LAN の設定を行います。次の手順を実行します。

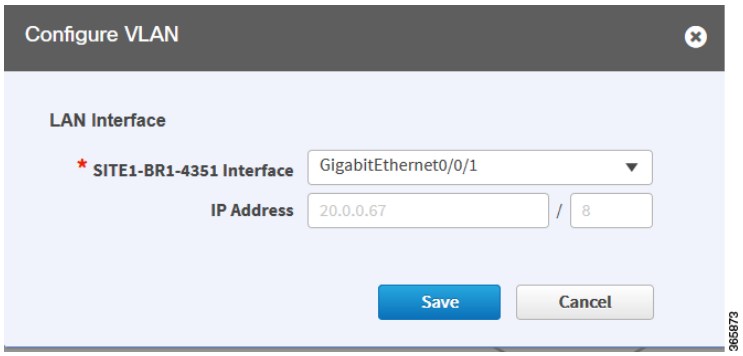
LAN の横にある [+]アイコンをクリックします。L2 トポロジを選択し、LAN インターフェイスが物理インターフェイスまたはスイッチポート インターフェイスである場合は、[Configure VLAN] ダイアログボックスが開きます（下の図を参照）。ドロップダウン リストから LAN インターフェイスを選択し、[Save]をクリックします。

（注）
- デュアル ルータ トポロジを選択した場合は、デバイス間の共通の VLAN が表示されます。
- ブラウンフィールド サイトに対してサイト固有の IP アドレス プールが設定されていないことを確認してください。
- [Configure VLAN] ダイアログボックスに表示される VLAN 情報は、ルータに対して選択した LAN インターフェイスに基づいて自動的に入力されます。
- [Configure VLAN] ダイアログボックスの自動入力情報は編集できません。
- LAN ブラウンフィールド IP アドレス プールは、ハブのプロビジョニング時に作成するか、ブラウンフィールドの導入のためにハブをプロビジョニングした後に追加できます。LAN ブラウンフィールド IP アドレス プールがない場合は、ブラウンフィールド デバイスに対してサイト固有のプールが自動的に作成されます。



L3 トポロジを選択した場合は、次のような [Configure VLAN] ダイアログボックスが開きます（次の図を参照）。次の手順を実行します。

a. ドロップダウン リストから LAN インターフェイスを選択します。IP アドレスが自動的に入力されます。

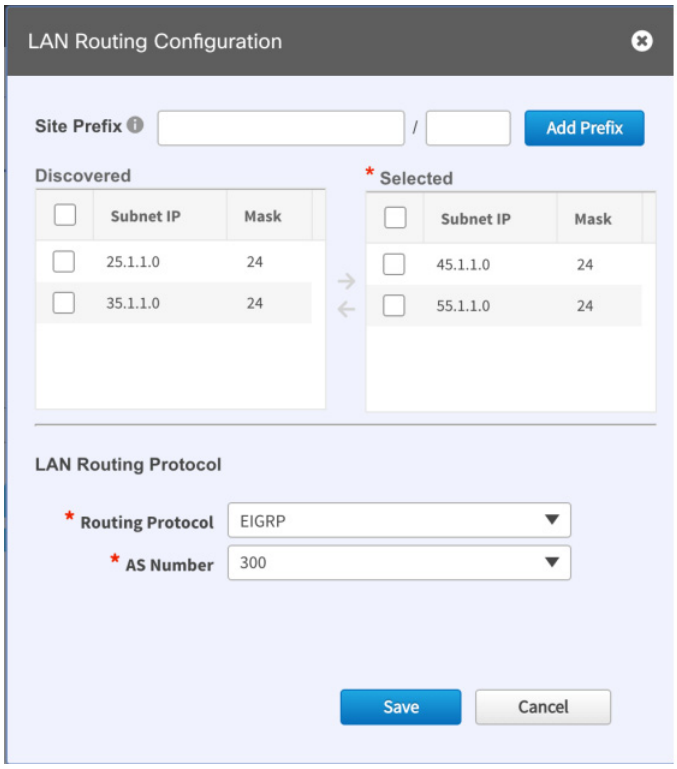


b. [Save（保存）] をクリックします。

c. デュアル ルータがある場合は、そのデバイスの LAN インターフェイスを選択して、[Save]をクリックします。

d. [Routing Configuration] の上にある [+]アイコンをクリックします。[LAN Routing Configuration] ダイアログボックスが開きます（次の図を参照）。プロパティを入力して、[Save]をクリックします。

（注）　デバイスごとに VLAN が表示されます。



フィールド	説明
Site Prefix	自動学習されたサイトのネットワーク プレフィックス。
[Add Prefix] ボタン	手動でサイト プレフィックスを追加するには、このボタンをクリックします。
[Discovered] ペイン	シスコ インテリジェント WANによって自動的に検出されたプレフィックス。
矢印	[Discovered] ペインから [Selected] ペインにプレフィックスを移動するには、[-->] 矢印をクリックします。 [Selected] ペインから [Discovered] ペインにプレフィックスを移動するには、[<--] 矢印をクリックします。
[Selected] ペイン	選択されたプレフィックスのリスト。
LAN ルーティング プロトコル	
Routing Protocol	デバイスで実行されているデフォルトのルーティング プロトコル。可能な値：EIGRP または OSPF (注)　EIGRP および OSPF はサポートされているルーティング プロトコルです。つまり、LAN-WAN の再配分はシスコ インテリジェント WANによって実行されます。シスコ インテリジェント WANは BGP プロトコルに対して LAN-WAN の再配分を実行しません。
Area Number/AS Number	ルーティング プロトコルに応じて、以下を入力します。 • OSPF のエリア番号。 • EIGRP の AS 番号。 (注)　デュアル ルータ サイトの場合は、OSPF のエリア番号および EIGRP の AS 番号が両方のデバイスで同じであることを確認してください。

ステップ 11　[Provisioning Sites] ページで、[Apply Changes]をクリックします。[Provisioning Site Summary]ダイアログボックスが開き、設定の概要が表示されます。

ステップ 12　情報を確認し、次のいずれかを実行します。

- [Apply Now] オプション ボタンをクリックして、[Submit] をクリックします。
- [Schedule] オプション ボタンをクリックして、プロビジョニングを適用する日時を指定し、[Submit] をクリックします。

(注)　[Apply Now]オプションを選択した場合、スケジュール済みのワークフローとの競合は検証されません。変更に基づいてスケジュール済みのジョブを再評価し、必要に応じてジョブを更新する必要があります。スケジュール済みジョブがアクティブなときに競合が発生すると、サイトのプロビジョニングに失敗する可能性があります。

サイト ステータス情報の表示

サイトに関する情報を表示して全体的なステータスを確認するには、次の手順を実行します。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Manage Branch Sites]をクリックします。[Sites] ページが開きます。

ステップ 2　[Site(s)]タブをクリックします。次のプロパティが表示されます。

フィールド	説明
状態	ハブの状態とサイトの状態。
App Health	ハブのアプリケーションの状態。 この情報を表示するには、Prime クレデンシャルを設定する必要があります。
サイト	必要に応じてハブ名またはサイト名をクリックし、次の詳細を表示します。 • [Site status]:サイトがプロビジョニングされているかどうか。 • [Application status]:アプリケーションのステータス。 • [Alarms] タブ:サイトで問題が発生すると、このタブに問題に関する説明が表示されます。さらに、問題をトラブルシューティングして解決するための提案も示されます。 • [Hub Topology] または [Site Topology] タブ:サイトのトポロジ。サイト名、サイトの場所、優先 POP などが含まれています。詳細を表示するには、トポロジ内のデバイスや WAN クラウドの上にカーソルを移動します。 • [IP Address Allocation] タブ:デバイスのリスト。サブネットマスクとデバイスが割り当てられている IP アドレス プールが含まれています。 • [Application] タブ:サイトでのアプリケーションの使用状況がグラフ表示されます。以下がグラフに表示されます。 – サイトで設定されているさまざまなアプリケーション – 各アプリケーションの帯域幅使用量 – 各アプリケーションの統計的なトレンド
Location	サイトの場所
Status（ステータス）	サイトがプロビジョニングされているかどうか。

Action	次のいずれかです。 • [Delete] アイコン：問題があるサイトを削除するには、このアイコンをクリックします。ハブ サイトの削除（9-4 ページ）、中継ハブの削除（9-5 ページ）、またはブランチ サイトの削除（9-5 ページ）を参照してください。 • [Recovery] アイコン：サイトのリカバリが可能な場合に使用できます。シスコ インテリジェント WANサイトのリカバリ（9-4 ページ）を参照してください。 • [Edit]（鉛筆）アイコン：以下を実行するときにクリックします。 – ハブのプロビジョニング後にサイトのプレフィックスを追加または削除する。このオプションは、L3 ブラウンフィールド サイトでのみ使用できます。サイト プレフィックスの追加または削除（9-7 ページ）を参照してください。 – 選択したブランチ サイトの QoS 帯域幅の割合を変更する。ブランチ サイトの QoS 帯域幅の割合の変更（5-27 ページ）。

WAN リンクに対する 4G/セルラー技術のサポート

IWAN アプリは、WAN 接続オプションとして、ブランチ サイトの Cisco ISR 4000 シリーズ ルータによる 4G セルラー接続の使用をサポートしています。

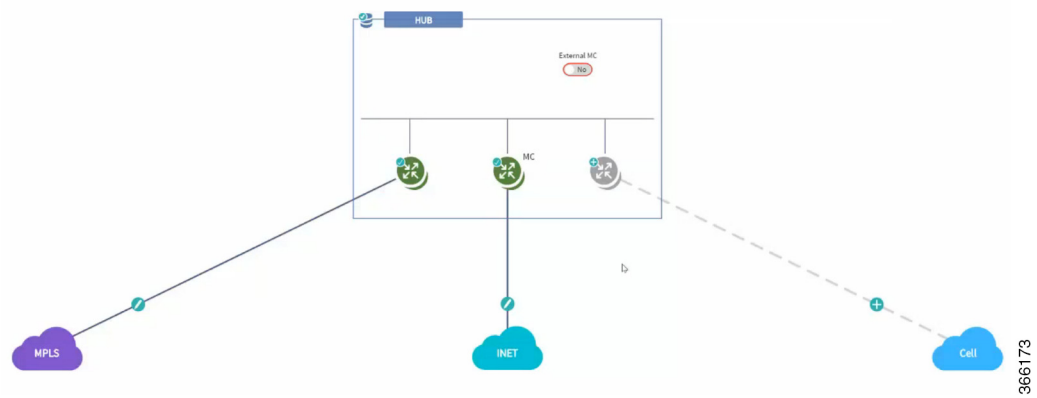
シナリオ例

プロビジョニングの完全な手順は、グリーンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング（5-5 ページ）およびブラウンフィールド デバイスの追加およびブランチ サイトに対するプロビジョニング（5-11 ページ）の項に記載されています。以下に、WAN リンクで 4G 接続を使用するシナリオを例にあげて、プロビジョニング手順の概要を示します。

手順

ステップ 1　[Configure Hub Site & Settings]> [Service Providers]タブで、サービス プロバイダーに 4G セルラー接続を設定します。セルラー接続には WAN タイプ値として Public を設定する必要があることに注意してください。

ステップ 2　[Configure Hub Site & Settings]> [IWAN aggregation site] タブのトポロジのグラフィック表示で、ハブ サイト デバイスを 4G セルラー WAN に接続します。



ステップ 3　Cisco ISR 4000 シリーズのデバイスを含むブランチで、デバイスを 4G セルラー WAN に接続します。

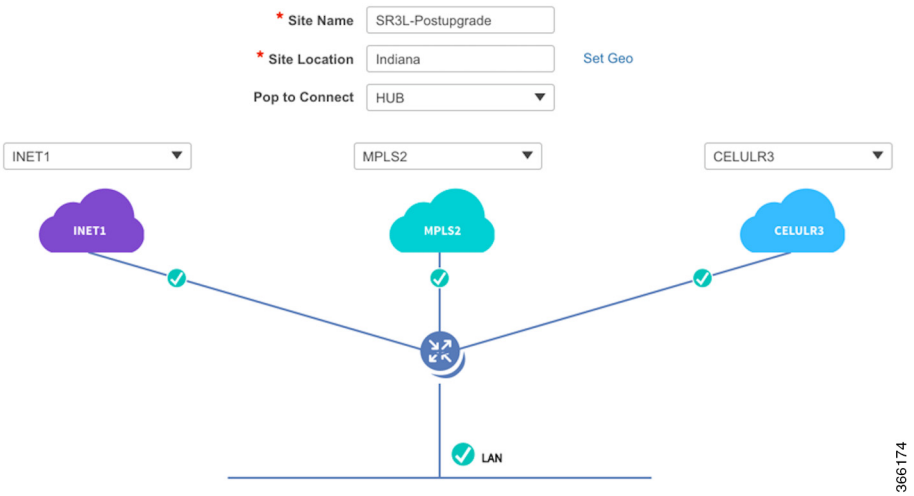
a. [Sites] ページで、[Device(s)] タブを選択します。要求されていない Cisco ISR 4000 シリーズ デバイスを選択します。[Provisioning Site] ページが表示されます。

b. [Select Topology] ステップで、トポロジを選択して [Next]をクリックします。

c. [Select L2/L3] ステップで、オプションを選択して [Next]をクリックします。

d. [Configure Topology] ステップで、デバイスと WAN「クラウド」オプションの 1 つをつないでいるリンク上のプラス記号をクリックします。[Configure WAN Cloud] ポップアップが開きます。デバイスのインターフェイスごとに、必要な詳細を設定して [Save]をクリックし、その次のインターフェイスを設定します。ポップアップの [Connect to WAN] フィールドに 4G セルラー WAN の名前が表示されたら、[Interface] フィールドに [Cellular] が設定されていることを確認します。[Save]をクリックし、デバイスの WAN 接続の設定を完了させます。[Configure VLAN] ポップアップが開きます。

e. LAN を設定するか、既存の設定を確認し、[Save] をクリックします。[Provisioning Site] ページが開き、ブランチ デバイスの WAN 接続が 4G セルラー WAN リンクも含めて表示されます。デバイスの WAN 接続はチェック アイコンが付いた実線で表示され、有効な設定であることが示されます。



f. [Apply Changes]をクリックして、設定をデバイスに適用します。[Provisioning Site Summary] ページが表示されます。サマリーにセルラー WAN リンクが表示されます。

注意事項と制限事項

グリーンフィールド デバイス

サポートされるトポロジ

- L2 グリーンフィールド シングル ルータ 2 リンク
- L2 グリーンフィールド シングル ルータ 3 リンク
- L2 グリーンフィールド デュアル ルータ 3 リンク
- L2 グリーンフィールド デュアル ルータ デュアル リンク
- L2 グリーンフィールド シングル ルータ シングル リンク

セルラー リンクを管理インターフェイスに使用

IWAN アプリで管理インターフェイスとして 4G セルラーを使用するには、セルラー インターフェイスが APIC-EM コントローラから到達可能でなければなりません。

ブラウンフィールド デバイス

サポートされるトポロジ

- ブラウンフィールド L2/L3 シングル ルータ シングル リンク
- ブラウンフィールド L2/L3 シングル ルータ デュアル リンク
- ブラウンフィールド L2/L3 シングル ルータ 3 リンク
- ブラウンフィールド L2/L3 デュアル ルータ シングル リンク
- ブラウンフィールド L2/L3 デュアル ルータ 3 リンク

セルラー リンクを管理インターフェイスに使用：サポート対象

IWAN アプリで管理インターフェイスとして 4G セルラーを使用するには、セルラー インターフェイスが APIC-EM コントローラから到達可能でなければなりません。

セルラー クラウドに接続されているハブ WAN アドレスに到達可能であること

プロビジョニング前に、セルラー クラウドに接続されているハブ WAN アドレスにセルラー ブランチ デバイスから到達できなければなりません。

プロビジョニング済みブランチ サイトの WAN 帯域幅の更新

ブランチ サイトがプロビジョニングされた後（「N 日目」）、アップロードまたはダウンロードの WAN 帯域幅を変更できます。プロビジョニング済みハブ サイトの WAN 帯域幅の更新（4-22 ページ）も参照してください。

有効な帯域幅値はインターフェイスのタイプに応じて異なります。

- 10 ギガビット インターフェイス：0.1 ～ 10000 Mbps
- ギガビット インターフェイス：0.1 ～ 1000 Mbps
- セルラー インターフェイス：0.1 ～ 300 Mbps

帯域幅の設定を更新するには、次の手順を実行します。

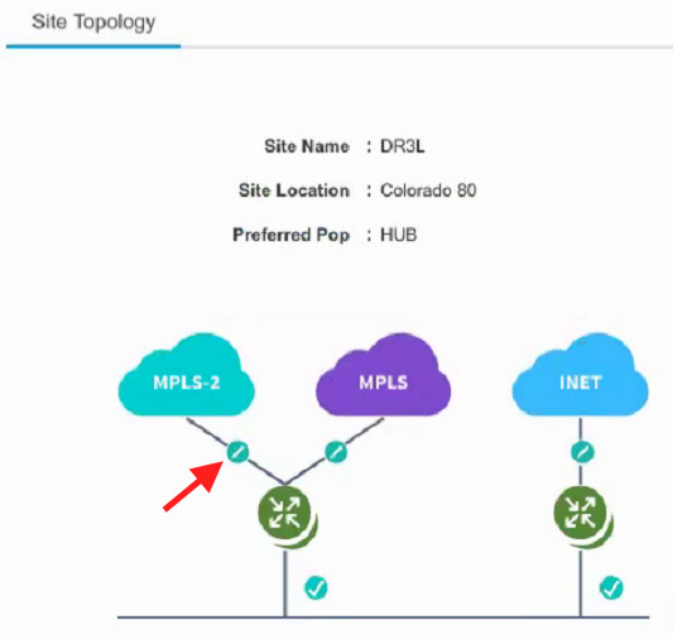
手順

ステップ 1　IWAN アプリのホームページで、[Set up Branch Sites]をクリックします。

ステップ 2　[Sites]タブをクリックします。

ステップ 3　スポーク（ブランチ）サイトの鉛筆アイコン（[Edit Site]）をクリックします。[Update Site] ダイアログボックスが開きます。

ステップ 4　[Site Topology] 領域で、WAN リンク上の鉛筆アイコンをクリックします。[Configure WAN Cloud] パラメータがダイアログボックスに表示されます。



ステップ 5　[Upload] または [Download] フィールドに新しい帯域幅値を入力します。

ステップ 6　[Update]ボタンをクリックします。

プロビジョニング済みブランチ サイトの WAN IP パラメータの更新

スポーク サイトがプロビジョニングされた後（「N 日目」）でも、スポーク サイトの WAN IP、マスク、ネクスト ホップの設定を変更できます。

IP の設定を変更するには、次の手順を実行します。

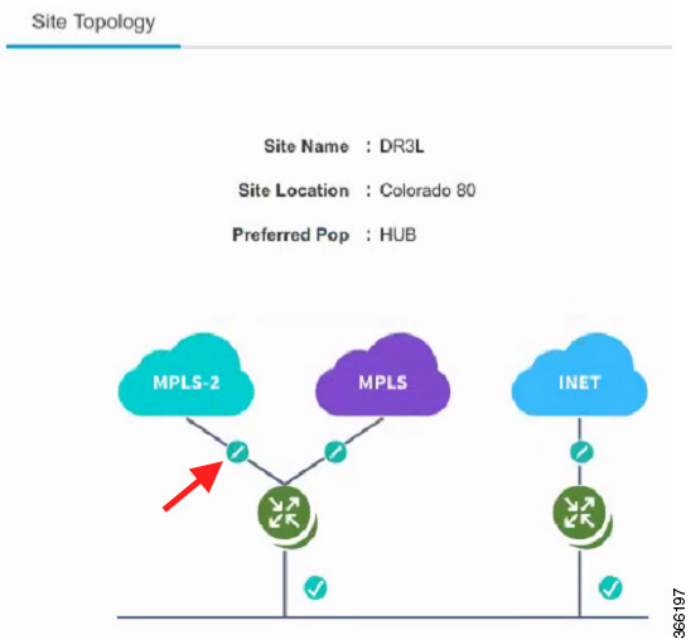
手順

ステップ 1　IWAN アプリのホームページで、[Set up Branch Sites]をクリックします。

ステップ 2　[Sites]タブをクリックします。

ステップ 3　スポーク（ブランチ）サイトの鉛筆アイコン（[Edit Site]）をクリックします。[Update Site] ダイアログボックスが開きます。

ステップ 4　[Site Topology] 領域で、WAN リンク上の鉛筆アイコンをクリックします。



ダイアログボックスにリンクの設定が表示されます。使用できるオプションは、WAN リンクのタイプに応じて異なります。

ステップ 5　次のフィールドで IP アドレスを編集します。

- [CE IP Address]:「カスタマー エッジ」の IP アドレス。これは、ブランチ WAN リンクの WAN IP アドレスです。
- [CE IP Mask]:「カスタマー エッジ」の IP マスク。
- [PE IP Address]:「プロバイダー エッジ」の IP。これは、WAN リンクのネクスト ホップのゲートウェイです。

ステップ 6　[Update]ボタンをクリックします。

（注）　変更を破棄するには、[Reset]ボタンをクリックします。

到達できない CE または PE の IP アドレス値を入力した場合、その入力操作は成功しますが、APIC-EM コントローラとサイト間の接続は失われます。これが発生した場合は、接続を復元してください。接続を復元する方法は、個々のネットワークに応じて異なります。有効な解決策は次のとおりです。

- 新しい IP アドレスによって指定したサイトがアクティブでない場合は、サイトをアクティブにして接続を有効にします。
- 新しい IP アドレスを誤って指定した場合は、以前の IP アドレスを復元します。これを行うには、(IWAN アプリを介さずに)IP アドレスの値をデバイスに直接設定する必要があります。完了したら、この項の「プロビジョニング済みブランチ サイトの WAN IP パラメータの更新」の手順を実行し、新しい有効な IP を使用して IWAN アプリを更新します。

ブランチ サイトの QoS 帯域幅の割合の変更

ブランチ サイトがプロビジョニングされた後(N 日目)、そのブランチ サイトの QoS 帯域幅の割合を変更できます。

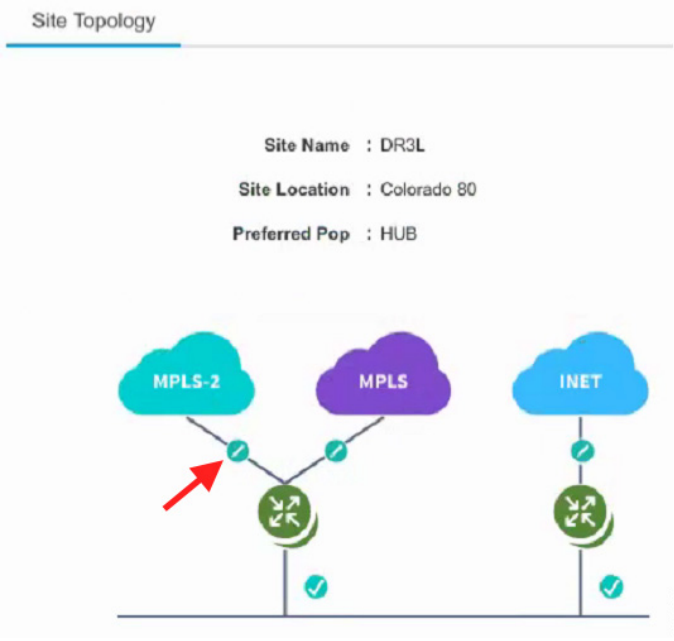
手順

ステップ 1　IWAN アプリのホームページで、[Set up Branch Sites]をクリックします。[Sites] ページが開きます。

ステップ 2　[Sites]タブをクリックします。

ステップ 3　ブランチ サイトの鉛筆アイコン([Edit Site])をクリックします。[Update Site] ダイアログボックスが開きます。

ステップ 4　[Site Topology] 領域で、WAN リンク(ルータとクラウド間のリンク)上の鉛筆アイコンをクリックします。



ステップ 5　[Service Provider] フィールドの横にある[Edit](鉛筆)アイコンをクリックします。[<サービス プロファイル名>]ダイアログボックスが開きます。

ステップ 6　必要に応じて QoS 帯域幅の割合を変更します。

ステップ 7　[Update]をクリックします。変更した帯域幅の割合が WAN リンクに適用されます。

CHAPTER 6

デバイスの管理

この章の内容は、次のとおりです。

概要

各ハブ サイトやブランチ サイトには 1 つ以上のデバイスを関連付けることができます。IWAN アプリは、ネットワーク内のデバイスに対するバッチ CLI コマンドの実行を有効化するカスタム設定機能など、デバイスを個別に管理する手段を提供します。

デバイスのカスタム設定

カスタム設定は、IWAN ネットワーク内のデバイスに対して CLI 設定コマンドを実行するためのメカニズムです。この機能はコマンドをバッチ ファイルで実行する場合と同じように機能しますが、IWAN アプリからリモートで動作します。一連のコマンドを入力し（後で使用するために任意に保存）、設定コマンドを実行するデバイスを選択します。IWAN アプリは指定されたデバイスにコマンドを送信し、コマンドの実行が成功したか否かを示します。実行に失敗した場合、この機能はロールバック メカニズムを備えているので、失敗した設定操作を無効にする一連のコマンドを実行できます。

（注） 本リリースでは、カスタム設定は「ベータ」機能として提供されます。

カスタム設定の有効化

カスタム設定機能による CLI 設定コマンドの実行を有効にするには、次の手順を実行します。

手順

ステップ 1 サイト リスト ページで、テーブルの上部にある歯車アイコンをクリックして [Custom Config Status]を選択し、[Custom Config Status] 列を表示します。列が表示され、テーブルの上部に [Custom Config]ボタンが表示されます。

カスタム設定の作成と実行

[Custom Configuration] ウィンドウを開いて、カスタム設定の CLI バッチ ファイルを作成したり、既存のカスタム設定（テンプレート）を実行したりするには、次の手順を実行します。

手順

ステップ 1　サイト リスト ページで、テーブルの上部にある [Custom Config]ボタンをクリックします。ボタンが表示されない場合は、カスタム設定の有効化（6-1 ページ）を参照してください。[Custom Config] ページが表示されます。

ステップ 2　既存のカスタム設定を選択するか、プラス記号アイコン（  ）をクリックして新しいカスタム設定を作成します。

ステップ 3　[Actual] ペインで、バッチ CLI コマンド ファイルの場合と同様に、実行する CLI コマンドを入力します。コマンドは、デバイスに対してコンフィギュレーション モードで実行されます。

（注）　IWAN アプリは入力されたコマンドを検証しません。

ステップ 4　（任意）選択したすべてのデバイスに対してコマンドのフル セットを実行します。設定コマンドを実行する各デバイス固有のパラメータを個々に入力するには、CLI コマンドで「パラメータ」値を使用します（パラメータ名の前にドル記号（$）を付けます）。
例：$interface

カスタム設定を実行すると、選択したターゲット デバイスごとにこの「パラメータ」の値を 1 つずつ入力することを要求されます。最大 10 個のパラメータを使用できます。

ステップ 5　[Rollback] ペインで、[Actual] ペインの設定コマンドの 1 つ以上が正常に実行されなかった場合に実行するコマンドを入力します。カスタム設定コマンドの実行に失敗した場合の対処方法については、カスタム設定の実行に失敗した場合の対処方法（6-3 ページ）を参照してください。

ステップ 6　[Devices] ペインで、CLI 設定コマンドを実行するデバイスを選択します。

ステップ 7　[Save]をクリックして、設定を実行せずに保存します。[Deploy]をクリックして、指定したデバイスに対して設定を実行します。サイト リスト ページが自動的に開き、設定コマンドの実行ステータス（[Success]または [Failure]）を表示できるようになります。

カスタム設定の実行ステータスの表示

サイト リスト ページの [Custom Config Status] 列には、設定コマンドの実行ステータス（[Success] または [Failure]）がサイトごとに表示されます。

サイト内のいずれかのデバイスで実行に失敗した場合は、そのサイトの [Custom Config Status] 列に [Failure]と表示されます。エラーが発生した場合は、[Custom Config Status] 列の [Failure]リンクをクリックすると、サイト内の各デバイスのステータスが表示されます。カスタム設定の実行に失敗した場合の対処方法については、カスタム設定の実行に失敗した場合の対処方法（6-3 ページ）を参照してください。

カスタム設定の実行に失敗した場合の対処方法

CLI カスタム設定コマンドの実行に失敗した場合は、次の手順を実行して対処します。

手順

ステップ 1　サイト リスト ページの [Custom Config Status] 列には、設定コマンドの実行ステータス（[Success] または[Failure]）がサイトごとに表示されます。サイト内のいずれかのデバイスで実行に失敗した場合は、そのサイトの [Custom Config Status] 列に [Failure]と表示されます。エラーが発生した場合は、[Custom Config Status] 列の [Failure]リンクをクリックすると、[Site Details] ポップアップが開きます。

ステップ 2　[Site Details] ポップアップには、サイト内の各デバイスのステータスが表示されます。スタータスが [Failure]の各サイトに対して、デフォルトで [Rollback] オプションが表示されます。次のいずれかを実行して、各デバイスのエラー状態を解決します。

- ロールバック コマンドを実行するには、[Deploy]をクリックします。
- ロールバック コマンドを変更するには、ウィンドウに表示されるロールバック コマンドを編集し、[Deploy]をクリックします。この操作はカスタム設定の保存されているバージョンには影響しません。
- カスタム設定コマンドを変更して再度実行するには、[Actual]をクリックして実行に失敗したコマンドを表示し、そのコマンドを編集してから、[Deploy]をクリックして編集済みコマンドを実行します。この操作はカスタム設定の保存されているバージョンには影響しません。
- 以降のコマンドの実行をスキップして、デバイスの [Failure]ステータスを解除するには、[Ignore/Reset] をクリックします。

カスタム設定に関する制限事項

カスタム設定機能には以下の制限があります。

- IWAN でプロビジョニングされたデバイスのみがサポートされます。
- 保存するカスタム設定テンプレート名の最大文字数：20
- 1 つのカスタム設定テンプレートに保存するコマンド（「Actual」コマンドと「Rollback」コマンド）は、10000 文字以内でなければなりません。
- デバイスごとに指定できる「パラメータ」（構文：**$<parameter-name>**）の最大数：10
- カスタム設定を同時に実行できるデバイスの最大数：20
- デバイスに新しい設定コマンドをプッシュしても、新しい設定はデータベースと自動的に同期されません。その結果、IWAN アプリによってプッシュされた設定と競合する設定は、アプリから N 日目の操作が実行されると上書きされます。

CHAPTER 7

アプリケーション ポリシーの管理

この章の内容は、次のとおりです。

[Categorize Applications] タブについて

Cisco IWAN アプリケーション（IWAN アプリ）は、IWAN ネットワーク内のルータで実行される NBAR2 プロトコル パックで動作します。NBAR2 は、ユーザ定義のカスタム プロトコルに加えてプロトコル パック内の個々のプロトコルを使用し、ネットワーク アプリケーションのトラフィックを分類します。（NBAR2 が特定のネットワーク アプリケーションを分類する方法は、各プロトコルによって定義されます）。IWAN アプリは、NBAR2 プロトコル パックで定義されたアプリケーションをカテゴリ別にグループ化して表示します。

IWAN アプリ リリース 1.4.0 は、NBAR2 Protocol Pack 27.0.0 で動作します。詳細については、プロトコル パックのマニュアルを参照してください。

カスタム アプリケーションを表示、編集、移動、追加するには、[Categorize Applications]タブを使用します。

表 7-1　[Categorize Applications] タブ

いいえ。	タスク	参照先
1	インストールされているすべてのアプリケーションをアルファベット順のリスト形式で表示するか、またはカテゴリ別に表示する。 アプリケーションのサマリーを表示する。 特定のアプリケーションを検索する。	アプリケーションの表示（7-2 ページ）
2	アプリケーションを別のカテゴリに移動する。	別のカテゴリへのアプリケーションの移動（7-2 ページ）
3	アプリケーションの情報を編集する。	アプリケーション情報の編集（7-3 ページ）
4	既存のカテゴリに新しいカスタム アプリケーションを追加する。	新しいアプリケーションの追加（7-3 ページ）
	Cisco IWAN カスタム アプリケーションを削除する。	NBAR2 カスタム アプリケーションの削除（7-4 ページ）

（注）　[Categorize Applications] ページで実行可能な操作についてクイック チュートリアルを参照するには、説明テキストの [Teach Me]をクリックします。

アプリケーションの表示

アプリケーションをリストやカテゴリで表示するか、またはインストールされているすべてのアプリケーションの概要を表示するには、次の手順を実行します。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Administer Application Policy]をクリックします。[Application Policy] ページが開きます。

ステップ 2　[Categorize Applications]タブをクリックします。インストールされているすべてのアプリケーションがアルファベット順のリストに表示されます。

ステップ 3　アプリケーションをカテゴリ別に表示するには、[ByApplication Category/By Applications] ドロップダウン リストをクリックし、[View By Application Category] を選択します。

すべてのカテゴリがデフォルトで表示されるわけではありません。すべてのカテゴリを表示するには、説明テキストの [Show]リンクをクリックします。

ステップ 4　特定のカテゴリに属するアプリケーションをすべて表示するには、カテゴリの下向き矢印をクリックします。

ステップ 5　アプリケーションの合計数、一般的なアプリケーション、およびカスタム アプリケーションについて概要を確認するには、[Applications Summary] 領域を参照します。

ステップ 6　特定のアプリケーションを検索するには、パラメータとしてアプリケーションの短縮名、長い説明、ポート、またはトラフィック クラスを [Search]フィールドに入力します。

別のカテゴリへのアプリケーションの移動

帯域幅を共有するために、別のカテゴリにアプリケーションを移動できます。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Administer Application Policy]をクリックします。[Application Policy] ページが開きます。

ステップ 2　[Categorize Applications]タブをクリックします。インストールされているすべてのアプリケーションがアルファベット順のリストに表示されます。

ステップ 3　特定のカテゴリに属するアプリケーションをすべて表示するには、カテゴリのそばにある下向き矢印をクリックします。

ステップ 4　別のカテゴリにアプリケーションを移動するには、アプリケーションを適切なカテゴリにドラッグアンドドロップして、[Apply Changes]をクリックします。

アプリケーション情報の編集

アプリケーション情報を編集するには、次の手順を実行します。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Administer Application Policy]をクリックします。[Application Policy] ページが開きます。

ステップ 2　[Categorize Applications]タブをクリックします。インストールされているすべてのアプリケーションがアルファベット順のリストに表示されます。

ステップ 3　特定のカテゴリに属するアプリケーションをすべて表示するには、カテゴリの下向き矢印をクリックします。

ステップ 4　アプリケーション情報を編集するには、アプリケーションの横にある鉛筆アイコンをクリックします。アプリケーションに関する情報が表示されます。

ステップ 5　[Edit]をクリックします。[Edit Application] ダイアログボックスが開きます。

ステップ 6　変更を加えて、[Save]をクリックします。

新しいアプリケーションの追加

新しいカスタム アプリケーションを追加するには、次の手順を実行します。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Administer Application Policy]をクリックします。[Application Policy] ページが開きます。

ステップ 2　[Categorize Applications]タブをクリックします。インストールされているすべてのアプリケーションがアルファベット順のリストに表示されます。

ステップ 3　新しいカスタム アプリケーションを追加するには、[Add Application]タブをクリックします。[Add Application] ダイアログボックスが開きます。

ステップ 4　次のプロパティを入力して、[Add]をクリックします。

フィールド	説明
名前	アプリケーションの名前。
[Type] オプション ボタン	次のいずれかを選択します。 • [URL]: このオプションボタンをクリックして、[URL] フィールドにアプリケーションの URL を入力します。 • [Server IP/Port]: このオプションボタンをクリックして、使用するアプリケーションの IP アドレス、ポート、およびプロトコルを入力します。 • [DSCP]: DiffServ コード ポイント（DSCP）。このオプション ボタンをクリックして、ドロップダウン リストから値を選択します。
Similar to	使用可能な類似のアプリケーションを一覧表示してアプリケーションを選択するには、このフィールドをクリックします。

カテゴリ	ドロップダウン リストから新しいアプリケーションが属するカテゴリを選択します。
ジッタ	(任意)別の値を指定するか、デフォルト値のままにします。
Packet loss	(任意)別の値を指定するか、デフォルト値のままにします。
遅延	(任意)別の値を指定するか、デフォルト値のままにします。

NBAR2 カスタム アプリケーションの削除

NBAR2 カスタム アプリケーションを削除するには、次の手順を実行します。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Administer Application Policy]をクリックします。[Application Policy] ページが開きます。

ステップ 2　[Categorize Applications]タブをクリックします。

ステップ 3　カスタム アプリケーションを削除するには、次の手順を実行します。

a. 左側のウィンドウで、[View By]フィルタを [Application Category] から [Applications] に変更します。

b. アプリケーションの横にある [Edit]アイコンをクリックします。[Edit Application] ダイアログボックスが開きます。

c. [Edit Application] ダイアログボックスの [Delete]ボタンをクリックします。

(注)　[Delete] ボタンはカスタム アプリケーションでのみ使用できます(EasyQoS カスタム アプリやデフォルトの Protocol Pack アプリケーションでは使用できません)。

d. 確認ボックスで [OK]をクリックします。ユーザ インターフェイスからアプリケーションが削除されます。(削除は、以降のステップで [Apply Changes]ボタンをクリックすると完了します)。

(注)　考えが変わってアプリケーションを削除する必要がなくなった場合は、ページを更新してください。アプリケーションがすべての設定とともに復元されます。

ステップ 4　アプリケーションの削除を完了させるには、[ApplyChanges](右上隅)をクリックします。

(注)　[Apply Changes]をクリックした後は、アプリケーションを復元できません。

ステップ 5　複数のアプリケーションを同時に削除するには、ユーザ インターフェイスからそれらを削除して [Apply Changes]をクリックします。[Application Policy Summary] ページが開き、削除するすべてのアプリケーションが一覧表示されます。

ステップ 6　サマリーの情報を確認し、次のいずれかを実行します。

- [Apply Now]オプション ボタンをクリックして、[Continue] をクリックします。
- [Schedule]オプション ボタンをクリックして、アプリケーションを削除する日時を指定し、[Continue] をクリックします。

[Define Application Policies] タブについて

ビジネスとの関連性に従ってポリシーを定義するには、[Define Application Policy]タブを使用します。アプリケーション ポリシーは次の 3 つのビジネス グループに分類されます。

- [Business Relevant]: 電子メール、音声およびビデオ、ファイル共有、バックアップとストレージなど、ビジネスにとって重要なアプリケーション。
- [Default]: 電子支払いなどのアプリケーション。
- [Business Irrelevant]: ソーシャル メディアやゲーム アプリケーションなど、ビジネスとは関係ないアプリケーション。

[Define Application Policy]タブを使用して、以下を実行します。

表 7-2　[Define Applications] タブ

いいえ。	タスク	参照先
1	別のビジネス グループにアプリケーションのカテゴリを移動する。	[Application Bandwidth] タブについて (7-7 ページ)。
2	アプリケーションのパフォーマンスを変更する。	アプリケーションのパフォーマンスの変更 (7-6 ページ)

別のビジネス グループへのアプリケーション カテゴリの移動

別のビジネス グループにアプリケーションのカテゴリを移動するには、次の手順を実行します。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Administer Application Policy]をクリックします。[Application Policy] ページが開きます。

ステップ 2　[Define Application Policy]タブをクリックします。アプリケーションが 3 つのカテゴリ ([Business Relevant]、[Default]、[Business Irrelevant]) に表示されます。

ステップ 3　別のビジネス グループにアプリケーションを移動するには、ドラッグアンドドロップ機能を使用します。たとえば、[Default] グループから電子支払いアプリケーションをドラッグして、[Business Irrelevant] グループにドロップすることができます。

アプリケーションのパフォーマンスの変更

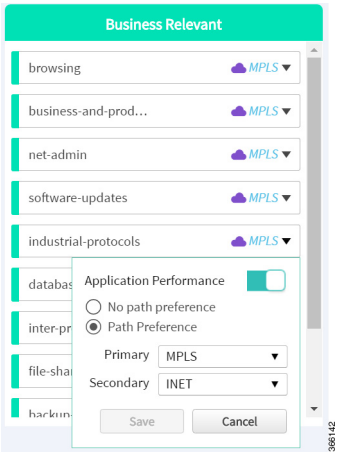
アプリケーションのパフォーマンス パラメータを変更するには、次の手順を実行します。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Administer Application Policy]をクリックします。[Application Policy] ページが開きます。

ステップ 2　[Define Application Policy]タブをクリックします。すべてのアプリケーションが 3 つのカテゴリ（[Business Relevant]、[Default]、[Business Irrelevant]）に表示されます。

ステップ 3　アプリケーションのパフォーマンスを変更するには、アプリケーションの横にある下向き矢印をクリックします。[Application Performance] ダイアログボックスが開きます（次の図を参照）。



ステップ 4　次の手順を実行します。

a.　[Application Performance]ボタンをクリックして有効または無効にする。

b.　該当するパス プリファレンス オプション ボタンを選択する。

c.　ドロップダウン リストからプライマリ パスとセカンダリ パスを選択する。セカンダリ パスは省略できます。

ステップ 5　パス プリファレンスを選択し、このカテゴリのトラフィックの優先パスを [Path 1] に設定します。例：Int（インターネット）

ステップ 6　パス プリファレンスを更新したら、[Save]をクリックします。

（注）　[Save]オプションを選択した場合、スケジュール済みのワークフローとの競合については検証されません。変更に基づいてスケジュール済みのジョブを再評価し、必要に応じてジョブを更新してください。スケジュール済みジョブがアクティブなときに競合が発生すると、その時点でジョブが失敗する可能性があります。

[Application Bandwidth] タブについて

さまざまなアプリケーションで使用される帯域幅を表示するには、[Application Bandwidth] タブを使用します。この情報に基づいて、別のカテゴリへのアプリケーションの移動を選択できます。別のカテゴリへのアプリケーションの移動（7-2 ページ）を参照してください。

アプリケーション帯域幅の表示

さまざまなアプリケーションで使用される帯域幅をグラフ表示するには、次の手順を実行します。

はじめる前に

次の作業が完了していることを確認する必要があります。

- Prime アプリケーションに Cisco APIC-EM コントローラの IP アドレスを追加する。
- Cisco APIC-EM に Prime クレデンシャルを追加する。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Administer Application Policy]をクリックします。[Application Policy] ページが開きます。

ステップ 2　[Application Bandwidth]タブをクリックします。各ハブのアプリケーション カテゴリごとに帯域幅の使用量がグラフ形式で表示されます。また、帯域幅が最も使用された日時も表示できます。

CHAPTER 8

サイトのモニタリングとトラブルシューティング

この章は以下の項から構成されています。

Cisco IWAN ネットワーク全体の表示

Cisco IWAN ネットワーク内の世界中のサイトをすべて表示し、各サイトのステータス情報を参照するには、[Monitoring] ページを使用します。[Monitoring] ページには、各サイトの地理的な場所を示す地図とサイトを簡潔な表形式で表示する代替リスト ビューがあります。

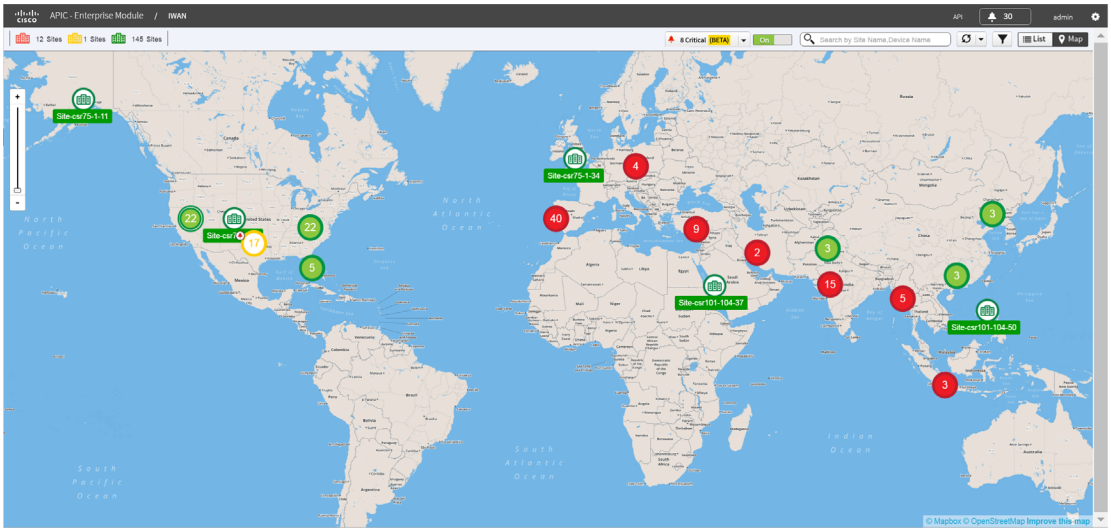
手順

ステップ 1 シスコ インテリジェント WANアプリのホームページで、[Monitor & Troubleshoot]をクリックします。[Monitoring] ページが開き、地図上にすべてのサイトが表示されます。サイト アイコンは特定の場所にある単一のサイトを示しています。特定の地域内に多数のサイトがある場合は、混雑を避けるために、ハブやブランチなどのサイトの総数を表す数字が付いた円が地図上に表示されます。

右上の [Map]ボタンと [List] ボタンによって、IWAN サイトのマップ ビューとリスト ビューを切り替えます。

[Monitoring] ページ、記号、コントロール

図 8-1　モニタリング ページ



地図の要素	説明
サイト記号	
	ハブ サイト。
	ブランチ サイト。
	同じ地域内の多数のサイト。サイトを個別に表示するには、地図を拡大します。
警告とアラーム	
	プロビジョニング済みサイト（警告もアラームもなし）。
	アウトオブバンド変更の警告が発生し、コンプライアンス機能によって報告されたサイト。 クリックして [Site Details] ページを表示し、[Policy Compliance] タブを選択すると、サイトの設定が表示されます。コンプライアンスのモニタリング（8-7 ページ）を参照してください。
	1 つ以上のアラームが発生しているサイト。サービス保証：ネットワーク接続アラーム（8-8 ページ）を参照してください。 クリックすると、アラームの詳細が表示されます。
	プロビジョニングに失敗したサイト。

	緑:ネットワーク アラームが発生していない、プロビジョニング済みのサイトの数。 黄色:ネットワーク アラームが発生しているサイトの数。アラームが発生しているサイトは、地図上に黄色で表示されます。 赤:プロビジョニングに失敗したサイトの数。
 	ネットワーク アラームを報告するコントロール(サービス保証(Service Assurance)ベータ機能)。サービス保証機能は、IWAN ネットワーク内のサイトに影響を及ぼす重大なネットワークの問題を報告します。アラームが発生しているサイトは黄色で表示されます。サービス保証:ネットワーク接続アラーム(8-8 ページ)を参照してください。 IWAN アプリは、30 分ごとにネットワーク内のサイトにアラーム情報を要求し、その情報を分析してアラーム表示を更新します。アラームが発生している場合、このコントロールにはネットワーク内のアラームの総数が表示されます。 オプション • アラームが発生している場合は、[Assurance]コントロールをクリックすると、[Alarms] ページにシステム内のすべてのアラームが一覧表示されます。 • 下向き矢印をクリックすると、[Refresh]ボタンが付いた小さいドロップダウン ウィンドウが開きます。スケジュールされている次回の自動更新を待たずに、今すぐネットワーク内の各サイトのアラーム情報を要求するには、[Refresh]をクリックします。IWAN アプリがアラーム情報を分析している間、ドロップダウン ウィンドウには進捗の割合が表示されます。完了すると、表示が更新されます。 • 地図上のサイト アイコンにカーソルを移動すると、サイトに影響を与えているアラームの情報が表示されます。[View Details]をクリックすると、[Site Details] ページにアラームの詳細が表示されます。 • 地図上のサイト アイコンをクリックすると、[Site Details] ページにアラームの詳細が表示されます。
追加機能	
	サイト名またはデバイス名によって特定のサイトを検索します。
	プロビジョニング ステータスなどのサイト情報を更新します。更新してもアラームの表示は影響を受けません。
	選択した条件に従って、サイトの表示をフィルタリングします。
	[Map] ビューと [Site List] ビューを切り替えます。

サイトの詳細の表示

Cisco IWAN ネットワーク内の各サイトには [Site Details] ページがあります。このページに表示される情報は、サイトのステータス、アプリケーション トラフィックの状態、サイトに対するアラームの有無に応じて異なります。

手順

ステップ 1　サイトをクリックします。[Site Details] が開き、次の情報が表示されます。

地図の要素	説明
Site Status	サイトがプロビジョニングされているかどうかを示します。
[Hub/Site Topology] タブ	サイト名、場所、優先 POP などを含む、サイト トポロジのグラフィック表示。 詳細情報を表示するには、トポロジの要素の上にカーソルを移動します。
IP Address Allocation	サイトのデバイスのリストおよびデバイスが割り当てられている IP アドレス。
[Application Health] タブ	アプリケーション トラフィックに関する情報が表示されます。アプリケーション トラフィックのパフォーマンスが良好な場合は、次の情報が表示されます。 • アプリケーション トラフィック情報 • 各アプリケーションの帯域幅使用量 • 各アプリケーションの統計的なトレンド サイトのアプリケーション トラフィックでアプリケーションに影響を及ぼす問題（パケット損失、超過遅延、過度のジッターなど）が発生した場合は、このタブに詳細が表示されます。8-5ページの図 8-2を参照してください。
[Alarms] タブ	（アラームが発生している場合に表示） アラームは、特定のアプリケーションや帯域幅割り当ての問題によって発生する可能性があります。アラームの問題を解決するための推奨アクションがシステムによって示されます。サービス保証：ネットワーク接続アラーム（8-8 ページ）を参照してください。
[Policy Compliance] タブ	（アウトオブバンド設定が検出された場合に表示） コンプライアンス レポート：アウトオブバンド設定変更（8-6 ページ）を参照してください。
[Troubleshoot] タブ	クリティカル アラームを引き起こしているアプリケーションを指摘して、サイトのパフォーマンスを向上させる推奨アクションを示します。たとえば、アプリケーションが割り当てよりも多くの帯域幅を必要とする場合は、帯域幅の設定を調整できます。8-5ページの図 8-3および8-6ページの図 8-4 を参照してください。

図 8-2　[Application Health] タブ

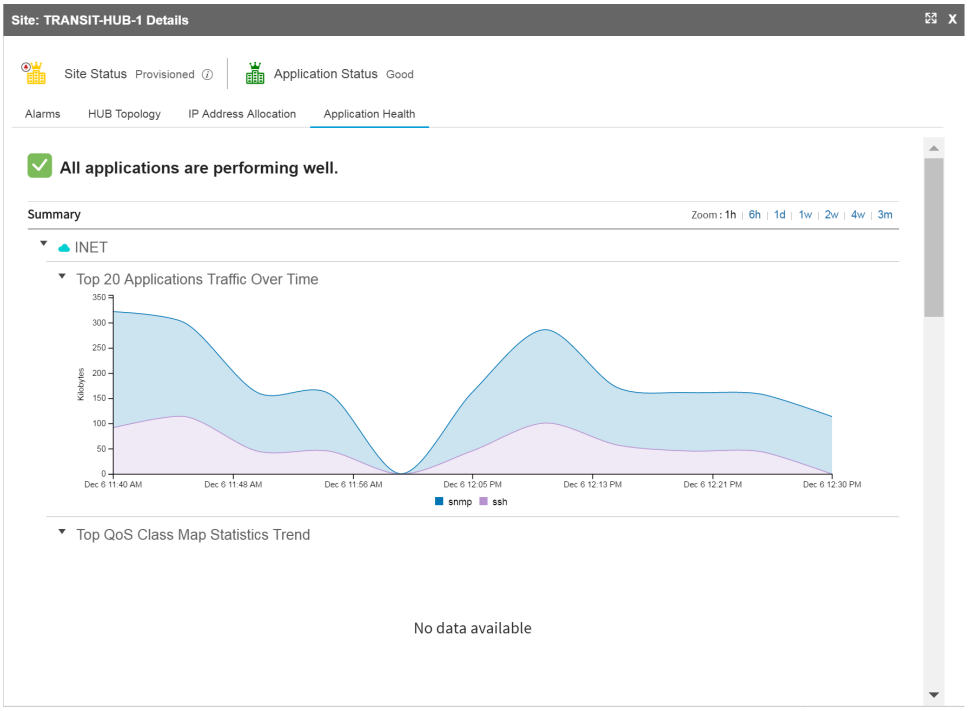


図 8-3　トラブルシューティング:検出

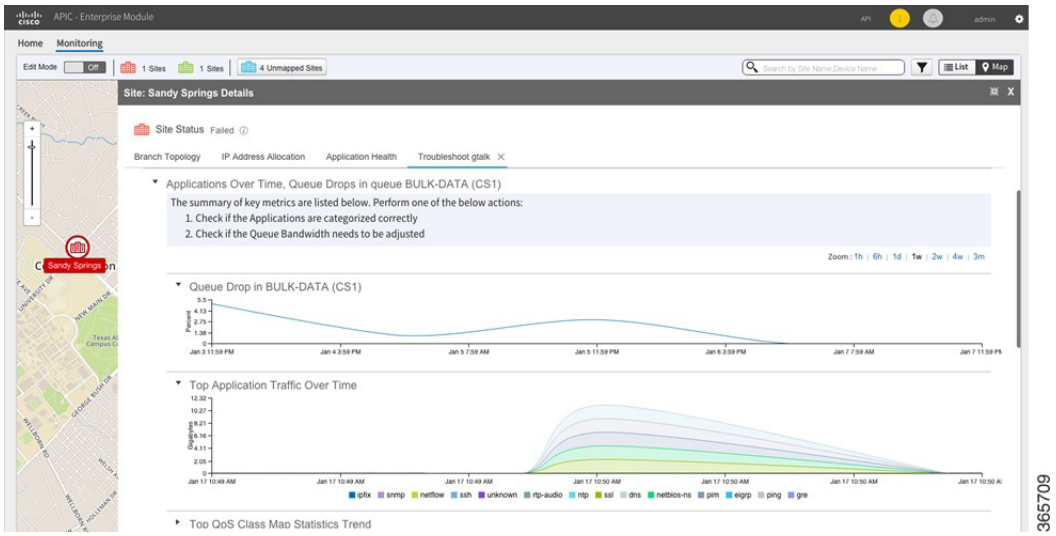
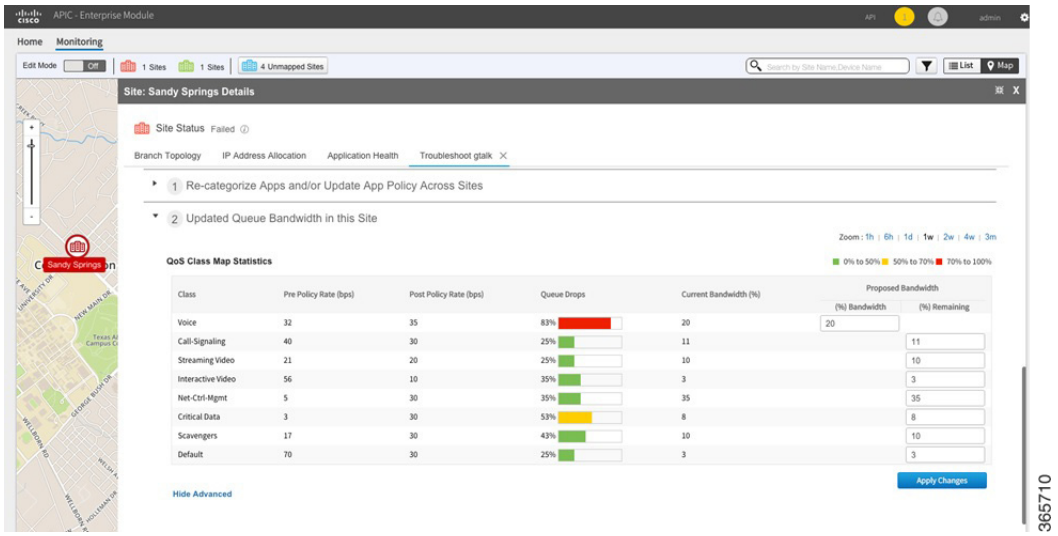


図 8-4　トラブルシューティング:帯域幅の調整



コンプライアンス レポート:アウトオブバンド設定変更

Cisco IWAN ネットワーク内のサイトの場合、通常は、管理者が IWAN アプリを使用して一元的に設定変更を行います。IWAN アプリを使用せずに、ネットワーク内のデバイスに対して直接行われたローカルな設定変更は、アウトオブバンド設定変更と呼ばれます。ローカルに設定変更されたサイトは非準拠と呼ばれます。

IWAN アプリでは、コンプライアンスについてネットワーク内のサイトをチェックできます。コンプライアンス レポート機能は、各サイトの設定情報を収集します。この機能は、アウトオブバンド設定変更が行われたサイトを検出すると、IWAN アプリの [Monitoring] ページでそのサイトに非準拠フラグを付けます。[Map] ビューではサイトに黄色いバッジが表示され、[Sites List] ビューでは警告を表す黄色い記号が表示されます。

非準拠サイトの [Site Details] ページには、ローカルに加えられた変更の詳細が表示されます。

コンプライアンス レポート機能

Cisco Prime Infrastructure は Cisco IWAN ネットワーク内のルータで動作し、ルータの設定に関する情報を収集します。Prime Infrastructure はこの設定情報を IWAN アプリに提供し、IWAN アプリはそれによってネットワーク内の各ルータのコンプライアンス ステータスを判断します。

IWAN アプリは、以下の場合にルータに非準拠フラグを付けます。

- IWAN アプリを介さずにルータでローカルに行われた設定変更を検出した場合。

  および

- 設定の不一致が 5 分の猶予期間を超えている場合。

コンプライアンス レポートの設定

Cisco IWAN アプリのコンプライアンス レポート機能を有効にして、アウトオブバンド設定変更が行われたサイトを報告させるには、次の手順を実行します。

ステップ 1　IWAN アプリのホームページで、[Configure Hub Site & Settings]をクリックします。[Network wide settings] ページが開きます。

ステップ 2　[System]タブをクリックします。

ステップ 3　[Show more]ボタンをクリックして、その他の設定を表示します。

ステップ 4　[Syslog] セクションで、[Server IP] フィールドに Cisco Prime サーバのアドレスを入力します。（ネットワーク管理者は Prime サーバのアドレスを入力できます）。

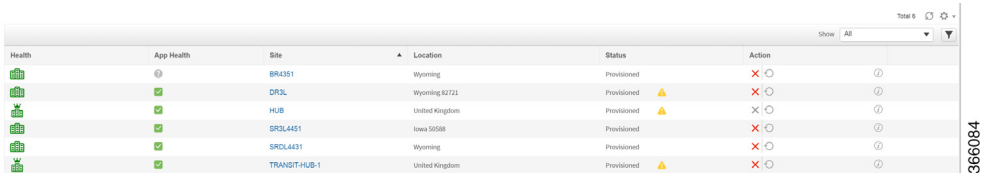
ステップ 5　[Save & Continue]ボタンをクリックして変更を保存します。コンプライアンス レポート機能が有効になります。

コンプライアンスのモニタリング

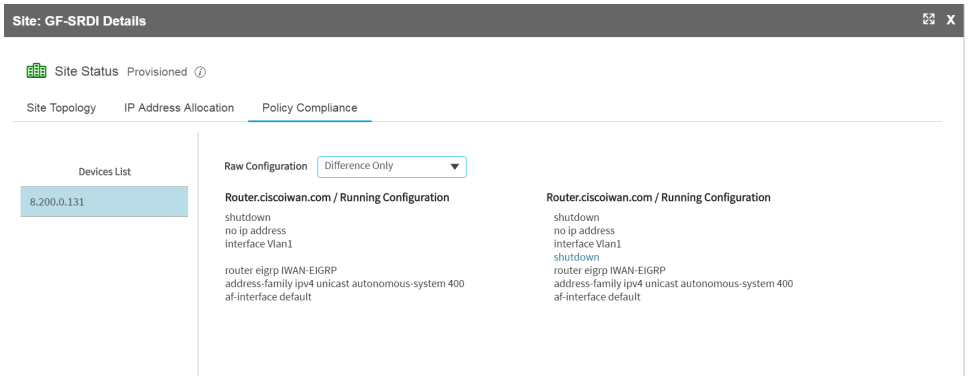
コンプライアンス レポート機能がアクティブになると、アウトオブバンド設定変更が行われたサイトが [Monitoring] ページに次のように表示されます。

- [Map] ビュー:サイト アイコン上に黄色い警告バッジ。

- [Sites List] ビュー:サイトの [Status] 列に黄色い警告アイコン。



サイトをクリックして [Site Details] ページを表示し、[Policy Compliance] タブを選択すると、サイトの設定の詳細が表示されます。[Raw Configuration] ドロップダウン メニューから、[All]を選択してサイト設定の全詳細を表示するか、[Difference Only] を選択してサイトに対するアウトオブバンド変更のみを表示します。



サービス保証:ネットワーク接続アラーム

IWAN アプリは、IWAN ネットワーク全体の接続に影響する重大なネットワーク問題について情報を提供します。この「サービス保証」は、IWAN アプリとネットワーク内のサイト間の通信に影響を及ぼす可能性がある問題について重要な情報を提供します。

IWAN ネットワーク全体のサイトが接続情報を IWAN アプリに報告します。IWAN アプリはその情報を処理し、重大なネットワーク問題を [Monitoring] ページにアラームとして示します。「Critical」というラベルが付いたボタンは、ネットワーク内のアラームの要約を表示します。

[Map] ビューと [Sites List] ビューには各サイトのアラームが表示され、各アラームの詳細情報に簡単にアクセスできます。

アラームのメカニズム

IWAN アプリは、30 分間隔で、ネットワーク内の各サイトにネットワーク機能に関する情報を要求します。その情報を分析した後、[Monitoring] ページにアラームを表示することによって、重大なネットワークの問題を示します。ネットワークの問題によって影響を受けるサイトは、赤いバッジが付いた黄色で示されます。

ネットワークで検出されたすべてのアラームの詳細を表示するには、[Monitoring] ページの上部にある [Assurance] ボタンをクリックします。特定のサイトに影響を及ぼすアラームの情報を表示するには、そのサイト アイコンの上にカーソルを移動するか、サイト アイコンをクリックします。

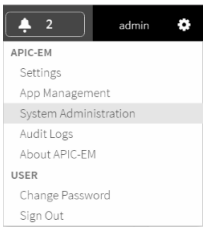
(注) ネットワーク アラームを報告するサービス保証機能は、本リリースでは「ベータ」機能です。ネットワークの問題を示す唯一のインジケータとして過信しないようにしてください。

ネットワーク アラーム レポートの設定

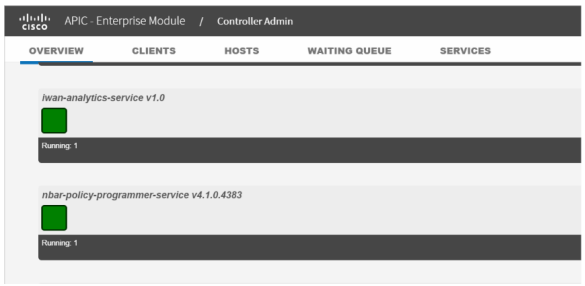
サービス保証機能を有効にする前に

IWAN アプリでサービス保証機能を有効にする前に、次の APIC-EM サービスが実行されていることを確認してください:**iwan-analytics-service**。

これを確認するには、APIC-EM で [Settings](歯車ボタン)>[System Administration] を選択し、アクティブなサービスを表示します。

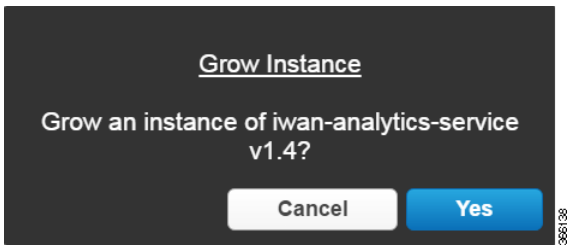


[Overview] タブで、**iwan-analytics-service** が実行されていることを確認します。

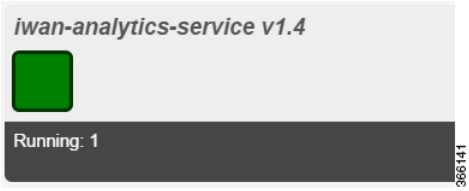


サービス リストの **iwan-analytics-service** の下に緑色の正方形が表示されていない場合、サービスは実行されていません。サービス名の下の [Running] ラベルの値は 0 になっています。

サービスをアクティブにするには、サービス名の右側にあるプラス アイコン( )をクリックします。インスタンスをアクティブにすることを求められたら、[Yes]をクリックします。



サービスが開始されるまでに数分かかることがあります。完了すると、サービス リストの **iwan-analytics-service** の名前の下に緑色の正方形が表示されます。



手順

サービス保証機能によるネットワーク アラームの報告を有効にするには、次の手順を実行します。

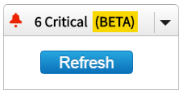
ステップ 1　IWAN アプリのホームページで、[Monitor & Troubleshoot]をクリックします。[Monitoring] ページが開きます。

ステップ 2　[Monitoring] ページで、上部付近にある [Assurance]ボタンの横の [On/Off] スイッチをクリックします。

ステップ 3　このサービス保証機能のベータ版では、ウィンドウで [Lab Environment] を選択することを求められます。[Lab Environment]をクリックします。

サービス保証機能がアクティブになります。IWAN は、ネットワーク内の全サイトのネットワーク機能について情報収集を開始し、30 分ごとに情報を更新します。

ステップ 4　(任意)[Assurance]ボタンの下向き矢印をクリックすると、[Refresh]ボタンが付いた小さいドロップダウン ウィンドウが開きます。スケジュールされている次回の自動更新を待たずに、今すぐネットワーク内の全サイトのアラーム情報を要求するには、[Refresh]をクリックします。



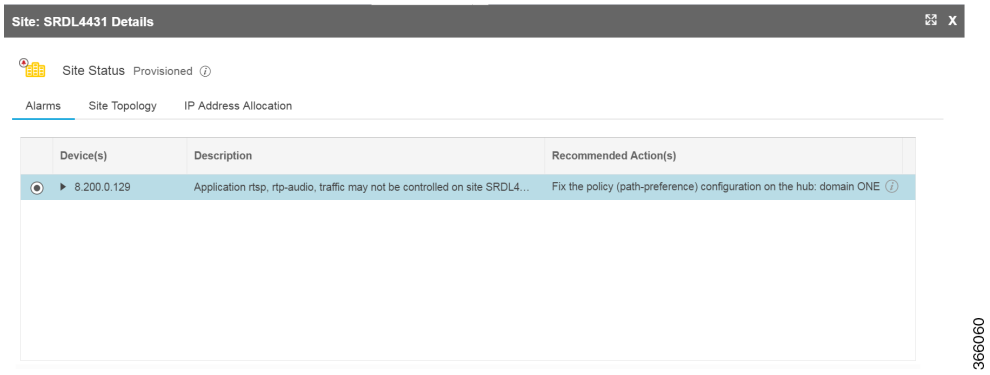
IWAN アプリがアラーム情報を分析している間、ドロップダウン ウィンドウには進捗の割合が表示されます。完了すると、表示が更新されます。

ネットワーク アラームの表示

ネットワーク アラームの詳細を表示するには、次のいずれかを実行します。

- [Map] ビュー:サイト アイコンの上にカーソルを移動すると、サイトに影響を与えているアラームの情報が表示されます。[View Details]をクリックすると、[Site Details] ページが表示されます。[Alarms] タブにアラームの詳細が表示されます。

- [Map] ビューまたは [Sites List] ビュー:地図上のサイト アイコンまたはリスト ビュー内のサイト名をクリックすると、[Site Details] ページが表示されます。[Alarms] タブにアラームの詳細が表示されます。



CHAPTER 9

バックアップと復元、リカバリ、および削除

この章の内容は、次のとおりです。

バックアップと復元

バックアップと復元に関する推奨事項

バックアップと復元を適切に機能させるために、以下を推奨しています。

- マルチホスト モードで実行する。これによりアクティブな高可用性（HA）が有効になるので、バックアップやリカバリの時間が短縮されます。
- サイトのプロビジョニングにデバイスを使用する前に、必要に応じて設定を復元できるように、実行中の設定を IWAN_RECOVERY.cfg ファイルとしてブートフラッシュに保存することを推奨します。
- サイトを削除した場合は、IWAN_RECOVERY.cfg ファイルに保存されている設定と共にルータをリロードする。
- 毎日バックアップを実行して、データベースとファイルの現在のバージョンを維持する。
- システムで変更を開始した後に、バックアップと復元を実行する。
- 前に実行した目的（インテント）を取り消すためにバックアップと復元を使用しない。アプリケーションでサポートされているワークフローを使用して、目的を遂行してください。
- シスコ インテリジェント WANに追加された（または証明書が更新された）デバイスを追跡する。
- シスコ インテリジェント WANから削除された（または証明書が取り消された）デバイスを追跡する。

バックアップと復元のシナリオ

バックアップと復元は以下の状況で*機能*します。

- IWAN アプリの機能的役割に対してコントローラが安定した状態である。
- バックアップから復元までの間に シスコ インテリジェント WANアプリケーションの機能的役割が実行されていない。
- サイトのステータスが成功または失敗になっており、サイト リカバリが進行していない。
- 同じ期間中に、アクティブになっているスケジュール済みジョブがない。

バックアップと復元は以下の状況では*機能しません*。

- シスコ インテリジェント WANが、内部データベースの操作やデバイス ポリシーの更新など、アプリケーションの機能的役割を遂行している。
- Cisco APIC-EM にはリスクがあります。復元後にコントローラとネットワークが同期しなくなり、その結果、一部またはすべてのサイトがポリシー違反状態になる場合があります([Site Status] 画面に表示)。セキュリティ関連の問題など、一部のポリシー違反の状況は検出されないことがあります。
- バックアップと復元の操作中にシスコ インテリジェント WANアプリケーションで実行されたワークフローが失われ、追跡することも回復することもできない。次の表は、ワークフロー シナリオと可能な回避策を示しています。

表 9-1　バックアップと復元に失敗したワークフロー シナリオと回避策

シナリオ	回避策

バックアップと復元の操作中に IWAN に追加されたサイト(1 つ以上のデバイス)。	1. PKI トラストポイントを削除し、各デバイスのキーをゼロに設定します。次のコマンドを使用して、各デバイスのトラストポイントと証明書をクリアします。
	`no crypto pki trustpoint sdn-network-infra-iwan`
	`crypto key zeroize rsa sdn-network-infra-iwan`
	2. プラグアンドプレイ ワークフローを再開します。これにより、デバイスは要求されていないデバイスとして Cisco IWAN アプリに表示されます。
	3. デバイスがサイトとしてすでに追加されている場合は、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーし、影響を受ける各ルータにそのルータをリロードします。PnP コール ホーム ワークフローが後を引き継ぎ、デバイスは要求されていないデバイスとしてワークフローに表示されます。
	4. サイト プロビジョニングを再適用します。
	5. 作成ワーク フローを繰り返します。

表 9-1　バックアップと復元に失敗したワークフロー シナリオと回避策(続き)

シナリオ	回避策

バックアップと復元の操作中に証明書が更新されたデバイス。	1. PKI トラストポイントを削除し、各デバイスのキーをゼロに設定します。
	2. 次のコマンドを使用して、各デバイスのトラストポイントと証明書をクリアします。
	`no crypto pki trustpoint sdn-network-infra-iwan`
	`crypto key zeroize rsa sdn-network-infra-iwan`
	3. デバイスまたは一連のデバイスに対してサイト作成ワーク フローを繰り返します。
	デバイスがシスコ インテリジェント WAN でプロビジョニングされると、身元を証明する証明書がデバイスに提供されます。この証明書の有効期間は 1 年です。証明書の有効期間の 80 パーセントが経過すると、デバイスは証明書の自動更新を試みます。
	バックアップと復元の間にデバイスが証明書の更新を試みた場合、データベースには証明書が未更新であると表示されます。
	デバイスとその証明書のステータスを追跡することは困難であるため、シスコでは、クライアント ID 証明書が失効したデバイスや間もなく期限切れになるデバイスを特定する API を提供しています。
	デバイスのクライアント ID 証明書が失効した後は、デバイスの再プロビジョニングが唯一の手段になります。

バックアップと復元の操作中にシスコ インテリジェント WANから削除されたサイト、または証明書が取り消されたサイト。	次のいずれかを実行します。 • コントローラのユーザ インターフェイスを介して各デバイスの証明書を取り消します。 • サイトがネットワークの一部の場合は、[Site Status] ページの [Actions]列で [X] アイコンをクリックし、サイトの証明書を取り消してアプリケーションをクリアします。
バックアップと復元の操作中に設定またはポリシーを更新。	シスコ インテリジェント WANアプリケーションは、コントローラと競合するデバイスでの変更を検出できます。バックアップと復元の間にサイトに更新が加えられた場合、そのサイトはポリシーから削除されます。以前に適用されたものと同じ変更セットを再適用することを推奨します。ただし、このアプローチが成功する割合は変更の性質に応じて異なります。サイトをポリシーから削除する場合は、手動による操作が必要です。手動による変更が成功しない限り、コントローラはサイトからのポリシーの削除を管理しないからです。 (注)　自動化スクリプトを使用することをお勧めします。このスクリプトは、証明書のステータス(取り消しまたは作成)とともに、デバイスの追加と削除に関する監査ログ エントリを自動的に追跡します。このスクリプトは、不安定なシステムを回復させる場合に役立ちます。監査レコードは、システムの不安定さにより失われた変更を再適用する場合にも役立ちます。システムを復元する準備として、バックアップの完了後にこの自動スクリプトを定期的に実行してください。

回復

シスコ インテリジェント WANサイトのリカバリ

サイトのプロビジョニングに失敗した場合は、次の手順でサイトをリカバリします。

ステップ 1　シスコ インテリジェント WANのホームページで、[Manage Branch Sites]をクリックします。[Sites] ページが開きます。

ステップ 2　[Site(s)]タブをクリックします。[Site Status] ページの [Action]列で、[Recovery] アイコンをクリックします。

サイトのリカバリを試みて成功した場合は、サイトのステータスが [Success] に変わります。成功しなかった場合は [Recovery]アイコンが再び表示され、サイトのリカバリを再度試みることができます。

サイトのリカバリは何度も試行できます。ただし、サイトをリカバリできない場合は、サイトを削除することが唯一の選択肢となります。

ハブ サイトおよびブランチ サイトのポストプロビジョニング リカバリ

ポストプロビジョニング リカバリ機能を使用すると、サイトのプロビジョニング後にハブとスポーク デバイスに最後の変更を再適用できます。

リカバリは何度も試行できます。ハブまたはブランチ サイトをリカバリするには、[Site Status] ページの [Action]列で [Recovery] アイコンをクリックします。

リカバリを複数回試みて失敗した場合は、削除 [X] アイコン（[Site Status] ページの [Action] 列）をクリックすることにより、サイトを完全に削除することもできます。

削除

ハブ サイトの削除

プライマリ ハブが障害状態にあり、どのブランチ サイトもプロビジョニングされていない場合は、プライマリ ハブを削除できます。

プライマリ ハブと中継ハブの両方が障害状態の場合に、プライマリ ハブを削除するには、最初に中継ハブを削除する必要があります。削除操作が成功すると、プライマリ ハブと中継ハブの両方がブラウンフィールド検証状態にリセットされます。

ハブのプロビジョニングに失敗した後にハブを削除した場合は、シスコ インテリジェント WAN アプリケーションにより以下が実行されます。

- PKI 証明書とトラストポイントが取り消される。
- IP アドレスが IP アドレス プールにリリースされる。
- インベントリからハブが削除される。

削除操作が成功すると、ハブは [Sites]ページから削除されます。

(注)　ハブ サイトはベスト エフォート方式で削除されます。デバイスに到達できない場合、デバイスは元の設定に復元されません。その場合は、デバイスの設定を手動でクリーンアップする必要があります。手動によるデバイスのクリーンアップ（9-6 ページ）を参照してください。

ハブのプロビジョニングの一環として、[Configure Hub Site] ページからハブを再プロビジョニングできます（ウィザードの手順 5：IWAN 集約サイトの設定（4-12 ページ）を参照）。

中継ハブの削除

中継ハブの状態（プロビジョニング済みまたは失敗）に関係なく、中継ハブを削除できます。

中継ハブを削除すると、IWAN により以下が実行されます。

- 中継ハブのすべてのデバイスの PKI 証明書とトラストポイントが取り消される。
- IP アドレスが IP アドレス プールにリリースされる。
- インベントリから中継ハブが削除される。
- Network and Wireless Services（NWS）状態が解消される

削除操作が成功すると、中継ハブは [Sites]ページから削除されます。

(注)　中継ハブ サイトはベスト エフォート方式で削除されます。デバイスに到達できない場合、デバイスは元の設定に復元されません。その場合は、デバイスの設定を手動でクリーンアップする必要があります。手動によるデバイスのクリーンアップ（9-6 ページ）を参照してください。

ブランチ サイトの削除

ブランチの状態（進行中、プロビジョニング済み、または失敗）に関係なく、ブランチ サイトを削除できます。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Manage Branch Sites]をクリックします。[Sites] ページが開きます。

ステップ 2　[Site(s)]タブをクリックします。[Site Status]ページの [Action] 列で、[X] アイコンをクリックしてサイトを削除します。

(注)　ブランチ サイトはベスト エフォート方式で削除されます。デバイスに到達できない場合、デバイスはブートストラップ コンフィギュレーションに復元されません。その場合は、デバイスの設定を手動でクリーンアップする必要があります。手動によるデバイスのクリーンアップ（9-6 ページ）を参照してください。

ブランチ サイトを削除すると、シスコ インテリジェント WANアプリケーションにより以下が実行されます。

- PKI 証明書とトラストポイントが取り消される。
- IP アドレスが IP アドレス プールからリリースされる。
- データベースからサイト情報が消去される。
- 削除したサイトのルータをブートストラップ コンフィギュレーション ファイル（IWAN_RECOVERY.cfg）に戻すには、以下を実行します。
  - IWAN_RECOVERY.cfg をスタートアップ コンフィギュレーションにコピーします。
  - デバイスがリロードされます。

バックアップと復元（9-1 ページ）を参照してください。

サイトを削除すると、ブランチ デバイスが [Devices]タブから削除され、要求されていないデバイスのリストに表示されるので、ブランチ サイトを再プロビジョニングできます。

手動によるデバイスのクリーンアップ

ハブ サイト、中継ハブ サイト、またはブランチ サイトを削除すると、そのサイトのデバイスがベスト エフォート方式で削除されます。デバイスに到達できない場合、デバイスは元の設定に復元されません。その場合は、デバイスの設定を手動でクリーンアップする必要があります。

デバイスの設定を手動でクリーンアップするには、次の手順を実行します。

手順

ステップ 1　IWAN PKI トラストポイントを削除します。次のコマンドを使用します。

no crypto pki trustpoint sdn-network-infra-iwan

ステップ 2　NVRAM から IWAN RSA キーを削除します。次のコマンドを使用します。

crypto key zeroize rsa sdn-network-infra-iwan

write erase

ステップ 3　元の設定を復元します。次のコマンドを使用します。

config replace bootflash:<original-config-file> force

write

例：

```
RPRE-GA-1-HUB-INET# config terminal
Enter configuration commands, one per line.End with CNTL/Z.
PRE-GA-1-HUB-INET(config)# no crypto pki trustpoint sdn-network-infra-iwan
% Removing an enrolled trustpoint will destroy all certificates
 received from the related Certificate Authority.

Are you sure you want to do this? [yes/no]: yes
% Be sure to ask the CA administrator to revoke your certificates.

PRE-GA-1-HUB-INET(config)# crypto key zeroize rsa sdn-network-infra-iwan
Do you really want to remove these keys? [yes/no]: yes
PRE-GA-1-HUB-INET(config)# end
PRE-GA-1-HUB-INET# write erase
```

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
PRE-GA-1-HUB-INET# config replace bootflash:clean-config force
%EIGRP: Deleting base topology is not allowed.
% Interface GigabitEthernet0/0/4 IPv4 disabled and address(es) removed due to enabling VRF
IWAN-TRANSPORT-2% Profile is applied to Tunnel11-head-0 (head) and possibly other crypto
maps
% No such key-chain% Profile is applied to Tunnel11-head-0 (head) and possibly other
crypto maps% Profile is applied to Tunnel11-head-0 (head) and possibly other crypto maps%
Profile is applied to Tunnel11-head-0 (head) and possibly other crypto maps% Profile is
applied to Tunnel11-head-0 (head) and possibly other crypto maps
The rollback configlet from the last pass is listed below:
********
!List of Rollback Commands:
no crypto ikev2 profile FVRF-IKEv2-IWAN-TRANSPORT-2
end
********


Rollback aborted after 5 passes
PRE-GA-1-HUB-INET# write
```

サイト プレフィックスの追加または削除

ハブのプロビジョニング後に、サイト プレフィックスを追加または削除できます。

(注)　このオプションは、L3 ブラウンフィールド サイトでのみ使用できます。

手順

ステップ 1　シスコ インテリジェント WANのホームページで、[Manage Branch Sites]をクリックします。[Sites] ページが開きます。

ステップ 2　[Site(s)]タブをクリックします。[Site Status] ページの [Action]列で、[Update Site Prefix]（ペン）アイコンをクリックします。[LAN Site Prefix] ダイアログボックスが開きます。

ステップ 3　サイト プレフィックスを追加するには、[+]アイコンをクリックします。

ステップ 4　サイト プレフィックスを削除するには、削除するプレフィックスの横にあるチェックボックスをオンにして、[X]アイコンをクリックします。

(注)　すべてのプレフィックスを削除することはできません。サイトごとに少なくとも 1 つのプレフィックスが必要です。

ステップ 5　[Apply Changes]をクリックします。

ブラウンフィールド検証メッセージ

この章の内容は、次のとおりです。

Cisco IWAN へのグリーンフィールド/ブラウンフィールド デバイスの追加

Cisco IWAN アプリケーション（IWAN アプリ）では、IWAN ネットワークに「グリーンフィールド」デバイスまたは「ブラウンフィールド」デバイスを追加できます。

「グリーンフィールド」とは、新しい未設定のデバイスのことです。これらのデバイスには既存の設定がないので、IWAN ネットワークに導入して IWAN アプリで設定するときに競合が発生しません。

「ブラウンフィールド」とは、IWAN ネットワークに追加されている既存のサイトに属するデバイスのことです。これらのデバイスには IWAN ベースの設定と同期する既存の設定があり、それによって競合が引き起こされる可能性があります。

検証

ブラウンフィールド デバイスのプロビジョニング時に、IWAN アプリは検証を実行して、設定の競合があるかどうかを確認します。競合は次の 2 つのカテゴリで報告されます。

- エラー：IWAN ネットワークへのデバイスの追加を妨げる競合。
- 警告：IWAN ネットワークへのデバイスの追加を妨げない競合。検証での警告を引き起こす設定の問題を修正することを推奨します。

プロビジョニング時に IWAN アプリによってエラーまたは警告が検出された場合は、デバイスの問題を修正して、再び検証を実行します。詳細については、エラーおよび警告の項を参照してください。

エラー

次の表は、検証中に発生する可能性があるエラーを示しています。これらのエラーは、IWAN ネットワークへのデバイスの追加を妨げます。

表 A-1　検証エラー

設定の競合	推奨事項
Username configuration must have privilege level 15（ユーザ名の設定には特権レベル 15 が必要です）	デバイスに権限レベル 15 のユーザ名を設定します。 **例：** **username** *username* **privilege 15 password 0** *password*
PfR configuration must not be present on the device（デバイス上に PfR の設定が存在しないようにしてください）	デバイスにパフォーマンス ルーティング（PfR）の設定がないことを確認します。 **例：** **no domain ONE**
QoS configuration must not be present on the device（デバイス上に QoS の設定が存在しないようにしてください）	デバイスに QoS の設定がないことを確認します。 **例：** **no class-map match-any nbar-12-cls#VOICE** **no policy-map nbar-12-cls** **no policy-map IWAN-INTERFACE-SHAPE-ONLY-INTERNET** **no service-policy input nbar-12-cls** **no service-policy output IWAN-INTERFACE-SHAPE-ONLY-INTERNET**
Interface loopback 47233 must not be configured on the device（デバイスに interface loopback 47233 を設定しないでください）	デバイスから interface loopback 47233 を削除します。 **例：** **no interface loopback47233**
IWAN trustpoint configuration must not be present on device（デバイス上に IWAN トラストポイントの設定が存在しないようにしてください）	デバイスから Cisco IWAN トラストポイントの設定を削除します。 **例：** **no crypto pki trustpoint sdn-network-infra-iwan**
VPN routing and forwarding (VRF) configuration must not be present on the device（デバイス上に VPN ルーティングおよび転送（VRF）の設定が存在しないようにしてください）	Cisco IWAN の設定に影響するため、既存の VRF を削除します。 ルータに以下の VRF がないことを確認します。 • IWAN-TRANSPORT-1 • IWAN-TRANSPORT-2 • IWAN-TRANSPORT-3 • IWAN-TRANSPORT-4 **例：** **no ip vrf IWAN-TRANSPORT-4**

表 A-1　検証エラー（続き）

設定の競合	推奨事項
Recovery configuration file unavailable in flash（フラッシュ内に使用可能なリカバリ設定ファイルがありません）	デバイスのリカバリを可能にするには、IWAN リカバリ設定ファイル「IWAN_RECOVERY.cfg」が必要です。 次の CLI コマンドを使用してリカバリ ファイルを作成します。 **copy running-config flash:IWAN_RECOVERY.cfg**
Conflicting EIGRP configuration present on the device（デバイス上に競合する EIGRP の設定があります）	次の CLI コマンドを使用して EIGRP の設定を削除します。 **no router eigrp IWAN-EIGRP**
Configure Port-Channel in aggregate mode to support QoS policy configuration（QoS ポリシー設定をサポートできるように、ポートチャネルを集約モードに設定してください）	ASR ルータにのみ該当します。ポートチャネルを WAN/LAN インターフェイスとして使用する場合は、ポートチャネルが集約モードであることを確認します。 次の CLI コマンドを使用して、ポートチャネルを集約モードに設定します。 **platform qos port-channel-aggregate <port-channel-number>**
QoS policy configuration is not supported for the targeted type of interface: Port-Channel（QoS ポリシー設定は、ターゲットのインターフェイス タイプ「Port-Channel」ではサポートされません）	デバイスのプラットフォーム タイプが、ポートチャネル インターフェイスで QoS ポリシー設定をサポートしていません。 他のタイプの LAN/WAN インターフェイスを選択します。

警告

次の表は、検証中に発生する可能性があるエラーを示しています。以下の警告は IWAN ネットワークへのデバイスの追加を妨げませんが、これらの警告を引き起こす問題を修正することをお勧めします。

表 A-2　検証の警告

設定の競合	推奨事項
Please make sure at least two interfaces for WAN and LAN are up and running（WAN および LAN 用として少なくとも 2 つのインターフェイスが確立され動作していることを確認してください）	WAN および LAN 用として 2 つのインターフェイスが確立され動作していることを確認します。 **show ip interface brief** コマンドを使用して確認します。
IWAN related crypto configuration found on the device（デバイスで IWAN 関連の暗号化設定が検出されました）	暗号化設定は Cisco IWAN の設定に影響を及ぼす可能性があるため、暗号化設定を削除します。 **例:** `crypto zeroize mypubkey rsa sdn-network-infra-iwan`

No routing protocol found on device（デバイスにルーティング プロトコルがありません）	デバイスで次のルーティング プロトコルのいずれかを有効にします。
	例:
	`router ospf AS number`
	`router eigrp AS number`
	`router bgp AS number`

表 A-2　検証の警告（続き）

設定の競合	推奨事項

EZPM configuration found on the device（デバイスで EZPM の設定が検出されました）	Easy Performance Monitor（EZPM）の設定は Cisco IWAN の設定に影響を及ぼす可能性があるため、EZPM の設定を削除します。
	
	例：
	`no class-map match-all Business-Critical-and-default-tcp-only`
	`no performance monitor context IWAN-Context profile application-experience`

NBAR configuration found on the device（デバイスで NBAR の設定が検出されました）	Network Based Application Recognition（NBAR）の設定は Cisco IWAN の設定に影響を及ぼす可能性があるため、NBAR の設定を削除します。
	
	例：
	`no ip nbar attribute-map Consumer_App_Prof`
	`no ip nbar attribute-map Other_Custom`
	`no ip nbar attribute-map Net_Admin_Custom`

No device information available for validation（検証に使用可能なデバイス情報がありません）	再度検証し、問題がまだ解決されない場合は以下を確認します。 • デバイスが起動して動作している。 • インターネット接続が確立されている。
Device does not have valid image version and K9 package（デバイス上に有効なイメージバージョンと K9 パッケージがありません）	Cisco IWAN アプリが、デバイスにロードされている Cisco ソフトウェア イメージをサポートしていません。15.5(3) または 15.5(4) のイメージと K9 機能パックを使用して、デバイスを起動します。 **例：** `asr1000rp1-adventerprisek9.03.16.00.S.155-3.S-ext.bin`
Insufficient number of VTY lines present on the device（デバイス上の VTY 回線の数が不十分です）	デバイスに最低 16 の VTY 回線を設定する必要があります。 **line vty <first-line-number> <last-line-number>**
One of the VTY line exec-timeout is less than 5 mins（いずれかの VTY 回線の実行タイムアウトが 5 分未満になっています）	VTY 回線の実行タイムアウトが 5 分以上であることを確認します。 次の CLI コマンドを使用して確認します。 **show running-config | sec line vty**
Configured Throughput on device does not match with installed license throughput（デバイスに設定されているスループットがインストール済みライセンスのスループットと一致しません）	CSR ルータにのみ該当します。最大スループットを達成するには、次のようにして **platform hardware throughput level** CLI コマンドを削除します。 **no platform hardware throughput level MB <configured-value>**
No active license found on the device（デバイスにアクティブなライセンスがありません）	CSR ルータにのみ該当します。ライセンスが失効しているか、サポートされていません。 次の CLI コマンドを使用して、ライセンスの問題を確認します。 **show self-diagnostics**

表 A-2　検証の警告(続き)

設定の競合	推奨事項
Device does not have required license(必要なライセンスがデバイスにありません)	必要なライセンスがデバイスで有効になっていません。使用しているプラットフォームのライセンスを有効にします。 • ASR ルータ:adventerprisek9(または advipservicesk9)および IPSEC EULA が承認されている必要があります。 • ISR 4000 シリーズ ルータ:appxk9 および securityk9 • ISR G2 ルータ:datak9 および securityk9 • CSR ルータ:ax
Device clock is not synchronized(デバイスのクロックが同期していません)	ルータのクロックがコントローラのクロックと同期していることを確認します。**show clock** コマンドを使用して確認します。 次の CLI コマンドを使用して NTP サーバを設定することを推奨します。 **ntp server <controller-ip>**