Cisco Business Dashboard & Probe バージョン 2.5.1 アドミニストレーション ガイド

初版：2022 年 11 月 14 日

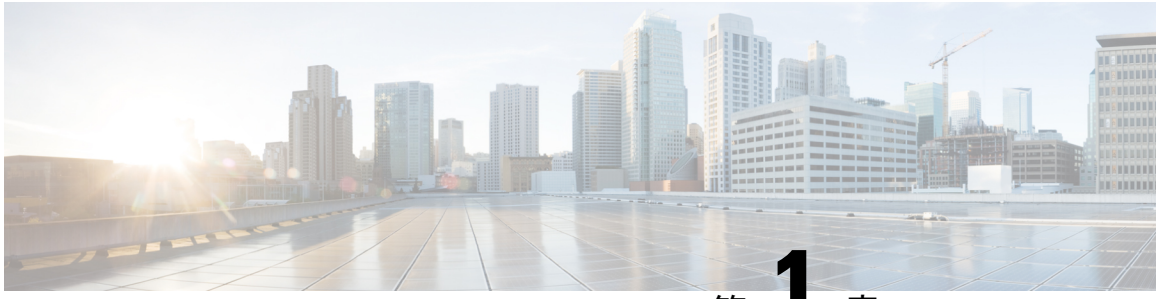
最終更新：2022 年 11 月 27 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

Cisco Business ダッシュボードの概要

この章は、次の項で構成されています。

About Cisco Business ダッシュボード

Cisco Business ダッシュボードは、Cisco Business ネットワーク内のデバイスを監視および管理するのに役立つツールを提供します。ネットワークを自動的に検出し、スイッチ、ルータ、ワイヤレスアクセスポイントなど、サポートされているすべてのデバイスを設定および監視できるようにします。また、ファームウェアの更新のリリースや、保証対象外またはサポート契約での対象外となったデバイスについても知らせます。

Cisco Business ダッシュボードは、以下に説明する 2 つの個別のコンポーネントまたはアプリケーションで構成される分散アプリケーションです。

ダッシュボード

ダッシュボードとも呼ばれる Cisco Business ダッシュボードは、ネットワーク内の便利な場所にインストールされます。Dashboard のユーザーインターフェイスから、ネットワーク内のすべてのサイトのステータスを大まかに把握したり、単一のサイトまたはデバイスに集中して、そのサイトまたはデバイスに固有の情報を表示したりすることができます。

プローブ

プローブとも呼ばれる Cisco Business ダッシュボードプローブ は、ネットワーク内の各サイトにインストールされ、ダッシュボードに関連付けられています。プローブはネットワーク検出を実行し、Dashboard に代わって各管理対象デバイスと直接通信します。

（注） 特定のネットワークデバイスのサポートは、Dashboard と直接関連付けられ、プローブを介在させずに管理されます。この方法でネットワークデバイスが直接管理されている場合、デバイスに対するすべての管理機能を使用できますが、ネットワーク検出プロセスは、プローブを介在させる場合と比較して検索範囲が狭くなることがあります。

対象読者

このガイドは主に Cisco Business ダッシュボード ソフトウェアのインストールと管理を担当するネットワーク管理者を対象としています。

新しいリリース情報とアップデート

このセクションでは、2022 年 9 月時点における Cisco Business Dashboard リリース 2.5.x の新機能について説明します。

表 *1 : Cisco Business* ダッシュボード リリース *2.5.1* の新機能と変更された動作

機能	説明	参照先
ワイヤレスネットワーク向けゲストポータル	ワイヤレスネットワーク向けゲストポータルは、Cisco Business Dashboard によって一元管理できます。	ワイヤレス LAN の設定（57 ページ）を参照してください ゲストポータルの設定 （60 ページ）を参照してください

表 *2 : Cisco Business* ダッシュボード リリース *2.5* の新機能と変更された動作

機能	説明	参照先
ワイヤレス設定の拡張	無線設定、無線周波数の最適化、不正アクセスポイント、干渉源の検出など、追加のワイヤレス設定を管理できるようになりました。	詳細なデバイス情報の表示（37 ページ）を参照してください ワイヤレス LAN の設定（57 ページ）を参照してください ワイヤレス無線の設定 （59 ページ）を参照してください

機能	説明	参照先
ユーザーベースのネットワークアクセスに対応した認証サービス。	Cisco Business Dashboard を認証サーバーとして使用して、ワイヤレスLANおよびスイッチポートでユーザーベースの認証を有効にできます。	ポート管理について （47ページ）を参照してください ワイヤレス LAN の設定（57 ページ）を参照してください ユーザー（101ページ）を参照してください セキュリティ上の留意事項の FAQ （171 ページ）を参照してください
新しい通知	デバイスの管理者パスワードの有効期限が切れた場合や、現行のデバイス構成が要件と一致しない場合に状況を把握できるように、新しい通知が追加されました。	サポートされる通知 （151ページ）を参照してください。
GUI での Let’s Encrypt 証明書の管理	Let's Encrypt 証明書をインストールし、管理 GUI からすべて管理できるようになりました。	証明書の管理（116ページ）を参照してください。

Dashboard と Probe のシステム要件が更新されました。詳細については、関連資料 （3 ページ） のインストールガイドを参照してください。

すべての正式なリリースノートは、Cisco Business Dashboard Release Notesにあります。

関連資料

Cisco Business ダッシュボード のドキュメントは、多数の個別のガイドで構成されています。これには次が含まれます。

- **アドミニストレーションガイド（このドキュメント）**：このソフトウェアが提供するすべての機能とオプションに関する詳細と、それらの設定方法および使用方法を示したリファレンスガイドです。
- **デバイスサポートリスト**：このリストには、Cisco Business ダッシュボード でサポートされるデバイスの詳細と、各デバイスタイプで利用可能な機能が記載されています。Cisco Business ダッシュボード でサポートされているすべてのデバイスのリストについては、『Cisco Business Dashboard Technical References』を参照してください。
- **クイックスタートガイド**：このガイドでは、最も一般的に選択されるオプションを使用した Cisco Business ダッシュボード の初期セットアップ方法について詳しく説明します。

ネットワークの管理に必要な基本的なタスクの概要については、『Cisco Business Dashboard Quick Start Guide』[英語] を参照してください。

- **リリースノート**：これらは、新しいファームウェアリリースごとにすべての新機能と修正をリストしたドキュメントです。これらは Cisco Business Dashboard Release Notes にあります。
- **インストールガイド**

  次の表に、異なるプラットフォームに展開できる Cisco Business ダッシュボード ソフトウェアのすべてのインストールガイドを示します。

  Cisco Business ダッシュボード および Cisco Business ダッシュボードプローブ のシステム要件については、これらのガイドを参照してください。

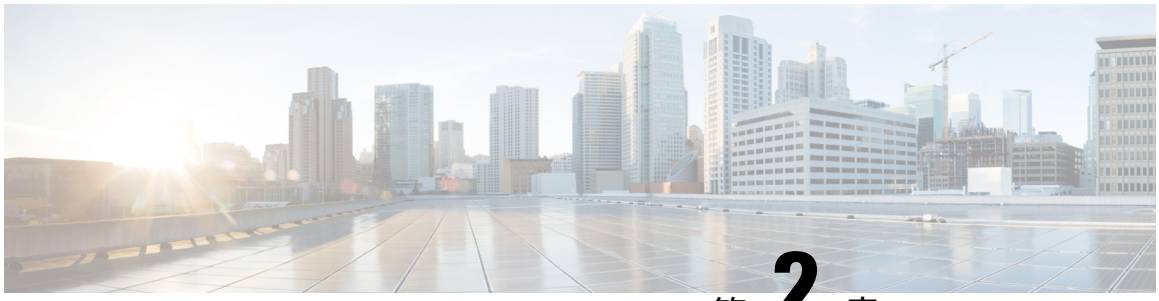
サポートされるプラットフォーム	参照先
Amazon Web Services	Cisco Business Dashboard Installation Guide for Amazon Web Services (AWS)
Microsoft Azure	Cisco Business Dashboard Installation Guide for Microsoft Azure
Oracle VirtualBox	Cisco Business Dashboard & Probe Installation Guide for Oracle VirtualBox
Microsoft Hyper-V	Cisco Business Dashboard Installation Guide for Microsoft Hyper-V
VMware vSphere、ワークステーション、およびフュージョン	Cisco Business Dashboard & Probe Installation Guide for VMWare
Ubuntu Linux（Dashboard および Probe）および Raspbian Linux（Probe のみ）	Cisco Business Dashboard & Probe Installation Guide for Linux

用語

用語	説明
Hyper-V	Microsoft Corporation によって提供されている仮想化プラットフォーム。
Open Virtualization Format（OVF）	1 つ以上の仮想マシンが OVF 形式で格納された TAR アーカイブ。仮想マシン（VM）をパッケージ化および配布するための、プラットフォームに依存しない手段です。

用語	説明
Open Virtual Appliance/Application（OVA）ファイル	次のファイルを含むパッケージは、仮想マシンの説明に使用され、**.TAR** 形式のパッケージングにより 1 つのアーカイブに保存されます。 • 記述子ファイル（.OVF） • Manifest（.MF）および証明書ファイル（任意）
Raspberry Pi	Raspberry Pi 財団によって開発された、極めて低コストのシングルボードコンピュータ。詳細については、*https://www.raspberrypi.org/* [英語] を参照してください。
Raspberry Pi OS	正式には Raspbian として知られる Raspberry Pi OS は、Raspberry Pi 用に最適化された、Debian ベースの Linux ディストリビューションです。詳細については、*https://www.raspberrypi.org/software/* [英語] を参照してください。
VirtualBox	Oracle Corporation によって提供されている仮想化プラットフォーム。
Virtual Hard Disk（VHD）	ハード ドライブの完全な内容を格納するためのディスク イメージ ファイル形式。
仮想マシン（VM）	ゲスト オペレーティング システムと関連するアプリケーション ソフトウェアが動作可能な、仮想コンピューティング環境。同一のホスト システム上で同時に複数の VM を実行できます。
• VMWare ESXi • VMWare V5 • vSphere Server • VMware Workstation	VMWare Inc. によって提供されている仮想化プラットフォーム。
vSphere クライアント	vCenter Server または ESXi に任意の Windows PC からリモートで接続できるようにするためのユーザ インターフェイス。vSphere Client のプライマリ インターフェイスを使用して、VM、そのリソース、およびホストの作成、管理、およびモニタを行うことができます。VM へのコンソール アクセスも提供します。
ハイパーバイザ	仮想マシンモニターまたは VMM とも呼ばれ、仮想マシン（VM）を作成して実行するソフトウェアです。ハイパーバイザでは、メモリや処理などのリソースを仮想的に共有することで、1 台のホストコンピュータで複数のゲスト VM をサポートできます。
Amazon Web Services（AWS）	オンデマンドのクラウド コンピューティング プラットフォームです。

用語	説明
Microsoft Azure Active Directory	サイバーセキュリティ攻撃の 99.9% からユーザーを保護するために、シングルサインオンと多要素認証を提供するクラウドベースの ID およびアクセス管理サービスです。



第 2 章

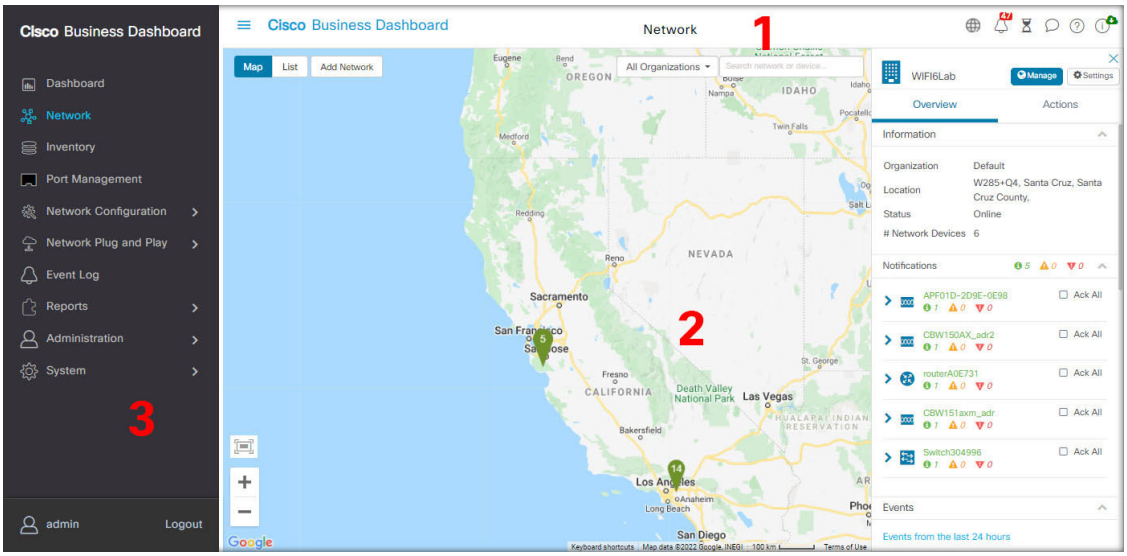
Cisco Business Dashboard & Probe の使用

この章は、次の項で構成されています。

Cisco Business Dashboard GUI の使用

この章では、ナビゲーションペインのリンクの説明を含む Cisco Business ダッシュボード GUI の概要を説明します。

Home ウィンドウ



1. [Header] ペイン

ヘッダー ツールバーには以下のオプションが含まれています。

- ナビゲーションペインを表示するためのメニューボタン
- ヘッダー テキスト
- 言語選択、通知、タスクアクティビティ、フィードバック、状況依存ヘルプ、バージョン情報などの機能を示す一連のアイコン

2. [Work] ペインは、機能インターフェイスが表示される領域です。

   ナビゲーションペインでオプションをクリックすると、対応するウィンドウがこの領域に表示されます。

3. [Navigation] ペインでは、Cisco Business ダッシュボード の機能にアクセスできます。ナビゲーションウィンドウは、[Menu] アイコンをクリックすると表示され、選択の操作をすると非表示になります。

   現在ログインしているユーザは、ナビゲーションウィンドウの下部に表示されます。

ナビゲーション ペインのオプション

ナビゲーション ペインには、Cisco Business ダッシュボード の主な機能にアクセスするためのオプションが用意されています。

アイコン	説明
	[Dashboard]を使用すると、ネットワークのパフォーマンスを、一定の時間に渡ってモニタできます。ダッシュボードでは、トラフィック レベル、接続されているデバイス数、ネットワークに関するその他の詳細をモニタできます。
	[Network] アイコンは、ネットワーク内のすべての場所の概要をマップまたはリストとして表示します。検出された各ネットワークとデバイスのさまざまなビューも含まれています。ビューには、ネットワークトポロジとネットワークの物理レイアウトを追跡するためのフロアプランなどがあります。
	[Inventory] ツールには、ネットワーク内のすべてのデバイスのリストが表示され、デバイスに関する詳細情報を表示したり、ファームウェアの更新、バックアップ構成、リブートなどのアクションを実行したりできます。
	[Port Management] オプションでは、すべてのネットワークデバイスのフロントパネルビューが提供され、個々のポートに関する詳細を表示したり、設定を変更したりできます。
	[Network Configuration] ページでは、ネットワーク内の設定プロファイルを管理できます。

アイコン	説明
	[Network Plug and Play] ページでは、ネットワークデバイスをゼロタッチで展開でき、インストール時に Cisco Business ダッシュボード からファームウェアと構成ファイルを自動的にダウンロードできます。
	[Event Log] ページには、ネットワークで発生したすべてのイベントのリストが表示されます。フィルタを使用して結果を制限することで、目的のイベントのみ表示できます。
	[Reports] オプションには、サービス終了のお知らせ、保証情報、サービス契約の詳細など、ネットワークデバイスに関するライフサイクル情報を提供する多数のレポートが表示されます。
	[Administration] の各ページでは、Cisco Business ダッシュボード をメンテナンスすることができます。
	[System] ページは、Cisco Business ダッシュボード アプリケーションの管理に使用されます。
	現在ログインしているユーザは、[Logout] オプションとともにナビゲーションバーの下部に表示されます。ユーザ名をクリックして、ユーザのプロファイルページを表示します。

ヘッダー ツールバーのオプション

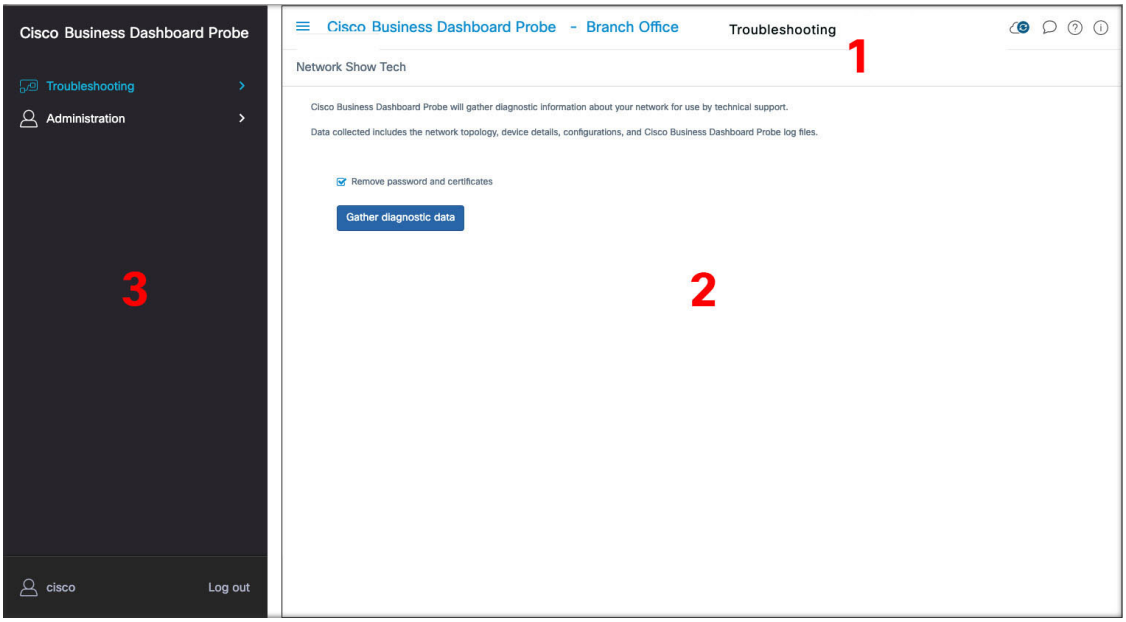
ヘッダーツールバーでは、その他のシステム機能にアクセスでき、システムの通知が表示されます。

アイコン	説明
	[Menu] ボタンはヘッダーの左上にあります。このボタンをクリックして、ナビゲーションペインを表示します。
	[Language Selection] ドロップダウンリストでは、ユーザーインターフェイスの言語を選択できます。
	[Notification Center] アイコンには、Cisco Business ダッシュボード の未処理の通知の数と重大度が表示されます。このアイコンをクリックすると、通知センターパネルが表示され、表示される通知イベントをフィルタリングするオプションが提供されます。詳細については、このガイドの現在のデバイスの通知の表示とフィルタリング （153 ページ）を参照してください。

アイコン	説明
	[Job Center] アイコンには、現在実行中のジョブのステータスと過去のジョブの履歴が表示されます。ジョブには、ユーザーが実行したジョブとシステムジョブの両方を含む、Cisco Business ダッシュボードによって実行されたアクションが含まれます。このアイコンをクリックすると、保留中、進行中、完了したジョブ、および後日スケジュールされたジョブが表示されます。
	[Feedback] アイコンをクリックして、Cisco Business ダッシュボード を使用した体験についてのフィードバックや、改善のための提案を提供します。
	[Help] アイコンをクリックし、Cisco Business ダッシュボード のオンラインドキュメントを開きます。
	[About Cisco Business Dashboard] アイコンをクリックして、現在のバージョンを含むこのバージョンに関する情報を表示します。新しいバージョンが利用可能な場合は、矢印の付いた緑色のアイコンがアイコンに表示され、更新を適用するためのリンクがポップアップに表示されます。

Cisco Business Dashboard Probe GUI の使用

Cisco Business Dashboard Probe にログインすると、[Home] ページが表示されます。



1. [Header] ペイン

   ヘッダー ツールバーには以下のオプションが含まれています。

- ナビゲーションペインを表示するためのメニューボタン
- ヘッダー テキスト
- 言語選択、通知、タスクアクティビティ、フィードバック、状況依存ヘルプ、バージョン情報などの機能を示す一連のアイコン

2. [Work] ペインは、機能インターフェイスが表示される領域です。

   ナビゲーションペインでオプションをクリックすると、対応するウィンドウがこの領域に表示されます。

3. [Navigation] ペインでは、Cisco Business ダッシュボードプローブ の機能にアクセスできます。ナビゲーションウィンドウは、[Menu] アイコンをクリックすると表示され、選択の操作をすると非表示になります。

   現在ログインしているユーザは、ナビゲーションウィンドウの下部に表示されます。

ナビゲーション ペインのオプション

ナビゲーション ペインには、Cisco Business ダッシュボードプローブ の主な機能にアクセスするためのオプションが用意されています。

アイコン	名前	説明
	**Troubleshooting**	これをクリックすると、ネットワークの問題を特定するのに役立つ診断ツールを含むページが [Troubleshooting] セクションから見つかります。
	**Administration**	[Administration] ページでは、 Cisco Business ダッシュボードプローブネットワーク アプリケーションをメンテナンスすることができます。
	**User Options**	現在ログインしているユーザは、[Logout] オプションとともにナビゲーションバーの下部に表示されます。ユーザ名をクリックして、ユーザのプロファイルページを表示します。

ヘッダー バーのオプション

ヘッダーバーでは、その他のシステム機能にアクセスでき、システムの通知が表示されます。

アイコン	オプション	説明
	メニューボタン	ヘッダーの左上にあります。このボタンをクリックすると、ナビゲーションペインが表示されます。
	言語の選択	このドロップダウン リストでは、ユーザ インターフェイスの言語を選択できます。

アイコン	オプション	説明
	ダッシュボードのステータス	Cisco Business ダッシュボード と Probe 間の接続のステータスが表示されます。このアイコンをクリックすると、Dashboard GUI が表示されます。
	フィードバック	Cisco Business ダッシュボードプローブ を使用した体験についてのフィードバックや、改善のための提案を送る場合にクリックします。
	ヘルプ	このアイコンをクリックして、Cisco Business ダッシュボードプローブ のオンラインドキュメントを開きます。
	Cisco Business Dashboard Probeについて	このアイコンをクリックすると、現在のバージョンなど、Cisco Business ダッシュボードプローブ に関する情報が表示されます。新しいバージョンが利用可能な場合、アイコンにバッジが表示され、更新を適用するためのリンクがポップアップ表示されます。詳細については、Cisco Business Dashboard & Probe のアップグレード （12 ページ）を参照してください。

Cisco Business Dashboard & Probe のアップグレード

シスコは随時、Cisco Business ダッシュボードとプローブ の新しいバージョンと更新プログラムをリリースしており、cisco.com のソフトウェアセンターで公開しています。Cisco Business ダッシュボードはソフトウェアセンターで更新プログラムを定期的に確認し、見つかった場合はUI のヘッダーパネルの  アイコンのバッジが表示されます。クリックして Dashboard に更新をダウンロードし適用させることができます。自分で更新をダウンロードし手動で適用することもできます。

更新をダウンロードして適用するように Dashboard を設定するには、次の手順を実行します。

1. [About Cisco Business Dashboard] をクリックし、ポップアップを開きます。Dashboard または関連する Probe の更新を入手できる場合、ここに一覧表示されます。
2. Dashboard の更新を入手できる場合、その更新の横にあるオプションボタンを選択し、[Upgrade] をクリックします。

   Dashboard により更新がダウンロードされ、適用されます。[About Cisco Business Dashboard] ポップアップでこの進行状況を確認できます。更新が完了すると、Dashboard アプリケーションは再起動します。

Dashboard の更新を手動で適用するには、次の手順を実行します。

1. *https://cisco.com/go/cbd-sw* [英語] に移動し、右下の製品選択パネルから [Download Software] オプションを選択して、Cisco Business ダッシュボード Linux インストーラファイルをダウンロードします。
2. Dashboard ファイルシステムにインストーラファイルをコピーします。
3. `sh <filename of installer>` Sudo コマンドを使用してインストーラを実行します。たとえば、`sh cisco-business-dashboard-2.2-ubuntu-xenial-amd64.sh` のようなコマンドを使用します。必要に応じて、sudo プロンプトでパスワードを入力します。このプロセス中に Dashboard アプリケーションが再起動します。

Dashboard からネットワーク内のすべての Probe に更新を適用することもできます。すべての Probe を並行して更新することも、Probe を個別に更新することもできます。

Dashboard からすべての Probe を並行して更新するには、次の手順を実行します。

1. [About Cisco Business Dashboard] をクリックし、ポップアップを開きます。

   Dashboard または関連する Probe の更新を入手できる場合、ここに一覧表示されます。

（注） Dashboard の更新を入手できる場合、Probe をアップグレードする前にその更新を実行します。

最初に Probe をアップデートしようとすると、エラー メッセージを受け取ります。

2. Probe のアップデートの横にあるオプションボタンを選択し、[Upgrade] をクリックします。
3. Probe のユーザ インターフェイスでアップデートの進行状況を確認できます。

Dashboard から個々の Probe を更新するには、次の手順を実行します。

1. Dashboard の更新を入手できる場合、プローブをアップグレードする前にその更新を実行します。

   Dashboard を更新する前にプローブを更新しようとすると、エラーメッセージが表示されます。

2. ナビゲーションで [Network] を選択します。
3. [Map View] または [List View] ビューで、更新するネットワークを選択します。
4. ネットワークの [Basic Info] パネルで [Action] タブを選択します。
5. **[Upgrade]** をクリックします。

   ジョブセンターで更新の進行状況を確認できます。

（注） ネットワークデバイスで実行されている組み込みプローブを使用する場合は、そのデバイスのドキュメントを参照して更新を実行してください。一部のデバイスでは、デバイスファームウェアから独立して Probe アプリケーションを更新することができません。

（注） Amazon Web Services（AWS）や Microsoft Azure で稼働している Cisco Business Dashboard をリリース 2.4.1 以前からリリース 2.5.0 以降にアップグレードする場合、ポート 1812 への着信 UDP トラフィックを許可するように AWS または Azure のセキュリティポリシーを手動で更新する必要があります。

Cisco Business Dashboard または Probe のオペレーティングシステムのアップグレード

Cisco Business ダッシュボードとプローブ バージョン 2.3.x 以前のバージョンは、Ubuntu Linux ディストリビューションバージョン 16.04（Xenial Xerus）で動作します。

Cisco Business ダッシュボード の将来のバージョンは、Ubuntu 20.04（Focal Fossa）でのみサポートされます。その結果、2.3.x 以降の既存の Cisco Business ダッシュボード または Probe のインストールをアップグレードするには、更新されたオペレーティングシステムが必要です。

Ubuntu 16.04 と 20.04 の間の大幅な変更により、Cisco Business ダッシュボードとプローブ のオペレーティングシステムのバージョンごとに個別のインストーラが提供されます。既存のダッシュボードまたはプローブのインストールでオペレーティングシステムのインプレースアップグレードを実行することはできません。以下のセクションでは、ダッシュボードとプローブのオペレーティングシステムを更新するための推奨アプローチについて説明します。

Cisco Business Dashboard オペレーティングシステムのアップグレード

既存の Cisco Business ダッシュボード を新しいバージョンのオペレーティングシステムにアップグレードするには、次のプロセスを使用します。

1. 既存の Cisco Business ダッシュボード アプリケーションのバックアップを作成します。
    1. ダッシュボード GUI にログオンし、ナビゲーションペインから**[System]** > **[Backup]**を開きます。
    2. 画面に表示されるフィールドにバックアップを保護するためのパスワードを入力し、[Backup & Download] ボタンをクリックします。
2. 更新されたオペレーティングシステム上で実行されている Cisco Business ダッシュボードの新しいインスタンスを作成します。

- 既存のダッシュボードが仮想マシンまたは Amazon Web Services などのクラウドプロバイダーで実行されている場合は、既存のインスタンスをシャットダウンしてから、事前に作成された Cisco Business ダッシュボード イメージを使用して新しいインスタンスを作成する必要があります。
- 既存のダッシュボードがサーバーで実行されている Ubuntu Linux 環境に直接インストールされている場合は、更新された Ubuntu バージョンでサーバーを再イメージ化してから Cisco Business ダッシュボード をインストールする必要があります。

Cisco Business ダッシュボードのインストールの詳細については、*https://cisco.com/go/cbd-docs* [英語] にあるインストールガイドを参照してください。

3. Cisco Business ダッシュボードの新しいインスタンスにログオンし、手順1で作成したバックアップを復元します。
   - **[System]** > **[Restore]** に移動します。
   - 表示されたフィールドに、バックアップを保護するために使用するパスワードを入力します。
   - [Upload & Restore] ボタンをクリックしてそのバックアップファイルをアップロードします。
4. 復元プロセスが完了し、新しいインスタンスが正常に実行されていることを確認したら、古いインスタンスを削除します。

   バックアップおよび復元機能の詳細については、後述の Dashboard 設定のバックアップと復元 （124 ページ） を参照してください。

（注） Cisco Business ダッシュボード バックアップファイルは、バックアップしたばかりのシステムと同じバージョンを実行しているシステム、または最大1つの新しいマイナーリリースに復元できます。たとえば、バージョン 2.2.0 を実行しているシステムから作成されたバックアップは、2.3.1 を実行しているシステムには復元できますが、2.4.0 を実行しているシステムには復元できません。

（注） Amazon Web Services（AWS）や Microsoft Azure で稼働している Cisco Business Dashboard をリリース 2.4.1 以前からリリース 2.5.0 以降にアップグレードする場合、ポート 1812 への着信 UDP トラフィックを許可するようにセキュリティポリシーを更新する必要があります。

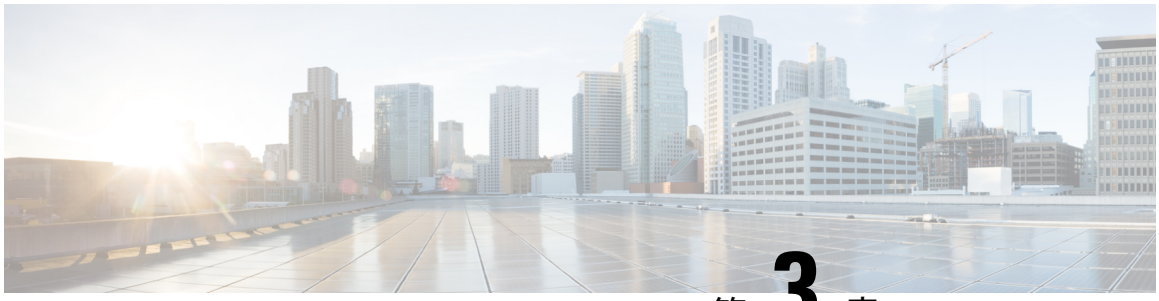
Cisco Business Dashboard Probe オペレーティング システムのアップグレード

Cisco Business ダッシュボードプローブ は、設定データをほとんど保存せず、長期的な統計情報も保存しません。そのため、プローブをホストしているオペレーティングシステムをアップ

グレードする場合は、既存のプローブインスタンスを削除し、新しいオペレーティングシステムで実行されている新しいプローブインスタンスをインストールすることをお勧めします。次に、新しいプローブが Cisco Business ダッシュボード に関連付けられ、関連付けプロセス中に既存のネットワークレコードが選択されます。

Cisco Business ダッシュボードプローブ ソフトウェアのインストールの詳細については、Cisco Business Dashboard Installation Documents [英語] にあるインストールガイドを参照してください。Cisco Business ダッシュボード とプローブの関連付けの詳細については、Cisco Business Dashboard Quick Start Guide [英語] にある 『Quick Start Guide』を参照してください。

（注） 組み込みプローブまたは直接デバイス管理を使用する場合、デバイスのオペレーティングシステムとは別にプローブまたはエージェントをアップグレードする必要はありません。プローブ/エージェントはデバイスファームウェアに含まれており、デバイスのアップグレード時に自動的に更新されます。



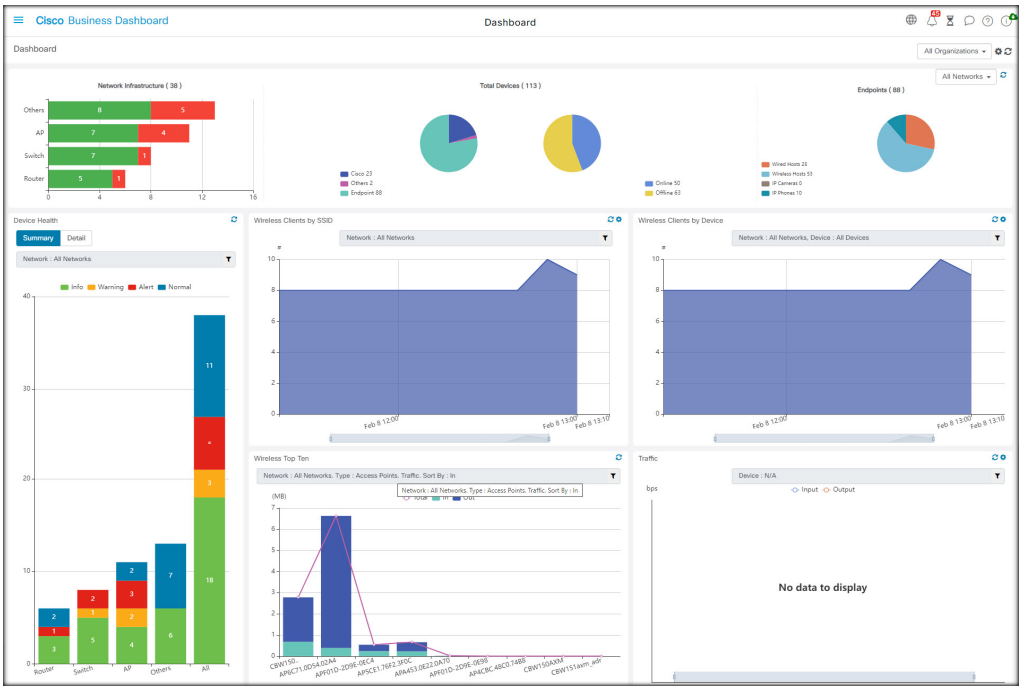
第 3 章

監視ダッシュボード

この章は、次の項で構成されています。

監視ダッシュボードについて

Cisco Business ダッシュボードの [Dashboard] ページでは、ネットワークのパフォーマンスをリアルタイムで表示できます。すべてのデバイスを表示し、データをグラフ形式で提供します。



この監視ダッシュボードは、選択可能なウィジェットのカスタマイズ可能な配置です。ダッシュボードにデフォルトで含まれているウィジェットは以下のとおりです。

ウィジェット	説明
インベントリの概要	ネットワークで検出されたデバイスの内訳を表示します。
デバイスヘルス	ネットワーク内のデバイスの全体的な状態を表示します。
WLAN クライアント カウント	選択したワイヤレスネットワークに関連付けられているデバイスの数を表示します。
デバイス クライアント カウント	選択したワイヤレスアクセスポイントに関連付けられているデバイスの数を表示します。
ワイヤレス トップ 10	トラフィックまたはクライアント数に基づいて、上位 10 のワイヤレスネットワーク、アクセスポイント、またはクライアントを表示します。
トラフィック	選択したインターフェイスを流れるトラフィックのグラフを表示します。

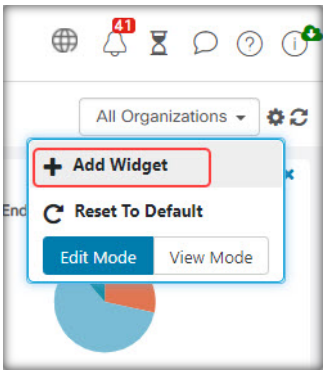
各ウィジェットのコントロールを使用すると、表示されるデータをカスタマイズできます。Dashboard の右上にある組織のドロップダウンを使用すると、特定の組織に表示される情報を制限できます。

グラフィカルウィジェットでは、グラフ上の凡例のラベルをクリックするとデータの各セットの表示を切り替えられます。これにより、表示されるデータをさらに絞り込むことができ、ネットワーク上の特定のデバイス、またはネットワーク自体のトラブルシューティングに役立ちます。

ウィジェットの追加

この機能を使用すると、1 つ以上のウィジェットをダッシュボードに表示されている既存のデフォルトウィジェットに追加して、表示したいデバイスまたはネットワークに固有のタスクをモニターできます。

ステップ 1 ダッシュボードウィンドウの右上にある歯車アイコンをクリックし、[Add Widget] を選択します。



ステップ 2 ポップアップ リストから、追加するウィジェットの種類を選択します。新しいウィジェットがダッシュボードに表示されます。

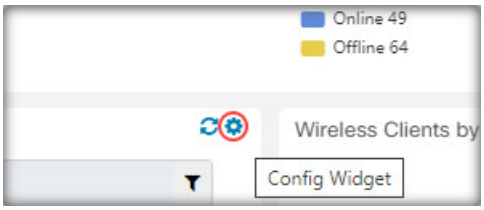
ステップ 3 新しいウィジェットをダッシュボード内の目的の場所にドラッグし、必要に応じてサイズを変更します。

ステップ 4 歯車アイコンをもう一度クリックし、[View Mode] を選択して変更内容を保持します。

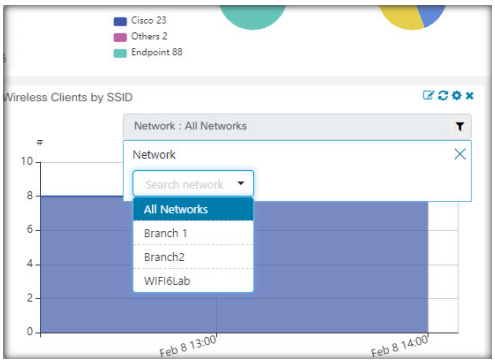
ウィジェットの変更

次の手順で、ダッシュボード上のウィジェットを変更できます。

ステップ 1 ウィジェットの右上にある [Config Widget] アイコンをクリックして、サンプル間隔やしきい値などのパラメータを変更します。



ステップ 2 新しいウィジェット内のドロップダウンリストを使用して、表示する特定のデータを選択します。



ステップ 3 ウィジェットのタイトルを変更するには、[Edit Mode] アイコンをクリックします。

重要 ウィジェットのタイトルを変更するには、ダッシュボードで [Edit Mode] になっている必要があります。

ウィジェットの削除

ステップ 1 ダッシュボード ウィンドウの右上にある歯車アイコンをクリックし、[Edit Mode] を選択します。

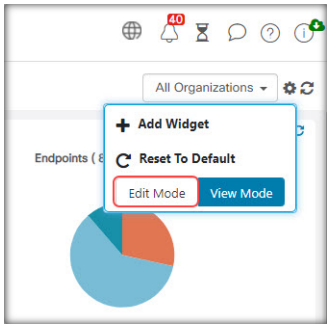
ステップ 2 削除するウィジェットの右上にある [remove widget] アイコンをクリックします。必要に応じて、残りのウィジェットを並べ替えます。

ステップ 3 歯車アイコンをもう一度クリックし、[View Mode] を選択して変更内容を保持します。

ダッシュボードのレイアウトの変更

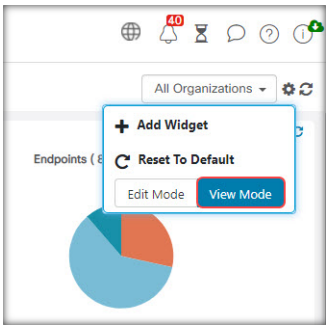
[Dashboard] のレイアウトは、次の手順を使用してカスタマイズできます。

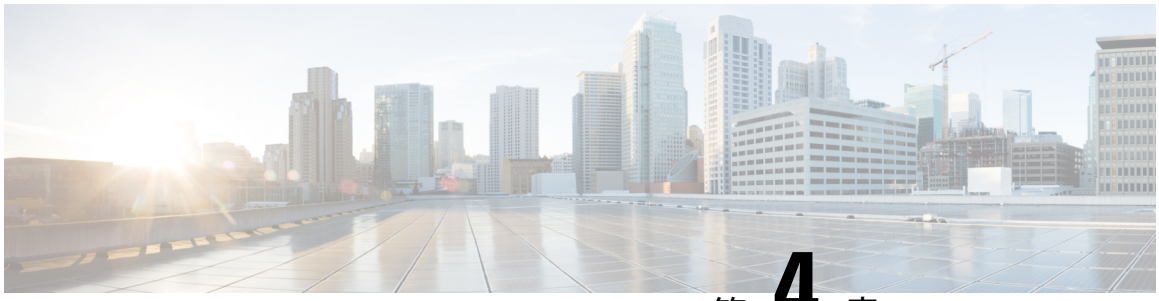
ステップ 1 ダッシュボード ウィンドウの右上にある歯車アイコンをクリックし、[Edit Mode] を選択します。



ステップ 2 ウィジェットを **Dashboard** 内で移動するには、ウィジェットのヘッダーをクリックしてドラッグします。他のウィジェットが動的に調整され、スペースが確保されます。ウィジェットの端または隅をクリックしてドラッグするとサイズを変更することができます。レイアウトを並べ替えると、ダッシュボードのサイズが使用可能な幅に合わせて動的に変更されます。

ステップ 3 歯車アイコンをもう一度クリックし、[View Mode] を選択して変更内容を保持します。


40
All Organizations
Add Widget
Reset To Default
Edit Mode
View Mode



第 4 章

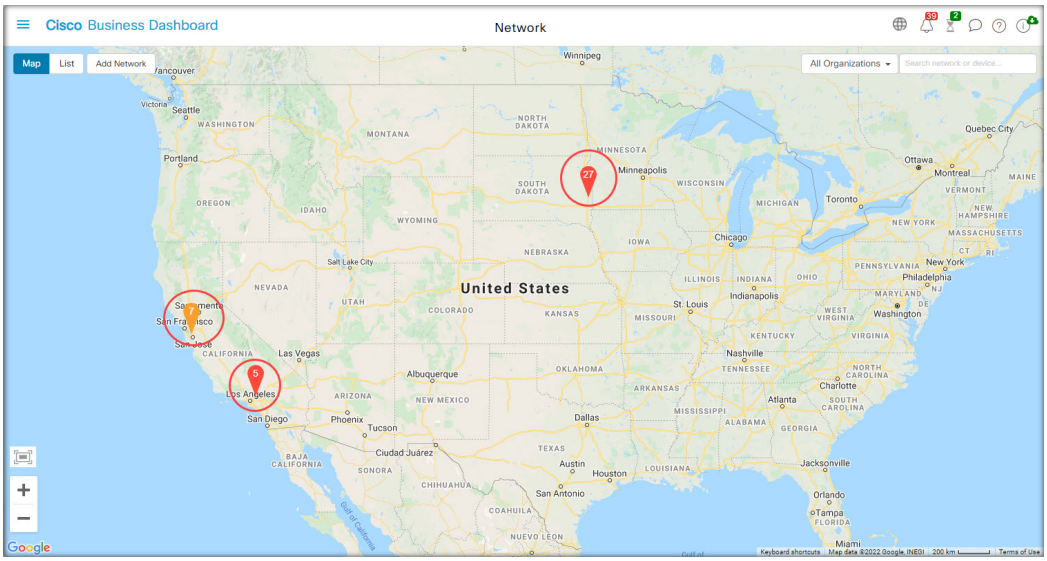
ネットワーク

この章は、次の項で構成されています。

ネットワークについて

[Network] ページにアクセスして、ネットワーク内の場所とすべてのデバイスの概要を表示します。近くにある他のネットワークやデバイスを表示することもできます。ネットワークを選択すると、そのネットワークとデバイスに関する詳細と、それらがすべてどのように機能しているかを確認できます。

[Network] ページには、ネットワーク内の各サイト位置とステータスを示すグラフィックマップとして、またはすべてのサイトのリストとして、ネットワークの概要が表示されます。

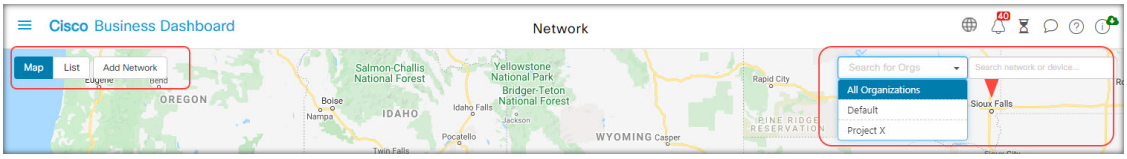


[Map] ビューでは、各ネットワークアイコンに表示される数値でそのサイトに関する未確認の通知の数が示され、アイコンの色で重要度が最も高い未確認の通知が示されます。

（注） マップ上で 2 つ以上のネットワークアイコンの表示位置が相互に近づきすぎていて区別しにくい場合は、単一のクラスタアイコンに置き換えられます。クラスタアイコンをクリックすると、そのクラスタ内のネットワークを分離できるレベルにマップが自動的にズームされます。

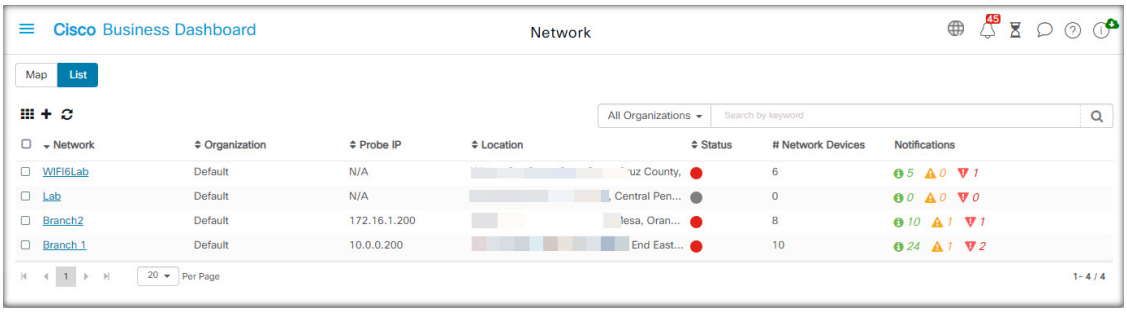
[Network Map] には以下のコントロールがあります。

また、マップ領域のいずれかの場所をクリックしてドラッグすることで、[Work] ペイン内でマップを移動することもできます。



コントロール名	コントロールアクション
[Map/List] 選択	このコントロールを使用して、ネットワークをマップまたはテーブルに表示することを選択します。
[Add Network] ボタン	このボタンを使用して、そのネットワークのプローブを展開する前に、新しいネットワークレコードを作成します。
[Organization] ドロップダウン	ドロップダウンリストから個々の組織を選択して、表示されるネットワークを制限します。

コントロール名	コントロールアクション
[Search] ボックス	ネットワークの名前、アドレスまたはIPアドレスの全体か一部を入力し、そのネットワークをマップ上で検索します。または、デバイスの名前、IPアドレス、シリアル番号、または MAC アドレスの全体か一部を入力し、デバイスが配置されているネットワークを特定することもできます。入力すると、一致する対象のリストが表示されます。 • 一致対象の上にマウスカーソルを移動すると、対応するネットワークが強調表示されます。 • 一致対象を選択すると、対応するネットワークが選択され、ビューの中央に表示されます。
[Zoom] コントロール	これらのコントロールを使用して、マップをズームインおよびズームアウトします。（+）プラス記号をクリックすると拡大し、（-）マイナス記号をクリックすると縮小します。
[Fit-to-view] ボタン	このボタンは、すべてのネットワークマーカーを表示できるように、マップを自動的にズームアウトします。

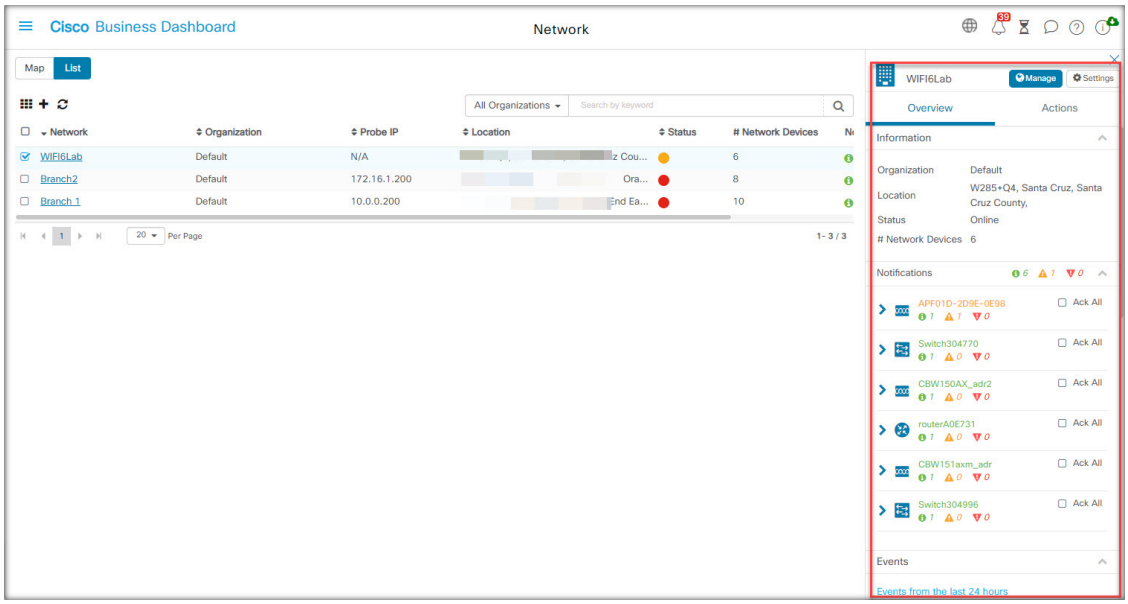


[List] ビューには、同じ情報が表の最後の列に表示されます。ネットワークに関する詳しい情報を表示するには、ネットワークアイコン、またはそのサイトのテーブルの行をクリックします。

[List View] では、次のコントロールを使用できます。

コントロール名	コントロールアクション
[Map/List] 選択	このコントロールを使用して、ネットワークをマップまたはテーブルに表示することを選択します。
[Column Select] アイコン	このアイコンを使用すると、表示する列を選択できます。列見出しをクリックすると、テーブルを並べ替えることができます。
[Add Network]	そのネットワークのプローブを展開する前に、プラス（+）記号をクリックして新しいネットワークを追加します。
[Refresh]	[Refresh] ボタンをクリックするとテーブルが更新され、最新の情報が表示されます。

コントロール名	コントロールアクション
[Organization] ドロップダウン	ドロップダウンリストから個々の組織を選択して、表示されるネットワークを制限します。
[Search] ボックス	ネットワークの名前、アドレス、またはIPアドレスの全体または一部を入力すると、テーブル内の一致しているネットワークのみのリストが表示されます。



ネットワークアイコンまたは行をクリックすると、そのネットワークの [Basic Info] パネルが表示されます。[Basic Info] パネルには以下の情報が含まれています。

- ネットワークの名前。
- ネットワークが属する組織。
- ネットワークの物理アドレス。
- ネットワークの Probe IP アドレスと、ネットワークで検出された IP サブネット。
- Probe のソフトウェアバージョン。
- 接続ステータス。
- このネットワーク内の管理対象デバイスの数。
- このネットワークで現在未確認のすべての通知のリスト。
- 過去 24 時間にこのネットワークで発生したイベントのリスト。

また、[Basic Info] パネルから、ネットワークに対して次の操作を行うこともできます。

- [Manage] をクリックすると、ネットワークトポロジやフロアプランなど、ネットワークに関する詳細情報が表示されます。
- [Settings] をクリックすると、[Network Detail] パネルが表示されます。[Network Detail] パネルの詳細については、以下の「About Network Detail」のセクションを参照してください。
- [Actions] タブをクリックすると、ネットワークに対して使用できるその他のアクションが表示されます。
  - [Remove] をクリックすると、このネットワークおよび関連付けられているすべてのデータがダッシュボードから削除されます。
  - [Upgrade] をクリックすると、このネットワークの Probe ソフトウェアが更新されます。
  - [Show Tech] をクリックすると、このネットワークの Network Show Tech アーカイブが生成されます。

ネットワーク詳細パネルについて

[Network Detail] パネルでは、そのネットワークに固有の情報を表示および更新できます。次の情報が含まれます。

- ネットワーク名、説明、組織、デフォルトのデバイスグループなどの主要なネットワークパラメータ。
- ネットワークの場所。
- Cisco Active Advisor にインベントリ情報をアップロードするときにネットワークに使用するログイン情報。
- このネットワーク内の Probe のロギング設定。Probe のログ設定の管理 （166 ページ） を参照してください。
- Cisco Business Dashboard によって検出および管理されるデバイスを、IP アドレスに基づいて制限できるコントロール機能。

ネットワークビューパネルについて

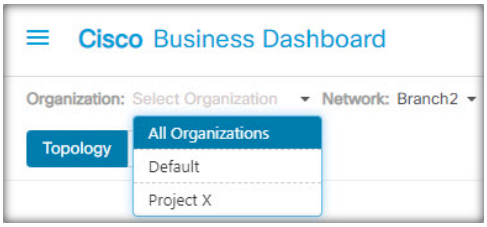
このパネルを開いて、ネットワークに関する詳細を表示および管理します。

ネットワークの [Basic Info] パネルで [Manage] をクリックして、そのネットワークの [Network View] を複数のビューで表示します。

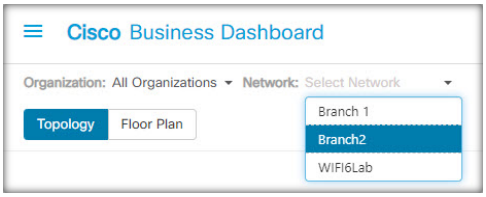
ネットワークで検出されたすべてのデバイスの論理トポロジを表示するには、[Topology] を選択します。各デバイスについての情報が表示され、選択したシスコ製品に対して操作を行うことができます。

[Floor Plan] を選択し、環境内のネットワークデバイスの物理的な場所を文書化して表示します。

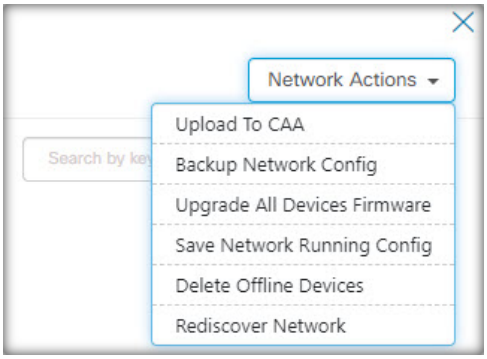
[Organization] ドロップダウンリストから選択し、メインネットワークページに戻らずに組織を切り替えます。



[Network] ドロップダウンリストから選択して、メインネットワークページに戻らずにネットワークを切り替えます。



[Network Actions] ドロップダウンリストを使用して、そのアクションをサポートするネットワーク内のすべてのデバイスで実行できるアクションを選択します。たとえば、1 回のクリックですべてのネットワークデバイスの設定をバックアップできます。



また、[Network Actions] ドロップダウンメニューでは、ネットワークに対する検出プロセスの再開や、Cisco Active Advisor（Cisco Active Advisor）へのインベントリのアップロードも実行できます。

トポロジ マップとツールの概要

トポロジ マップについて

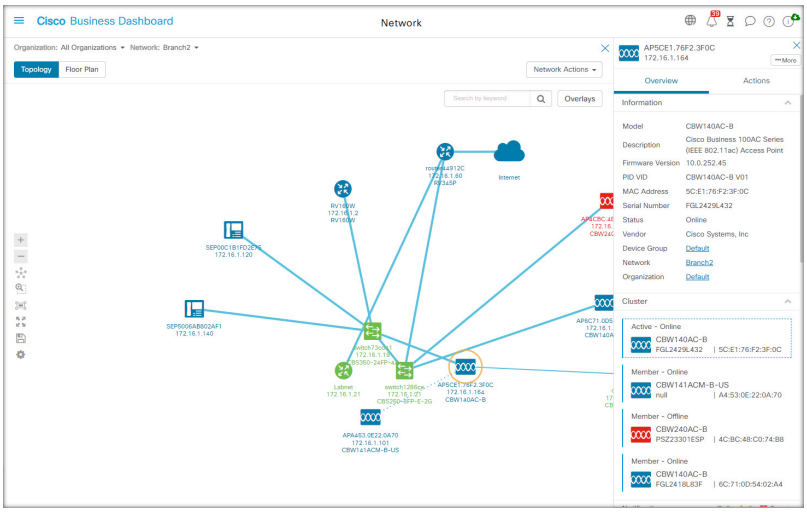
Cisco Business ダッシュボード は、検出されたデバイスにネットワーク接続の詳細を問い合わせ、収集した情報からグラフィカルな表示またはトポロジを作成します。収集されるデータは次のとおりです。

- CDP & LLDP ネイバー情報
- MAC アドレステーブル
- Cisco Business スイッチの関連デバイステーブル
- ルータ
- ワイヤレス アクセス ポイント

この情報を使用して、ネットワークがどのように構成されているかを判定します。何らかの理由で管理できないネットワーク インフラストラクチャ デバイスがネットワークに含まれている場合、Cisco Business ダッシュボード は収集可能な情報に基づいてトポロジを推論しようと試みます。

トポロジ内のデバイスまたはリンクをクリックすると、そのデバイスまたはリンクの [Basic Info] パネルが表示されます。このパネルには、デバイスまたはリンクに関するより詳細な情報が表示され、デバイスに対してさまざまな操作を行うことができます。

[Topology Map] マップで [Overlays] をクリックすると [Overlays & Filters] パネルが表示されます。このパネルでは、トポロジに表示されるデバイスを、デバイスの種類またはタグによって制限できます。また、リンク上のトラフィック負荷や特定の VLAN がネットワーク上でどのように設定されているかなど、追加情報を表示するようにトポロジを拡張できます。



トポロジ マップへのアクセス

[Topology Map] にアクセスするには、次を実行します。

1. [Navigation] ペインから [Network] パネルを開きます。
2. 関心のあるネットワークのアイコンまたは表の行をクリックします。

そのネットワークの [Topology] が作業ペインに表示されます。

トポロジ コントロール

トポロジコントロールは、[Topology Map] の左にあります。

アイコン	説明
	[Zoom in]：[Topology] ウィンドウのビューを調整します。表示エリアでネットワークのサイズを拡大するには、メニューバーの✚（プラス）アイコンをクリックします。
	[Zoom out]：[Topology] ウィンドウのビューを調整します。表示エリアでネットワークのサイズを縮小するには、━（マイナス）アイコンをクリックします。
	[Re-layout Topology] をクリックし、手動で変更してトポロジを無効にした後、トポロジの自動レイアウトを再度有効にします。自動レイアウト アルゴリズムを使用してトポロジを再描画します。
	[Zoom by selection] をクリックし、ドラッグして、拡大する領域を選択します。
	[Fit stage] をクリックして、ネットワーク全体が表示領域に収まるようにズームします。
	[Enter full screen mode] をクリックして、画面全体に Cisco Business ダッシュボード ユーザーインターフェイスを表示します。
	[Export Topology] をクリックして、現在のトポロジビューを PNG 形式の画像としてエクスポートします。この画像は、ブラウザのデフォルトのダウロード場所に保存されます。
	[Topology Settings] をクリックして、トポロジアイコンに表示されるラベルを調整します。

トポロジのアイコン

次のアイコンが [Topology] ウィンドウに表示されます。

アイコン	説明
	アクセス ポイント
	[Cloud]：Cisco Business ダッシュボードで管理されていないネットワークまたはネットワークの部分を表します。
	[Links]：デバイス間の接続線です。リンクをクリックすると、接続先と接続元のデバイス名と、速度などの基本的な情報が表示されます。 リンクの太さはリンクの速度を表しており、細い線は 100Mbps 以下、太い線は 1Gbps 以上を表します。破線はワイヤレス接続を表します。
	ルータ
	スイッチ
	[Host]：有線接続でネットワークに接続したホストを表します。
	[Wireless Host]：ワイヤレス接続でネットワークに接続したホストを表します。

[Overlays & Filters] パネル

このパネルは、[Overlays] をクリックすると [Topology] マップの右側に表示されます。トポロジ画面の右上、[Search] ボックスの横にあります。

アイテム	説明
Select Overlay	この機能は、ビューの選択に基づく追加情報で [Topology] マップを拡張します。次のいずれかを指定できます。 • [Link Utilization View] はトラフィック量を監視することで、現在のネットワークパフォーマンスを特定します。このトラフィックは、[Topology] マップ内の色分けされたリンクを使用して表示されます。色分けは、リンクの使用パーセンテージに基づいて変化します。緑は適度に負荷がかかっているリンクを表し、オレンジと赤は容量制限に近づいているリンクを表します。 それぞれの色のしきい値を調整できるコントロールが用意されています。 • [VLAN View] はネットワーク内で VLAN が有効になっている場所を表示します。これは、分割された VLAN などの設定ミスを特定するために使用できます。 [Overlay] ドロップダウンで [VLAN View] を選択すると、第 2 のドロップダウンボックスがこのフィールドの下に表示され、表示する VLAN ID を選択できます。 • [POE View] はトポロジマップ内のリンクを強調表示し、POE が有効になっているスイッチから現在電力を供給されているデバイスを示します。 • [L2 Path Trace] は選択された 2 つのデバイス間のレイヤ 2 パストラフィックがネットワークを通過することを示します。表示されたフィールドにホスト名、MAC アドレス、または IP アドレスを入力してデバイスを選択するか、トポロジマップで 2 つのデバイスを Shift キーを押しながらクリックします。
Select Tag	[Select Tag] の下のテキストボックスで [Device Tag] を指定してトポロジをフィルタ処理し、指定したタグに一致するデバイスを表示します。デバイスタグは、[Detailed Info] パネルに割り当てられます。
Show only: • **Routers** • **Switches** • **Wireless** • **Unmanaged Networks** • **Hosts** • **Others**	[Topology] マップに表示するデバイスのチェックボックスをリスト内でオンにします。この機能は、マップに表示するデバイスをフィルタリングするのに役立ち、デバイスリストでオンになっていないデバイスを削除します。

アイテム	説明
Show Discovery: • **Both** • **Blocked** • **Enabled**	オプションボタンを使用して、管理用にブロックされている、ダッシュボードによって検出されたデバイスを表示するかどうかを制御します。

基本的なデバイス情報の表示

ネットワークやルータなどのネットワークデバイスか、2つのデバイスを接続しているリンクをクリックすると、未確認の通知や実行可能なアクションなど、デバイスに関する基本情報が表示されます。

[Basic Info] パネルでは、デバイスのより詳細な情報にアクセスしたり、デバイスの管理インターフェイスに直接アクセスすることもできます。

（注） デバイスの詳細情報を表示するには、現在のデバイスの通知の表示とフィルタリング（153ページ）を参照してください。

デバイス管理インターフェイスへのアクセスについての詳細は、デバイス管理インターフェイスへのアクセス（37ページ）を参照してください。

次のセクションの表に、デバイスの表示される詳細の種類を示します。基本的なデバイス情報を表示するには、以下の手順に従います。

ステップ1 [Network] ページでネットワークを選択し、[Manage] をクリックしてトポロジを表示します。

ステップ2 トポロジマップで、スイッチやルータなどのネットワークデバイスをクリックして詳細を表示します。

ステップ3 [Basic Info] パネルの [Overview] タブの下に、デバイスの詳細が表示されます。これらの各項目について次の表で説明します。

[Information]パネル	
Model	デバイスのモデル名。
Description	デバイスまたは製品の説明。
Firmware Version	デバイスのファームウェア バージョン。
PID VID	製品 ID とバージョン ID。

MAC Address	Media Access Control（MAC）アドレスは、標準化されたデータ リンク レイヤ アドレスであり、特定のネットワークインターフェイスタイプで必要です。これらのアドレスはデバイスごとに固有かつ一意であり、ネットワーク内の他のデバイスでは使用されません。
Serial Number	デバイスのシリアル番号。
Status	デバイスのオンライン/オフライン ステータス。
Domain	デバイスのドメイン名。
Vendor	デバイスのメーカー。
Network	デバイスがあるネットワークの名前。
Organization	デバイスが属する組織。

[Notification]パネル	[Notifications] パネル ヘッダー：[Notifications] パネルのヘッダーには、デバイスの未確認の通知の集計が表示されます。 [Notifications] パネル本文：[Notifications] パネルの本文にデバイスの未確認の通知がリストされます。すべてのデバイス通知の完全なリストを表示およびフィルタリングするには、現在のデバイスの通知の表示とフィルタリング （153 ページ）を参照してください。通知を確認し、通知の一覧から削除するには、通知のチェックボックスをオンにします。必要であれば、通知フィルタリングを使用して、確認済みの通知を表示できます。
[Events] パネル	[イベント] パネルには、すべての通知と過去 24 時間に発生したその他のイベントがリストされます。すべてのデバイスのすべてのイベントの完全なリストを表示してフィルタリングするには、[Event Log] にアクセスします。
[POE] パネル	[POE] パネルは POE 対応のスイッチに表示され、デバイス内の各ポートの電力使用量の概要が提供されます。
[Stack Information] パネル	[Stack Information] パネルは、スイッチ スタックが表示され、モデル情報、シリアル番号、および MAC アドレスなどスタックの各メンバーのハードウェアの詳細が表示されます。
[Service] パネル	デバイス上で識別されたネットワークサービスのリストが表示されます。
[Connected Device] パネル	ホストデバイスには、[Connected Device] パネルが含まれます。このパネルにはネットワークへのホストの接続方法が表示され、アップストリーム ネットワーク デバイスと、該当する場合は、ホストが接続されているポートのリストが表示されます。

[Overview] タブに加え、[Basic Info] パネルにも [Actions] タブが表示され、デバイスでさまざまな操作タスクを実行することができます。詳細については、デバイス アクションの実行 （35 ページ）を参照してください。

デバイス アクションの実行

ネットワーク内のデバイスで、ファームウェアの更新、構成のバックアップと復元、再起動などのアクションを簡単に実行できます。これらのアクションを実行するには、以下の手順を実行します。

ステップ 1 [Topology Map] ページまたは [Inventory] ページで、スイッチやルータなどのネットワークデバイスをクリックします。

ステップ 2 [Basic Info] パネルで、[Actions] タブを選択します。デバイスの機能に応じて、以下のアクションが 1 つ以上表示されます。

Update firmware to latest	デバイスに最新のファームウェアの更新を適用できます。Cisco Business ダッシュボード はシスコから更新をダウンロードし、デバイスにアップロードします。更新の完了時にデバイスはリブートします。
Upgrade From Local	ローカルドライブからファームウェア アップグレード ファイルをアップロードできます。Cisco Business ダッシュボード がファイルをデバイスにアップロードし、更新の完了時にデバイスが再起動します。
Backup Configuration	現在のデバイス設定のコピーを Dashboard に保存できます。 **1.** [Backup Configuration] をクリックします。 **2.** [Backup Configuration] ウィンドウでは、実行するバックアップについてのメモを必要に応じてテキストボックスに追加できます。 （注） このメモは、バックアップが GUI で一覧表示されるときに必ず表示されます。 **3.** [Save Backup] をクリックしてこのアクションを完了するか、続行しない場合は [Cancel] をクリックします。 バックアップ設定ジョブが作成されます。このジョブは [Task Center] に表示される場合があります。

Restore Configuration	以前バックアップした設定をデバイスに復元できます。 [Restore Configuration] をクリックします。 次のバックアップ設定オプションが用意されています。 • [Backups for device name]：特定のデバイスを設定するために使用可能なすべてのバックアップが一覧表示されます • [Backup for other device]：同じ種類または同じ製品 ID の他のデバイスを設定するために使用可能なすべてのバックアップが一覧表示されます • [Backup for other compatible device]：選択したデバイスと互換性がある、シリーズ内の他のデバイスを設定するために使用可能なすべてのバックアップが一覧表示されます バックアップ設定を行うには、以下の手順を実行します。 **1.** [Restore Configuration] ウィンドウで、デバイスに復元するバックアップを選択します。 スクロール バーを使用して使用可能なすべてのバックアップを参照し、対応するオプション ボタンをクリックします。これにより、[Restore Configuration] ボタンが有効になります。 また、設定ファイルをアップロードすることもできます。これを実行するには、設定ファイルをターゲット領域にドラッグアンドドロップするか、またはターゲット領域をクリックしてファイルシステムからファイルを選択します。 **2.** [Restore Configuration] をクリックしてこのアクションを完了します。 復元設定ジョブが作成されます。このジョブは [Task Center] に表示される場合があります。
Reboot	デバイスを再起動します。 このボタンをクリックすると、確認のために再度クリックするよう求められます。
Save Running Configuration	個別の実行コンフィギュレーションとスタートアップ コンフィギュレーションをサポートしているデバイスの場合、このアクションは現在の実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。これにより、デバイスを次回利グーとしたときに、設定変更が保持されます。
Delete	トポロジとインベントリからオフラインのデバイスを削除します。

ステップ 3 オプションで、デバイスアクションを後で実行するようにスケジュールできます。デバイスアクションをスケジュールするには、[Schedule] ボタンをクリックし、フォームに入力して新しい [Schedule Profile] を作

成します。スケジューリングプロファイルの詳細については、スケジュールプロファイルの管理（159ページ） を参照してください。

デバイス管理インターフェイスへのアクセス

状況によっては、ネットワークデバイスの管理インターフェイスに直接アクセスすることが必要な場合があります。管理インターフェイスにアクセスするには、以下の手順を実行します。

ステップ 1 [Topology] ページまたは [Inventory] ページで、管理インターフェイスにアクセスする必要があるスイッチやルータなどのネットワーク デバイスをクリックします。

ステップ 2 [Basic Info] パネルで、右上隅にある [View] をクリックします。ブラウザ内に新しいウィンドウが開き、デバイス管理インターフェイスが表示されます。

（注） [View] をクリックして管理インターフェイスにアクセスすると、ブラウザは Dashboard 経由でデバイスに接続します。つまり、ネットワークにリモートでアクセスしている場合、サイトの外から直接到達できるのは Dashboard のみでよいことになります。

これらの接続は同じホスト（Dashboard）を経由するため、あるデバイスの cookie が他のデバイスに提供され、名前が同じ場合は他のデバイスによって更新される可能性があります。一般的な症状として、第 2 のデバイスに接続した直後に、最初のデバイス上のブラウザ セッションがログアウトされます。これは、セッション cookie が更新されたためです。

詳細なデバイス情報の表示

ステップ 1 [Topology] ページまたは [Inventory] ページで、詳細情報を表示するスイッチやルータなどのネットワーク デバイスをクリックします。

ステップ 2 [Basic Info] パネルで、右上隅にある [More] をクリックします。

ステップ 3 [Detailed Info] パネルでは、左側にデバイス情報の詳細リストが表示され、次のタブの下に追加機能が表示されます。

- [Dashboard]：デバイスに固有の一連のダッシュボードウィジェットが表示されます
- [PnP]：デバイスのネットワーク プラグアンドプレイ設定を管理できます。
- [Port Management]：スイッチ ポートの設定を管理できます

  （注） この情報は、スイッチ ポートのあるデバイスでのみ参照できます。

- [Wireless LANs]：ワイヤレス LAN を表示し、デバイスの無線設定を管理できます。

各無線は有効または無効にすることができ、チャネルおよび送信電力はこのタブから制御できます。

（注） この情報は、ワイヤレス デバイスでのみ参照できます。

- [Event Log]：このデバイスの過去のアクションと通知のリストが表示されます
- [Config Backups]：デバイスのバックアップ設定のリストを表示し、設定の復元、保存、削除などのアクションを実行できます

（注） この情報は、バックアップ設定の操作をサポートしているデバイスでのみ参照できます。

- [Pending Config]：定義されている設定プロファイルに基づいた目的の設定と、デバイス上の現在の設定とを比較し、相違点を強調表示します。

（注） このパネルは、現在の設定が目的の設定と一致しない設定動作の場合にサポートされているデバイスに対してのみ表示されます。

これらの各項目について以下の手順で説明します。

ステップ 4 デバイスに関する情報の詳細なリストが左側に表示されます。このリストには、次の情報が含まれています。

項目名	説明
Hostname	デバイスのホスト名を変更するには、デバイス名の横にある [Edit] をクリックします。[Save] をクリックして変更を保存します。
Model	デバイスのモデル名。
MAC Address	Media Access Control（MAC）アドレスは、標準化されたデータ リンク レイヤ アドレスであり、特定のネットワーク インターフェイス タイプで必要です。これらのアドレスはデバイスごとに固有かつ一意であり、ネットワーク内の他のデバイスでは使用されません。
Status	デバイスの現在のステータスを表示します。たとえば、オンラインやオフラインなどです。
Actions	[Actions] ドロップダウンと [Open Device GUI] アイコンを使用すると、[Detailed Info] パネルからデバイスに対して操作できます。
IP	デバイスの IP アドレス。
Domain	デバイスのドメイン名。
PID VID	製品 ID とバージョン ID。
Serial Number	デバイスのシリアル番号。
Vendor	デバイスのメーカー。
Description	デバイスまたは製品の説明。

項目名	説明
Network	このデバイスが属するネットワーク。
Organization	このデバイスが属する組織。
Device Group	デバイスが属するグループを変更するには、デバイスグループの横にある [Edit] をクリックします。 **[Save]**をクリックして、変更内容を保存します。
Monitoring Profile	モニタリングプロファイルの横にある [Edit] をクリックして、このデバイスに使用するモニタリングプロファイルを選択します。または、モニタリングプロファイルは、このデバイスが属するデバイスグループから継承することもできます。 **[Save]**をクリックして、変更内容を保存します。
TAGs	[TAG] フィールドに任意の英数字を入力し、**Enter** キーを押すと、このデバイスの新しいタグが作成されます。既存のタグを削除するには、タグの ✖ をクリックします。[Save] をクリックして変更を保存します。 タグは、共通の特性でデバイスを識別するのに役立ちます。タグを Cisco Business ダッシュボードプローブ の任意の場所に使用して、デバイスのサブセットの表示にネットワークのビューを限定することができます。
Discovery Method	このデバイスが検出されたプロトコルとデバイスを表示します。
Pending Config	デバイス設定のステータスと、デバイスの現在の設定と予期される設定との間に違いがあるかどうかを表示します。

ステップ 5 [Dashboard] をクリックすると、デバイスの現在の状態を示す一連のウィジェットが表示されます。詳細については、「監視ダッシュボードについて」を参照してください。

ステップ 6 [PnP] をクリックして、Network Plug and Playを使用してデバイスに適用される設定を表示します。

ステップ 7 フォームを使用して変更を加え、[Save] をクリックして変更を適用します。

ステップ 8 デバイス上のスイッチ ポートの設定を表示および管理するには、[Port Management] をクリックします。[Port Management] ページに表示されるのと同様の、デバイスの視覚的な表現が表示されます。

このウィンドウに、デバイスのポートの詳細が視覚的に表現されます。デバイスのモデルとシリアル番号がイメージの上に表示され、ポートの表形式のビューが下に表示されます。操作の詳細については、ポート管理について （47 ページ）を参照してください。

ステップ 9 このデバイスで設定されている無線設定を管理し、ワイヤレス LAN を表示するには、[WLAN] をクリックします。

ステップ 10 [Event Log] をクリックして、このデバイスについて記録されている履歴通知と、他のイベントのリストを表示します。フィルタを使用して、表示されるエントリを制限できます。詳細については、イベントログについて （79 ページ）を参照してください。

ステップ 11 このデバイスの設定バックアップを表示および管理するには、[Config Backups] をクリックします。このタブには、Probe に保存されている各バックアップと以下の詳細を一覧表示する表が表示されます。

表 *3 :* 設定のバックアップ

アイテム	説明
Timestamp	コンフィギュレーション バックアップが取得された日付と時刻。
Comment	バックアップを行ったときにユーザによって入力されたメモ。
Backed up by	コンフィギュレーションをバックアップしたユーザ。
Actions	次のいずれかのバックアップ操作を選択します。 • [Restore configuration to device]：選択したバックアップをデバイスに復元します。 • [Save configuration to PC]：バックアップを zip ファイルとして PC 上のローカル ドライブに保存します • [Delete configuration]：バックアップを削除します。 • [View configuration]：設定バックアップの内容をブラウザに表示するのに役立ちます。

また、[Backup Configuration] をクリックすることで、設定バックアップをタブからトリガーすることもできます。

ステップ 12 [Pending Config] をクリックして、現在のデバイス設定と、デバイスに適用された設定プロファイルに基づいて予期される設定との対象比較を表示します。デバイスに依存しない形式で設定が表現され、相違点が強調表示されます。ページ上部のボタンを使用して、未処理の変更を適用したり、現在のデバイス設定を承認したり、現在のデバイス設定を再読み取りしたりできます。

[Floor Plan] の使用方法

[Floor Plan] ビューでは、ネットワーク機器の物理的な位置を追跡できます。建物の各フロアのプランをアップロードし、各ネットワーク デバイスをプラン上に配置できます。これにより、メンテナンスが必要な場合にデバイスの位置を容易に特定できます。フロア プランの操作はトポロジ マップと同様であり、フロア プランに配置したデバイスはトポロジ マップ内のデバイスと同様に操作できます。

新しいフロア プランの作成

1. [Network View] に移動し、[Floor Plan] をクリックします。既存のフロアプランが表示される場合は、フロアプランの左上にある [Home] アイコンをクリックします。
2. フロアプランを追加しようとしている建物がすでに作成されている場合は次のステップに進みます。そうでない場合は、フロアがある建物の名前を [New Building] フィールドに入力します。[保存] アイコンをクリックします。

3. フロア プランが含まれる画像ファイルを新しいフロアのターゲット領域にドラッグ アンドドロップするか、ターゲット領域をクリックしてアップロードするファイルを指定します。サポートされる画像形式は、png、gif、および jpg です。画像ファイルの最大サイズは 500KB です。
4. フロアの名前を [New Floor] フィールドに入力します。[Save] アイコンをクリックします。
5. ネットワークデバイスがある建物とフロアごとに手順 2 ～ 4 を繰り返します。

フロア プラン上のネットワーク デバイスの配置

1. [Network View] に移動し、[Floor Plan] をクリックします。関心があるフロア プランが表示されていない場合は、フロア プランをクリックします。
2. [Add Devices] をクリックし、左下にある検索ボックスを使用して、配置するデバイスを探します。ホスト名、デバイスの種類、またはIPアドレスで検索できます。入力中に、一致するデバイスが検索ボックスの下に表示されます。灰色のアイコンは、フロアプランにすでに追加されているデバイスを表します。
3. デバイスをクリックし、フロアプランの正しい場所にドラッグして追加します。すでに別のフロア プランに配置されているデバイスを選択すると、削除されてこのフロア プランに追加されます。
4. すべてのデバイスをフロア プランに追加するまでステップ 2 および 3 を繰り返します。

フロア プランからのデバイスの削除

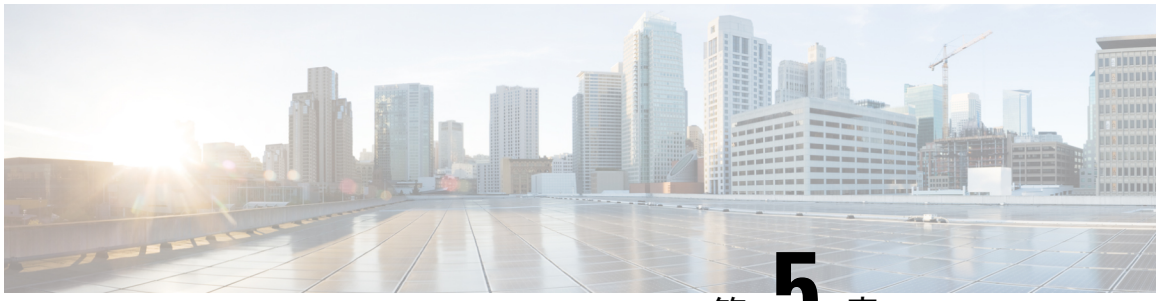
1. [Network View] に移動し、[Floor Plan] をクリックします。関心があるフロア プランが表示されていない場合は、フロア プランをクリックします。
2. 削除するデバイスを特定し、クリックして選択します。
3. 表示される赤い×印をクリックして、フロア プランからデバイスを削除します。

フロア プランの変更

1. [Network View] に移動し、[Floor Plan] をクリックします。既存のフロアプランが表示される場合は、フロアプランの左上にある [Home] アイコンをクリックします。
2. 建物の名前を変更するには、名前の横の [Edit] アイコンをクリックします。変更が完了したら、[Save] アイコンをクリックします。
3. フロア プランを変更するには、フロア プラン名の横の [Edit] アイコンをクリックします。新しい画像ファイルをターゲット領域にドラッグするか、ターゲット領域をクリックして新しいファイルを PC からアップロードすることにより、フロア プランを変更できます。また、フロア プランの名前を変更することもできます。変更が完了したら、[Save] アイコンをクリックします。

フロア プランの削除

1. [Network View] に移動し、[Floor Plan] をクリックします。既存のフロアプランが表示される場合は、フロアプランの左上にある [Home] アイコンをクリックします。
2. 削除するフロアプランを特定し、イメージのターゲット領域の右上隅にある [Delete] アイコンをクリックします。
3. すべてのフロア プランを含む建物全体を削除する場合は、建物の名前の横にある [Delete] アイコンをクリックします。



第 5 章

インベントリ

デバイス インベントリの表示

このページにアクセスして、ネットワーク内のすべてのデバイスとインベントリを表示、監視、およびサポートします。[Inventory] ページには、デバイスの完全なリストとその詳細が表形式で表示されます。さらに、設定タスクを実行したり、サポート対象のデバイス用の最新のファームウェアアップデートを適用したりするためのアクションボタンも提供されています。以下の表に、表示される情報の詳細を示します。

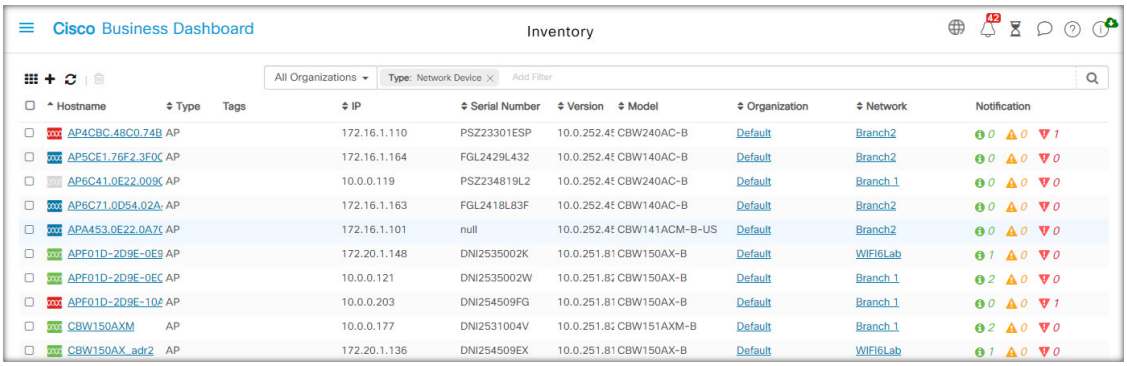


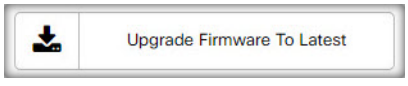
表 *4*:インベントリの詳細

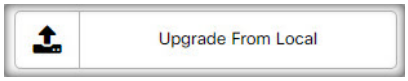
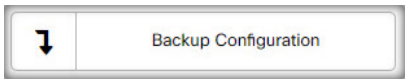
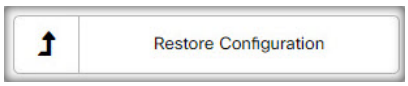
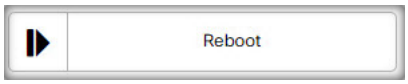
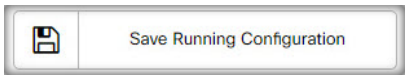
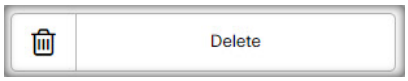
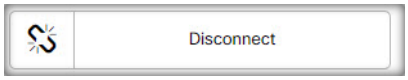
項目	説明
Hostname	デバイス名を表示します。
Type	デバイスの種類（スイッチ、ルータ、ワイヤレス アクセス ポイント（WAP）など）。
Tags	デバイスに関連付けられているタグのリストが表示されます。
IP	デバイスの Internet Protocol（IP）アドレス。

項目	説明
MAC（デフォルトでは非表示）	Media Access Control（MAC）アドレスは、標準化されたデータ リンク レイヤ アドレスであり、特定のネットワーク インターフェイス タイプで必要です。これらのアドレスはデバイスごとに固有かつ一意であり、ネットワーク内の他のデバイスでは使用されません。
Serial Number	デバイスのシリアル番号。
Version	デバイスの現在のファームウェア バージョン。
Vendor（デフォルトでは非表示）	デバイスを製造したベンダー。
Model	デバイスのモデル名。
Organization	デバイスが属する組織。
Network	デバイスが属するネットワーク。
Notification	デバイスの未処理通知の数
PnP Status（デフォルトでは非表示）	デバイスの現在のネットワーク プラグアンドプレイ ステータス。詳細については、「**ネットワーク プラグアンドプレイ**」のページを参照してください。

[Inventory] ページでは、次の追加のコントロールを使用できます。

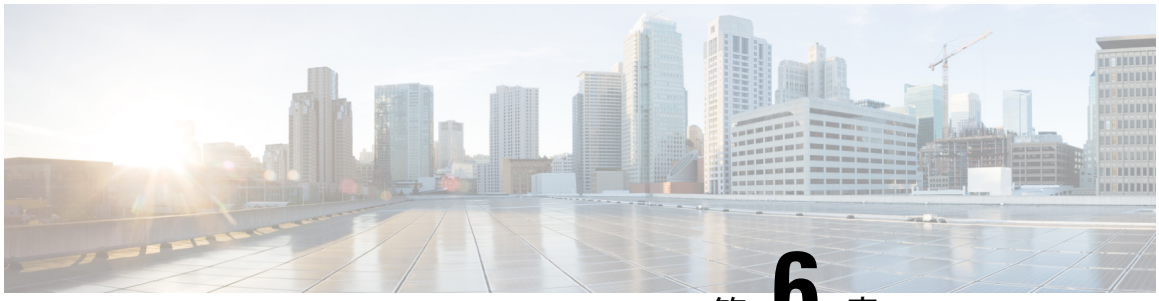
- [Select columns] ボタン：テーブルの左上にあるこのボタンを使用して、表示する列を選択します。
- [Filter Box] ：[Filter Box] を使用してデバイス名、デバイスタイプ、シリアル番号などを入力し、表示を制限することができます。デフォルトでは、インベントリはネットワークデバイスのみを表示するようにフィルタ処理されます。
- [Add] アイコン：デバイスが検出される前に、[+] アイコンをクリックして新しいデバイスをインベントリに追加します。インベントリにデバイスを手動で追加する場合は、アイデンティティ情報、組織とデバイス グループ、PnP 設定など、デバイスに関する基本情報を指定できます。この情報を事前に提供することで、ネットワークに接続するときにデバイスを正しく管理できるようにします。
- [Refresh] ボタン：このボタンをクリックしてテーブルを更新し、使用可能な最新情報を表示します。
- [Actions] ボタン：次のアクション ボタンを使用すると、選択した 1 台以上のデバイスでアクションを実行できます。

	**Upgrade Firmware To Latest**

	**Upgrade From Local**
	**Backup Configuration**
	**Restore Configuration**
	**Reboot**
	**Save Running Configuration**
	**Delete**
	**Disconnect**

アクションボタンは、アクションをサポートする 1 台以上のデバイスが選択されている場合にのみ表示されます。

（注） アクションの詳細については、19 ページの「デバイス アクションの実行」を参照してください。



第 6 章

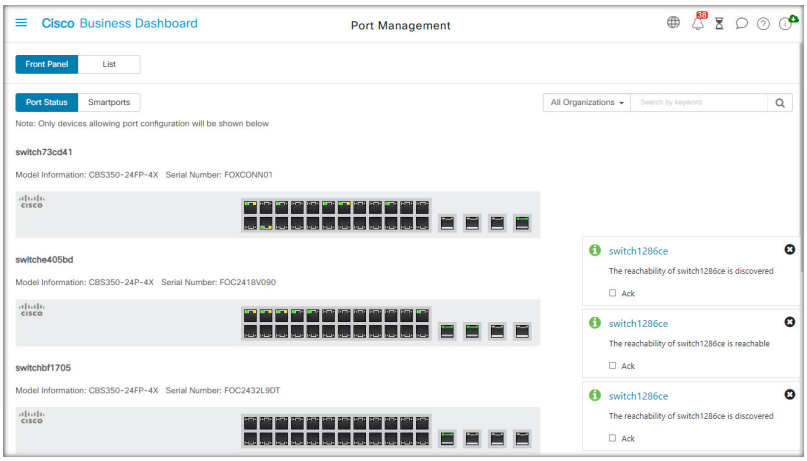
ポート管理

ポート管理について

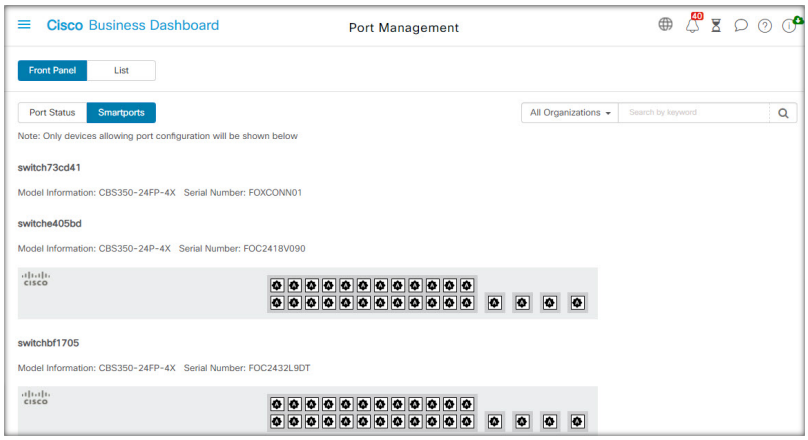
[Port Management] は、Cisco Business ダッシュボードによって設定可能なスイッチポートを含む各デバイスの前面パネルビューとして利用できます。このページでは、トラフィックカウンタなどのポートのステータスを参照したり、ポートの設定を変更することができます。また、このページでは、Smartport をサポートするデバイス上のポートについて、Smartport ロールを表示および設定することもできます。検索ボックスを使用して表示するデバイスを制限できます。デバイス名、製品 ID、シリアル番号の全部または一部を入力して、目的のデバイスを探します。

同じ情報のリストビューも提供され、すべてのスイッチポートを表形式で表示します。**ポート管理**の前面パネルビューには、デバイスについての次の 2 つの異なるビューが表示されます。

[Physical] ビューでは、物理レイヤでポートのステータスを確認したり、設定を変更したりできます。速度、デュプレックス、Energy Efficient Ethernet（EEE）、Power over Ethernet（PoE）、および VLAN の設定を表示または変更できます。各ポートは、リンクを示す緑色の LED と、接続されているデバイスに電力が供給されていることを示す黄色の LED とともに表示されます。

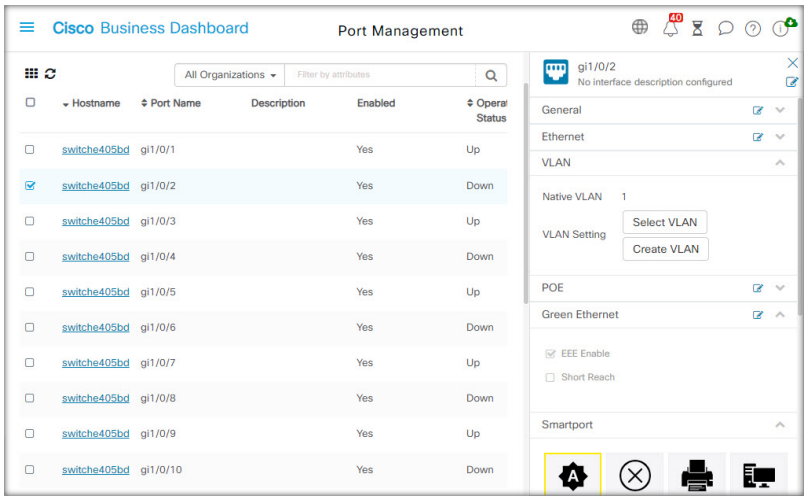


[Smartport] ビューでは、各ポートの現在の Smartport ロールを表示したり、ロールを変更したりできます。各ポートには、現在のロールを示すアイコンがオーバーレイ表示されます。



（注） [Smartport] は、組み込み（またはユーザー定義）テンプレートを適用できるインターフェイスです。これらのテンプレートは、デバイスで通信要件をサポートするための設定作業を省力化するとともに、さまざまなタイプのネットワークデバイスの機能を活用できるようにするための手段として設計されています。

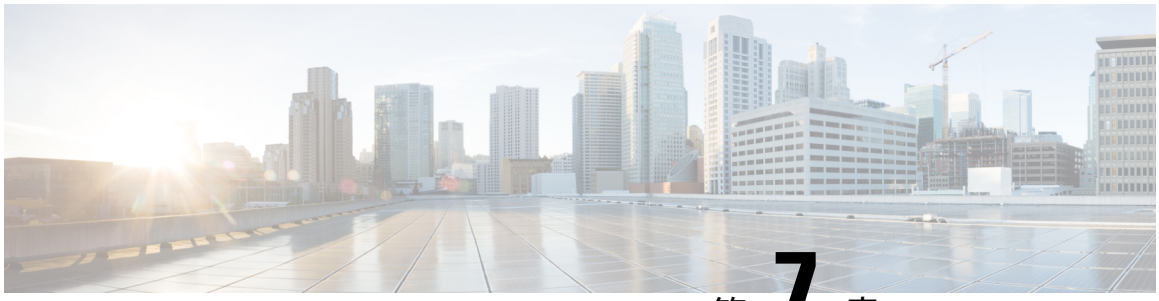
ポートのステータスを表示するには、前面パネルビューまたはリストビューのいずれかでポートをクリックします。ポートの [Basic Info] パネルが表示され、次のような一連のパネルが表示されます。



General	このパネルにはポートの物理レイヤのステータスが表示され、このパネルを使用してポートを有効または無効にすることができます
Ethernet	このパネルを使用して、速度とデュプレックス設定を制御します

Port Authentication	このパネルを使用すると、このポートの 802.1x ポート認証を有効にすることができます。認証は、デバイスに割り当てられた認証プロファイルで指定された認証サーバーに対して実行されます。 認証サーバーが定義されていない場合、Cisco Business Dashboard がデフォルトの認証サーバーとして使用されます。
VLAN	このパネルには、ポートに現在設定されている VLAN が表示されます。[Select VLAN] または [Create VLAN] ボタンをクリックして、この設定を変更します。
POE	このパネルは、POE 対応ポートの場合のみ表示され、ポートの POE 設定を設定することができます。[Toggle Power] ボタンをクリックして、接続している POE デバイスの電源を入れ直すこともできます
Green Ethernet	このパネルでは、ポートの Energy Efficient Ethernet（EEE）設定を管理できます
Smartports	このパネルには、ポートで利用可能な Smartports のロールが表示されます。ロールをクリックしてポートに設定を適用します。現在設定されているロールが強調表示されます。

ポートの設定を変更するには、その設定を含むペインの右上にある [edit] アイコンをクリックします。変更を加えたら、[Save] アイコンをクリックします。



第 7 章

ネットワーク設定

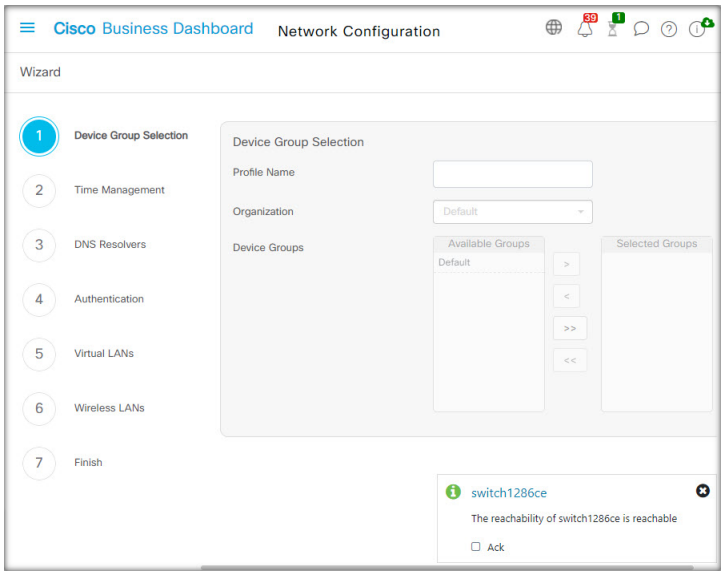
この章は、次の項で構成されています。

ネットワーク設定について

[Network Configuration] ページでは、通常、ネットワーク内の一部またはすべてのデバイスに適用されるさまざまな設定パラメータを定義できます。これらのパラメータには、時刻設定、ドメイン名サービス、管理者の認証、仮想 LAN およびワイヤレス LAN などの設定が含まれています。これら各分野の設定プロファイルを個別に作成できます。また、ウィザードを使用して、各分野のプロファイルを 1 つのワークフローで作成することもできます。設定プロファイルは 1 つ以上のデバイスグループに適用された後、デバイスにプッシュされます。

ウィザードの使用方法

ウィザードを使用すると、ネットワーク設定の要素ごとに設定プロファイルを作成し、それらのプロファイルを 1 つ以上のデバイスグループに 1 つのワークフローで割り当てることができます。



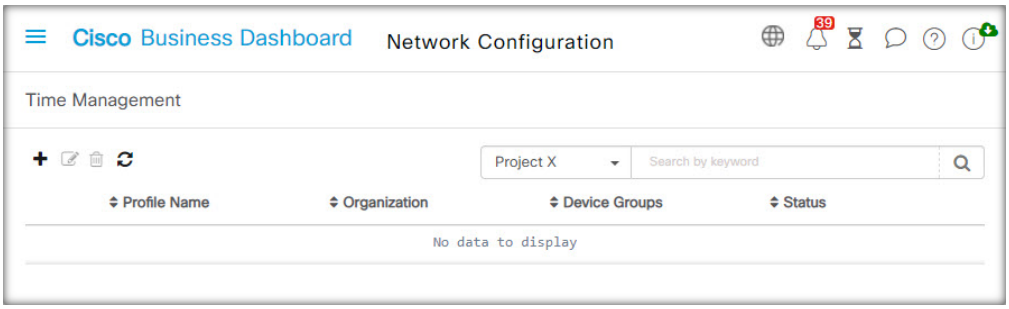
1. **[Network Configuration]** > **[Wizard]** に移動します。
2. [Device Group Selection] 画面で、この設定のプロファイル名を入力し、組織を選択し、設定する 1 つ以上のデバイス グループを選択します。
3. [Next] をクリックします。

   以降の各画面で、必要に応じて設定を選択します。これらのパラメータの詳細については、以降のセクションを参照してください。
4. 各画面で設定を行い、[Next] をクリックします。

   このプロファイルの特定の画面で設定を行わない場合は、[Skip] をクリックします。
5. 前の画面に戻る場合は、[Back] をクリックするか、左側の見出しをクリックします。
6. 設定を完了し、最終画面で設定を確認します。[Finish] をクリックして、選択したデバイスに設定を適用します。

時刻管理の設定

[Time Management] ページでは、ネットワークのタイムゾーン、夏時間、NTP サーバを設定できます。以下のセクションでは、時刻設定プロファイルを作成、変更、削除するための手順を示します。



時刻管理設定プロファイルを作成

1. **[Network Configuration]** > **[Time Management]** に移動します。
2. ✚（プラス）アイコンをクリックして新しいプロファイルを追加します。
3. [Device Group Selection] セクションで、この設定のプロファイル名を入力し、組織を選択し、設定する 1 つ以上のデバイスグループを選択します。
4. [Time Setting] セクションで、ドロップダウン リストから適切なタイムゾーンを選択します。
5. 必要に応じて [Daylight Saving] を有効にします。そのためには、チェックボックスをオンにし、夏時間調整用のパラメータをフィールドに入力します。固定の日付か繰り返しパターンを指定できます。また、使用するオフセットを指定することもできます。
6. 必要に応じて、Network Time Protocol（NTP）を有効にします。そのためには、時刻同期の [Use NTP] セクションで、チェックボックスをオンにします。ボックスに、1 つ以上の NTP サーバ アドレスを指定します。
7. [Save] をクリックします。

時刻管理設定プロファイルを変更

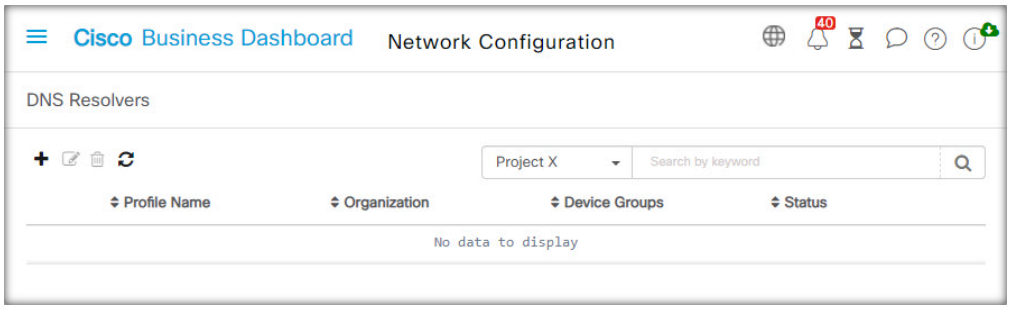
1. 変更するプロファイルの横にあるオプション ボタンを選択し、[Edit] アイコンをクリックします。
2. プロファイル設定に必要な変更を加え、[Update] をクリックします。

時刻管理設定プロファイルを削除

1. 削除する必要があるプロファイルの横にあるオプション ボタンを選択します。
2. [Delete] アイコンをクリックします。

DNS リゾルバの設定

[DNS Resolvers] ページでは、ネットワークのドメイン名とドメイン名サーバを設定できます。以下のセクションでは、DNS リゾルバ設定プロファイルを作成、変更、削除するための手順を示します。



DNS リゾルバ設定プロファイルを作成

1. **[Network Configuration]** > **[DNS Resolvers]** に移動します。
2. ✚（プラス）アイコンをクリックして新しいプロファイルを追加します。
3. [Device Group Selection] セクションで、この設定のプロファイル名を入力し、組織を選択し、設定する 1 つ以上のデバイスグループを選択します。
4. ネットワークのドメイン名を指定します。
5. 1 つ以上の DNS サーバ アドレスを指定します。
6. [Save] をクリックします。

DNS リゾルバ設定プロファイルを変更

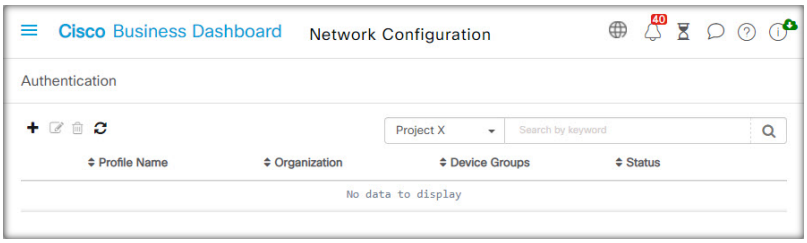
1. 変更するプロファイルの横にあるオプション ボタンを選択し、[Edit] アイコンをクリックします。
2. プロファイル設定に必要な変更を加え、[Update] をクリックします。

DNS リゾルバ設定プロファイルを削除

1. 削除するプロファイルの横にあるオプション ボタンを選択します。
2. [Delete] アイコンをクリックします。

認証の設定

[Authentication] ページでは、ネットワークデバイスへの管理ユーザーアクセスを設定し、ユーザーに基づいてネットワークアクセスを認証するときに使用する認証サーバー（RADIUS サーバー）を設定できます。以下のセクションでは、認証設定プロファイルを作成、変更、削除するための手順を示します。



認証設定プロファイルを作成

1. **[Network Configuration]** > **[Authentication]** に移動します。
2. ✚（プラス）アイコンをクリックして新しいプロファイルを追加します。
3. [Device Group Selection] セクションで、この設定のプロファイル名を入力し、組織を選択し、設定する 1 つ以上のデバイスグループを選択します。
4. オプションで、ローカルユーザー認証用に 1 つ以上のユーザー名とパスワードの組み合わせを指定します。✚（プラス）アイコンをクリックすることでユーザを追加できます。
5. 複雑なパスワードの使用を義務付けることも選択できます。
6. オプションで、認証に使用する 1 つ以上の RADIUS サーバーを指定します。チェックボックスをオンにすると、Cisco Business Dashboard の認証への使用を有効にすることができます。
7. [Save] をクリックします。

（注） ネットワークアクセスを必要とするユーザーには、ネットワークアクセス権限を付与する必要があります。詳細については、「ユーザー（101 ページ）」を参照してください。

（注） ネットワークアクセス認証に Cisco Business Dashboard を使用する場合は、ダッシュボードにおいて公的認証局による署名付きの証明書が取得されていることを強くお勧めします。これを行わないと、ほとんどのクライアントデバイスでユーザーに対して証明書の警告が表示され、一部のクライアントでは認証処理が一切続行されません。

認証設定プロファイルを変更

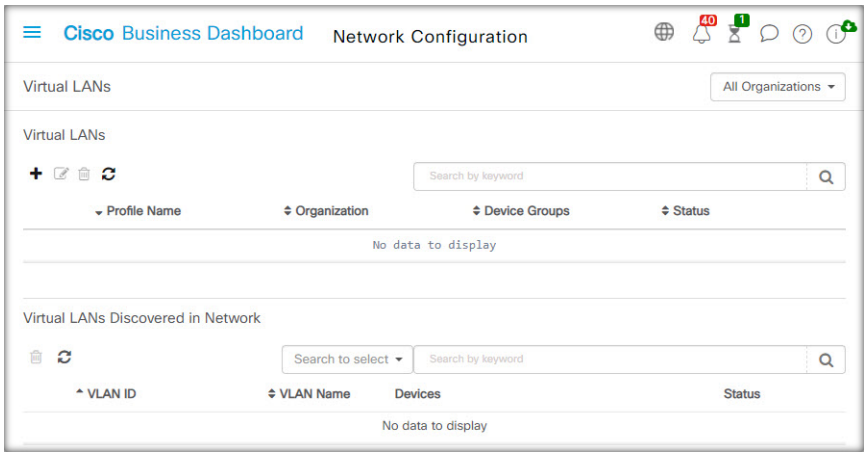
1. 変更するプロファイルの横にあるオプション ボタンを選択し、[Edit] アイコンをクリックします。
2. プロファイル設定に必要な変更を加え、[Update] をクリックします。

認証設定プロファイルを削除

1. 削除する必要があるプロファイルの横にあるオプション ボタンを選択します。
2. [Delete] アイコンをクリックします。

仮想 LAN の設定

[Virtual LANs] ページでは、スイッチネットワークを複数の仮想ネットワーク（VLAN）に分割できます。Cisco Business ダッシュボード で設定されなかったネットワーク内の既存の VLAN も、このページの別のテーブルに表示されます。以降のセクションでは、仮想 LAN 設定プロファイルを作成、変更、削除するための手順を示します。



仮想 LAN を作成

1. **[Network Configuration]** > **[Virtual LANs]** に移動します。
2. ✚（プラス）アイコンをクリックして新しい VLAN を追加します。
3. [Device Group Selection] セクションで、この設定のプロファイル名を入力し、組織を選択し、設定する 1 つ以上のデバイスグループを選択します。
4. VLAN のわかりやすい名前と、使用する VLAN ID を指定します。VLAN ID は 1 ～ 4094 の範囲内の数値である必要があります。
5. 1 つのプロファイルを使用して複数の VLAN を作成できます。このプロファイル内に追加の VLAN を作成する場合は、[Add Another] をクリックし、手順 4 に戻ります。

6. [Save] をクリックします。新しい VLAN が、選択したグループ内のすべての VLAN 対応デバイスで作成されます。

新たに作成した VLAN の VLAN ID が、デバイスグループ内のデバイスにすでに存在する既存の VLAN と一致する場合、その VLAN は Cisco Business ダッシュボード によって採用され、検出された仮想 LAN テーブルから削除されます。

VLAN を変更

1. 変更する VLAN の横にあるオプションボタンを選択し、[Edit] アイコンをクリックします。
2. VLAN の設定に必要な変更を加え、[Update] をクリックします。

VLAN を削除

削除する VLAN の横にあるオプションボタンを選択し、[Delete] アイコンをクリックします。

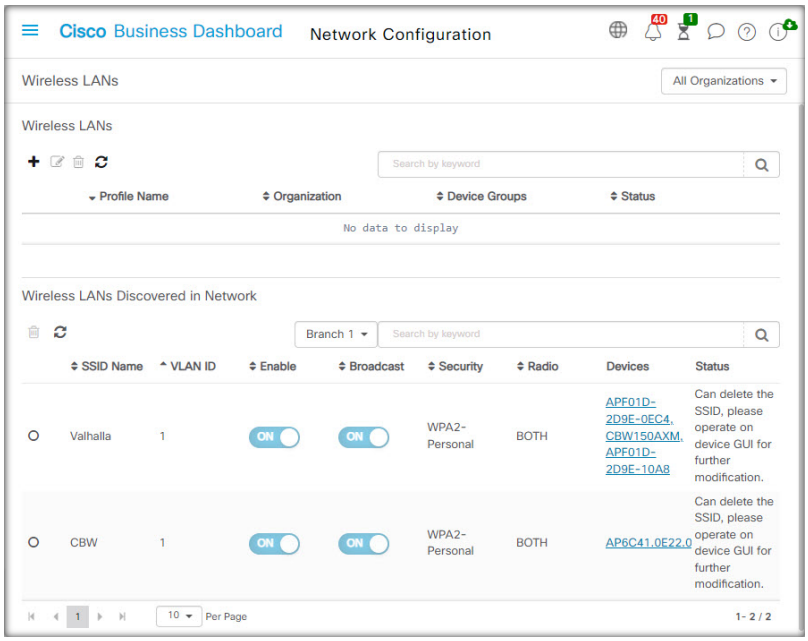
Cisco Business ダッシュボード によって作成されていない VLAN を削除

検出された VLAN の表で、削除する 1 つ以上の VLAN の横の [Delete] アイコンをクリックします。

（注） VLAN 1 は削除できません。

ワイヤレス LAN の設定

[Wireless LANs] ページでは、環境内のワイヤレスネットワークを管理できます。ネットワーク内の、Cisco Business ダッシュボード で設定されていない既存のワイヤレス LAN も個別の表に表示されます。以降のセクションで、ワイヤレス LAN 設定プロファイルを作成、変更、削除するための手順について説明します。



ワイヤレス LAN を作成

1. [Network Configuration] > [Wireless LANs] に移動します。
2. ✚（プラス）アイコンをクリックして新しいワイヤレス LAN プロファイルを追加します。
3. [Device Group Selection] セクションで、プロファイル名を入力し、組織を選択し、設定する 1 つ以上のデバイスグループを選択します。
4. ✚（プラス）アイコンをクリックして新しい SSID を追加します。
5. ワイヤレス LAN の SSID 名と、関連付けが必要な VLAN ID を指定します。VLAN ID は 1 ～ 4095 の範囲の数値である必要があります。ネットワーク内にすでに存在していなければ、新しい VLAN が自動的に作成されます。
6. 必要なセキュリティのタイプを選択します。

   セキュリティタイプとして [Guest] を選択した場合は、ゲストポータルで使用する認証のタイプを指定する必要があります。ユーザー名/パスワード、Web での同意、電子メールアドレスなどのオプションがあります。これらのオプションの詳細については、ゲストポータルの設定 （60 ページ）を参照してください。

   [Enterprise] セキュリティタイプを選択した場合は、使用する優先 RADIUS サーバーを含むデバイスに認証プロファイルを割り当てるようにしてください。このデバイスに対して定義されているものがない場合、Cisco Business Dashboard がデフォルトで使用されます。
7. 必要に応じて [Advanced Settings] をクリックして展開し、[Broadcast]、[Application Visibility]、[Local Profiling]、および [Radio] の設定を要件に合わせて変更します。

8. [Save] をクリックして続行するか、[Cancel] をクリックして変更を破棄します。
9. 1 つのプロファイルを使用して複数のワイヤレス LAN を作成できます。このプロファイルで追加のワイヤレス LAN を作成する場合は、手順 4 に戻ります。
10. [Save] をクリックします。新しい WLAN が、選択したグループ内のワイヤレス アクセス ポイント機能を持つすべてのデバイスで作成されます。

新たに作成したプロファイルのワイヤレス LAN 設定が、デバイスグループ内のデバイスにすでに存在する既存のワイヤレス LAN と一致する場合、そのワイヤレス LAN が Cisco Business ダッシュボード によって採用され、検出されたワイヤレス LAN のテーブルから削除されます。

ワイヤレス LAN を変更

1. 変更するワイヤレス LAN の横にあるオプションボタンを選択し、[Edit] アイコンをクリックします。
2. ワイヤレス LAN の設定に必要な変更を加え、[Update] をクリックします。

ワイヤレス LAN を削除

削除するワイヤレス LAN の横にあるオプションボタンを選択し、[Delete] アイコンをクリックします。

（注） ワイヤレス LAN の作成時に仮想 LAN が自動的に作成された場合、ワイヤレス LAN が削除されても仮想 LAN は削除されません。仮想 LAN は [Virtual LANs] ページで削除できます。

Cisco Business ダッシュボード で作成されていないワイヤレス VLAN を削除

検出されたワイヤレス LAN のテーブルで、削除するワイヤレス LAN のオプション ボタンをクリックし、[Delete] アイコンをクリックします。場合によっては、特定のデバイスから WLAN を削除できないことがあります。その場合は、デバイス設定を直接変更することが必要です。

ワイヤレス無線の設定

[Wireless Radios] ページでは、環境内のワイヤレスネットワーク全体の無線周波数（RF）最適化を管理できます。[Wireless Radio] プロファイルを使用すると、アクセスポイントが環境に合わせてそのワイヤレス無線設定を自動的に調整するかどうかを制御できるだけでなく、不正なアクセスポイントと干渉源の検出やレポート作成を有効にすることもできます。

以降のセクションで、ワイヤレス無線プロファイルを作成、変更、削除するための手順について説明します。

ワイヤレス無線プロファイルの作成

1. **[Network Configuration]** > **[Wireless Radios]** に移動します。
2. ✚（プラス）アイコンをクリックして新しいワイヤレス無線プロファイルを追加します。
3. [Device Group Selection] セクションで、以下の手順を完了します。
   - この設定のプロファイル名を入力します。
   - 組織を選択します。
   - 設定する 1 つ以上のデバイスグループを選択します。
4. ネットワーク内のアクセスポイントで自動 RF 最適化を実行するかどうかを選択します。RF 最適化を有効にする場合は、[Client Density] と [Traffic Type] に適切な値を選択してください。
5. 必要に応じて、不正アクセスポイントの検出を有効にします。
6. 必要に応じて、干渉源の検出を有効にします。
7. [Save] をクリックします。

   新しいワイヤレス最適化設定は、選択したグループ内の RF 最適化機能を備えたすべてのワイヤレスアクセスポイントに適用されます。

ワイヤレス無線プロファイルの変更

1. 変更するワイヤレス無線プロファイルの横にあるオプションボタンを選択し、[Edit] アイコンをクリックします。
2. RF 最適化の設定に必要な変更を加えて、[Update] をクリックします

ワイヤレス無線プロファイルの削除

1. 削除するワイヤレス無線プロファイルの横にあるオプションボタンを選択し、[Delete] アイコンをクリックします。

ゲストポータルの設定

[Guest Portals] ページでは、ゲスト ワイヤレス ネットワークに接続するときにゲストユーザーに表示される Web ページを集中管理できます。Cisco Business Dashboard は、組織ごとに 1 つのゲストポータルをホストします。各ポータルは、組織のアイデンティティを表すように個別にカスタマイズできます。

ゲストポータルは、複数のユーザー認証方法をサポートしていて、同じポータルが異なるネットワーク上の異なる認証方法を提示することができます。次の認証方法がサポートされています。

- ユーザー名/パスワード：各ゲストユーザーを事前にダッシュボードで定義し、ユーザー名とパスワードを割り当てる必要があります。その後、ワイヤレスネットワークに接続するときに、ゲストポータルにユーザー名とパスワードを入力する必要があります。
- Web での同意：ゲストユーザーに組織のアクセプタブルユースポリシーが提示され、ネットワークにアクセスするにはそのポリシーに同意する必要があります。
- 電子メールアドレス：ゲストユーザーは、ネットワークにアクセスする前に電子メールアドレスを入力するように求められます。電子メールアドレスはクライアントのユーザー名として記録され、ワイヤレス クライアント レポートおよびデバイスのユーザーインターフェイスに表示される場合があります。

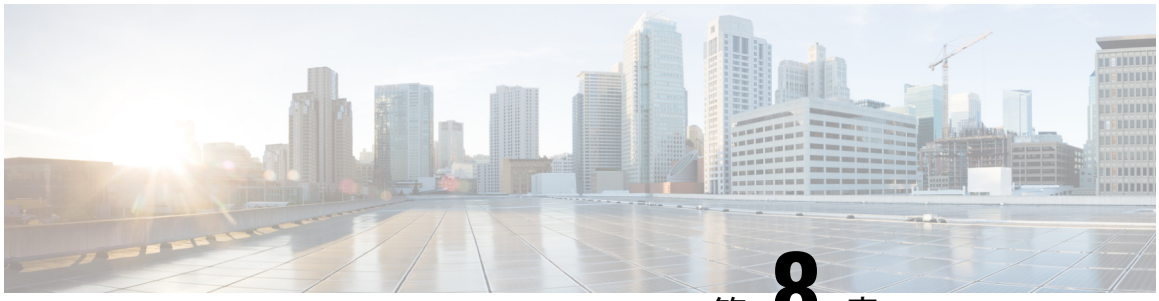
各ゲストポータルの外観は、使用するフォントを含むすべてのテキストフィールドの変更、色の変更、背景とロゴの画像の更新によってカスタマイズすることができます。

ゲストポータルをカスタマイズするには、次の手順を実行します。

1. [Network Configuration] > [Guest Portals] に移動します。
2. カスタマイズするゲストポータルのオプションボタンを選択し、[Edit] アイコンをクリックします
3. 表示されたフォームを使用して、キャプティブポータルの外観を更新します。テキストフィールドを変更したり、新しい画像をアップロードして背景やロゴとして使用したり、使用する色やフォントを変更したりすることができます。

   ゲストポータルのコンテンツは、選択した認証方法に応じて若干異なります。ページ下部にあるタブを選択すると、さまざまなバージョンのポータル向けにフィールドが更新されます。

   異なる認証方法のそれぞれで [Preview] ボタンをクリックすることで、変更を確認してから保存することができます。ポータルをデフォルトの外観に戻すには、右上の [Reset to defaults] ボタンをクリックします。
4. [Update] をクリックして変更内容を保存するか、[Cancel] をクリックして変更内容を取り消します。



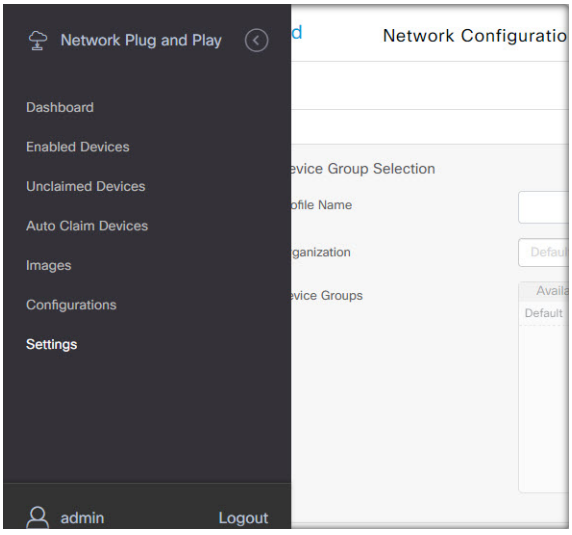
第 8 章

ネットワーク プラグアンドプレイ

この章は、次の項で構成されています。

ネットワーク プラグ アンド プレイについて

[Network Plug and Play] は、ネットワーク プラグ アンド プレイ対応デバイスと連動するサービスで、ファームウェアと設定を集中管理し、新しいネットワーク デバイスをゼロタッチ展開することができます。デバイスは、ネットワーク プラグアンドプレイ プロトコルを使用して直接展開できます。Dashboard に関連付けられているプローブによって検出された場合は、間接的に展開されます。



ネットワーク プラグアンドプレイ対応デバイスが設置されると、そのデバイスは、手動設定、DHCP、DNS、またはプラグ アンド プレイ接続サービスのいずれかを通じてネットワーク プ

ラグ アンド プレイ サーバを識別します。次のセクションでは、Cisco Business ダッシュボードでのネットワーク プラグアンドプレイ サービスの設定について詳しく説明します。

ネットワーク要件

ネットワーク プラグ アンド プレイ デバイスは、次のいずれかの方法を使用して、ネットワーク プラグ アンド プレイ サーバーのアドレスを自動的に見つけます。アドレスが見つかるまで、またはすべての方法が失敗するまで、各方法が順番に試行されます。これらの方法は以下の順番で使用されます。

- [Manual configuration]：管理インターフェイスを使用して、ネットワーク プラグ アンド プレイ対応デバイスにサーバーのアドレスを手動で設定できます
- [DHCP]：サーバーのアドレスは、ベンダー固有の情報オプションでデバイスに提供できます
- [DNS]：DHCP によるベンダー固有の情報オプションが提供されていない場合、デバイスは既知のホスト名を使用して、サーバについて DNS ルックアップを実行します。
- [Plug and Play Connect Service]：他のどの方法も成功しない場合、最終的にデバイスはプラグアンドプレイ接続サービスへの接続を試みます。このサービスにより、デバイスはサーバーにリダイレクトされます。

デバイスは、サーバを識別すると、そのサーバに接続し、サーバの指定に従いファームウェアと設定を更新します。

証明書の要件

ネットワーク プラグアンドプレイ サーバへの接続を確立する場合、クライアントは、サーバによって提示された証明書が有効であり、信頼できることを確認します。証明書が受け入れられ、接続が続行されるには、証明書が次の条件を満たしている必要があります。

- 証明書は信頼された証明機関（CA）によって署名されているか、または証明書自体がクライアントによって信頼されている必要があります。DHCP から学習した TrustpoolBundleURL か、またはプラグアンドプレイ接続サービスからダウンロードされた証明書は、クライアントによって信頼されます。
- サーバ ID が手動設定、DHCP、またはプラグアンドプレイ接続を使用して検出され、それが IP アドレスである場合は、[Common Name] フィールドまたは [Subject-Alt-Name] フィールドにその IP アドレスが含まれている必要があります
- サーバ ID が手動設定、DHCP、またはプラグアンドプレイ 接続を使用して検出され、それがホスト名である場合は、[Common Name] フィールドまたは [Subject-Alt-Name] フィールドにそのホスト名が含まれている必要があります。
- DNS 検出を使用してサーバ ID が検出された場合は、[Common Name] フィールドまたは [Subject-Alt-Name] フィールドに既知のホスト名である pnpserver.<*local domain*> に対応する IP アドレスが含まれている必要があります。

（注） 古いネットワーク プラグアンドプレイ クライアントの実装によっては、証明書内のサーバ ID の存在を確認しません。

DHCP を使用したディスカバリの設定

デバイスは、DHCP を使用してサーバ アドレスを検出するために、「ciscopnp」という文字列を含むオプション 60 を使用した DHCP discover メッセージを送信します。DHCP サーバは、ベンダー固有の情報オプション（オプション 43）を含む応答を送信する必要があります。デバイスは、このオプションからサーバアドレスを取得し、そのアドレスを使用してサーバに接続します。ネットワーク プラグアンドプレイ サーバのアドレスを含むオプション 43 の文字列は、たとえば「5A1N;B2;K4;I172.19.45.222;J80」などです。

このオプション 43 の文字列には、セミコロンで区切られた次のコンポーネントが含まれています。

- 5A1N：プラグ アンド プレイの DHCP サブオプション、アクティブ操作、バージョン 1、デバッグ情報なしを示します。文字列のこの部分は変更する必要がありません。
- B2：IP アドレスのタイプ。
  - B1 = ホスト名
  - B2 = IPv4
- K4：Cisco プラグ アンド プレイ エージェントとサーバの間で使用されるトランスポート プロトコル。
  - K4 = HTTP（デフォルト）
  - K5 = HTTPS
- Ixxx.xxx.xxx.xxx：サーバの IP アドレスまたはホスト名（大文字の i に続く部分）。この例では、IP アドレスは 172.19.45.222 です。
- Jxxxx：サーバに接続するために使用するポート番号。この例では、ポート番号は 80 です。HTTP のデフォルトはポート 80、HTTPS のデフォルトはポート 443 です。
- T*trustpoolBundleURL*：トラストプール バンドルの外部 URL を指定するオプション パラメータ（サーバ以外の場所からトラストプール バンドルを取得する場合）。たとえば、10.30.30.10 の TFTP サーバからバンドルをダウンロードするには、パラメータを「Ttftp://10.30.30.10/ca.p7b」と指定します。
- トラストプール セキュリティを使用し、T パラメータを指定しない場合、デバイスはサーバからトラストプール バンドルを取得します。
- Zxxx.xxx.xxx.xxx;：NTP サーバの IP アドレス。trustpool セキュリティを使用してすべてのデバイスを同期させる場合、このパラメータは必須です。

DHCP オプションの設定方法について詳しくは、DHCP サーバのマニュアルを参照してください。

DNS を使用したディスカバリの設定

DHCP ディスカバリでサーバの IP アドレスを取得できない場合、デバイスは次に DNS ルックアップを方法として使用します。デバイスは、DHCP サーバによって返されるネットワーク ドメイン名に基づいて、プリセットのホスト名「pnpserver」を使用してサーバの完全修飾ドメイン名（FQDN）を生成します。

たとえば、DHCP サーバがドメイン名「example.com」を返した場合、デバイスは「pnpserver.example.com」という FQDN を生成します。次に、この FQDN の IP アドレスを解決するために、ローカル ネーム サーバを使用します。

プラグ アンド プレイ接続を使用したディスカバリの設定

プラグアンドプレイ接続は、シスコ提供のサービスで、ネットワーク プラグアンドプレイ対応デバイスがサーバを検出するために使用する最後の手段です。プラグアンドプレイ接続を使用してサーバを検出するには、最初に PnP サーバを表すコントローラプロファイルを作成し、次に各デバイスをプラグアンドプレイ接続サービスに登録する必要があります。

プラグ アンド プレイ接続サービスへのアクセス

プラグ アンド プレイ接続サービスにアクセスするには、以下を行います。

1. Web ブラウザで *https://software.cisco.com* を参照します。
2. 画面の右上にある [Log In] ボタンをクリックします。Cisco スマート アカウントに関連付けられている cisco.com ID でログインします。
3. [Network Plug and Play] という見出しの下の [Plug and Play Connect] リンクを選択します。**プラグ アンド プレイ接続**サービスのメイン ページが表示されます。

コントローラ プロファイルの作成

PnP サーバのコントローラプロファイルを作成するには、次の手順を実行します。

1. ブラウザでプラグ アンド プレイ接続の Web ページを開きます。必要に応じて、使用する正しい仮想アカウントを選択します。
2. [Controller Profiles] リンクを選択し、[Add Profile] ボタンをクリックします。
3. ドロップダウンリストからコントローラタイプとして [PNP SERVER] を選択します。その後、[Next] をクリックします。
4. プロファイルの名前を指定し、オプションで説明を指定します。
5. [Primary Controller] という見出しの下で、表示されているドロップダウンを使用して、名前と IP アドレスのどちらでサーバーを指定するか選択します。表示されるフィールドに、サーバの名前またはアドレスを入力します。

6. サーバとの通信時に使用するプロトコルを選択します。プロビジョニングプロセスを完全なものにするために、HTTPS を使用することを強くお勧めします。
7. 選択したプロトコルが HTTPS の場合、サーバが使用する証明書を表示されたコントロールを使用してアップロードする必要があります。Cisco Business ダッシュボード からの証明書のダウンロードに関する詳細については、証明書の管理 （116 ページ） を参照してください。
8. オプションでセカンダリ コントローラを指定します。
9. [Next] をクリックし、設定を確認した後、[Submit] をクリックします。

デバイスの登録

シスコから直接購入した特定の製品は、注文の時点で Cisco スマート アカウントに関連付けることができ、それらの製品はプラグアンドプレイ接続に自動的に追加されます。ただし、Cisco Business プラグアンドプレイ対応製品の大部分は、手動で登録する必要があります。デバイスをプラグ アンド プレイ接続に登録するには、以下を行います。

1. ブラウザでプラグ アンド プレイ接続の Web ページを開きます。必要に応じて、使用する正しい仮想アカウントを選択します。
2. [Devices] リンクを選択し、[Add Devices] をクリックします。アカウントにデバイスを手動で追加する場合、場合により承認を受ける必要があります。これは 1 回限りのプロセスであり、必要な場合は、承認が付与された後に電子メールで通知を受け取ることができます。
3. デバイスを手動で追加するか、または CSV 形式で詳細をアップロードすることで複数のデバイスを追加するか選択します。用意されているリンクをクリックすると、サンプルの CSV ファイルをダウンロードできます。CSV ファイルのアップロードを選択した場合、[Browse] ボタンをクリックしてファイルを選択します。
4. **[次へ (Next)]** をクリックします。
5. デバイスの手動追加を選択した場合、[Identify Device] をクリックします。追加するデバイスのシリアル番号と製品 ID を指定します。ドロップダウンからコントローラプロファイルを選択します。オプションで、このデバイスの説明を入力します。
6. すべてのデバイスを追加するまで手順 4 を繰り返し、[Next] をクリックします。
7. 追加したデバイスを確認し、[Submit] をクリックします。

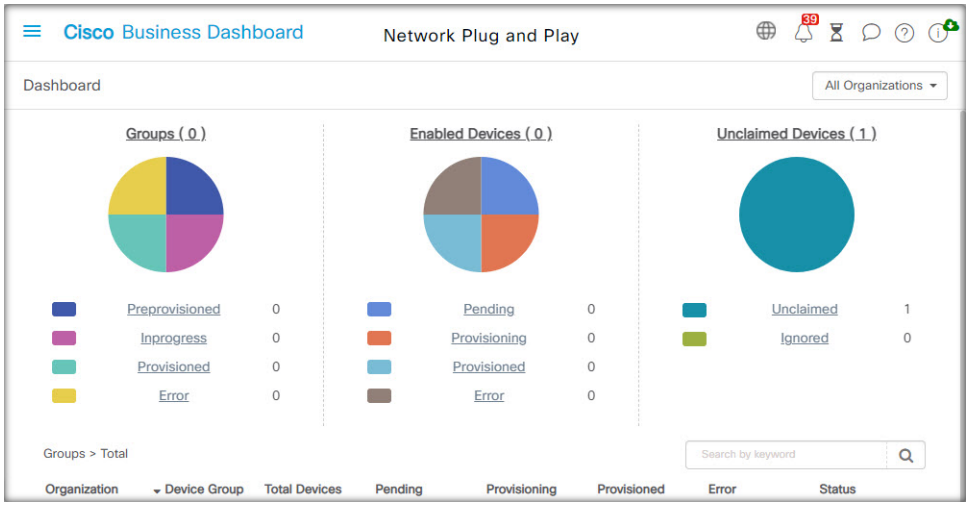
ネットワーク プラグ アンド プレイ サービスの設定

ご使用の環境でネットワーク プラグ アンド プレイ サービスを設定する場合、実行する必要があるタスクがいくつかあります。これには、設定とイメージのアップロード、ネットワークプラグアンドプレイを使用するためのデバイスの追加と設定、およびこれまでサービスに登録さ

れたことがないサービスに接続するデバイスの管理が含まれます。次のセクションで、これらのタスクについて詳しく説明します。

ネットワーク プラグアンドプレイ ダッシュボードの使用方法

[Network Plug and Play] ダッシュボードにより、[Network Plug and Play] を使用して現在プロビジョニングされているデバイスの概要が提供されます。



デバイスのステータスを次のように分類した 3 つのグラフが表示されます。

- Device Group
- PnP 対応デバイス
- Cisco Business ダッシュボード インベントリで定義されていないデバイス（要求されていないデバイス）

各チャートには、一覧表示されたそれぞれの状態のデバイスまたはグループの数が表示されます。チャートの状態の見出しをクリックすると、そのカテゴリに分類されるデバイスまたはグループの詳細なリストを表示できます。次の表に、それぞれのステータスの内訳を示します。

表 *5:* ネットワーク プラグアンドプレイ ダッシュボード：ステータスの定義

ステータス	説明
グループ	
事前プロビジョニング済み	保留状態の PnP 対応デバイスのみが含まれるデバイスグループ。
進行中	一部の PnP 対応デバイスが保留状態で、一部がプロビジョニング中の状態またはプロビジョニング済みの状態のデバイスグループ。
プロビジョニング	すべての PnP 対応デバイスがプロビジョニング済み状態のデバイスグループ。

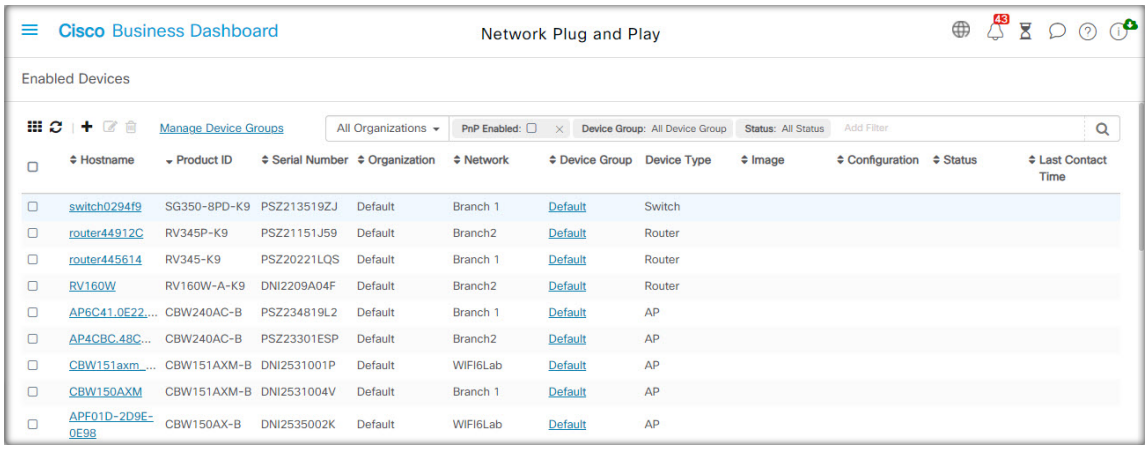
ステータス	説明
エラー	エラー状態の PnP 対応デバイスが 1 つ以上含まれるデバイスグループ。
有効なデバイス	
保留中	PnP が有効になっているものの、PnP サーバーにまだ接続していないインベントリ内のデバイス。
プロビジョニング	PnPサーバーに接続してプロビジョニングを開始したものの、プロビジョニングプロセスを完了していないデバイス。
プロビジョニング	PnP を使用して正常にプロビジョニングされたデバイス。
エラー	PnP プロビジョニングプロセスが失敗したデバイス。
要求されていないデバイス	
リクエスト元不明	PnP サーバーに接続したものの、インベントリで定義されていないデバイス。
無視	ユーザーによって明示的に無視された要求されていないデバイス。

ページの右上の組織のドロップダウンを使用して、特定の組織に対して表示されるデータを制限できます。テーブルに表示されるグループを制限するには、デバイス グループを表示するときに検索ボックスにグループ名全体または一部を入力します。または、個々のデバイスの現在のステータスを表示するには、プロビジョニングルールを表示するときにデバイス名、製品 ID、またはシリアル番号を検索ボックスに入力します。

（注） 要求元不明デバイスのチャートは、[All Organizations] のデータを表示する [Administrators] にのみ表示されます。

対応デバイスの管理

対応デバイスとは、イメージファイルか設定ファイルを使用してプロビジョニングされるように設定されているか、または以前に Cisco Business ダッシュボード によって検出され、ネットワーク プラグアンドプレイ プロトコルを使用して接続しようとしたことがあるインベントリ内のデバイスのことです。



イメージファイルまたは設定ファイルで設定された対応デバイスは、次の機会にそのイメージおよび/または設定がデバイスに適用されます。デバイスがDashboardに接続されて管理されている場合、変更はすぐに適用されます。それ以外の場合は、次回デバイスが接続された時点で、プローブまたは直接管理を介して、またはネットワーク プラグアンドプレイ プロトコルを使用してチェックインするときに、変更が適用されます。

新しい有効なデバイスを作成するには、次の手順に従います。

1. **[Network Plug and Play]** > **[Enabled Devices]** に移動します。
2. [+]（プラス）アイコンをクリックして、新しい対応デバイスをインベントリに追加します。
3. デバイスやそのデバイスが所属する組織、ネットワーク、およびデバイスグループの詳細の識別など、要求されたパラメータを [Add New Device] に入力し、[Next] をクリックします。
4. 必要に応じて、デバイスに適用するファームウェアイメージを選択します。イメージに [Default] を選択した場合、そのデバイスはサーバに接続するときにその製品のIDのデフォルトとして指定されたイメージを使用します。
5. 必要に応じて、デバイスに適用する設定と、複数のバージョンがある場合はその設定のバージョンも選択します。設定がプレースホルダを含むテンプレートである場合は、このデバイスに使用する値の入力を求めるフォームが表示されます。必要に応じて、これらのフィールドに値を入力します。システムで定義されたパラメータがテンプレートに使用されている場合は、チェックボックスをクリックして、使用される値を表示することができます。
6. [Next] をクリックして、[Summary] 画面に進みます。入力したデータが正しいことを確認します。下部の [Preview] ウィンドウで、最終的なデバイス設定を確認することもできます。問題がなければ、[Finish] をクリックします。

既存のデバイスを編集するには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Enabled Devices]** に移動します。

2. 変更するデバイスのチェックボックスをオンにして、[Edit] をクリックします。または、デバイスの名前をクリックすることもできます。
3. [Next] をクリックして [Provision Device] 画面を表示します。必要に応じて、イメージや構成ファイルを変更し、その設定に関連付けられているパラメータ値に変更を加えます。
4. [Next] をクリックして、[Summary] 画面に進みます。入力したデータが正しいことを確認します。下部の [Preview] ウィンドウで、最終的なデバイス設定を確認することもできます。問題がなければ、[Finish] をクリックします。

（注） すでにプロビジョニングされているデバイスのイメージファイルまたは構成ファイルの設定が変更されると、そのデバイスの状態は保留中にリセットされ、次回 Dashboard にチェックインする時にデバイスが再プロビジョニングされます。

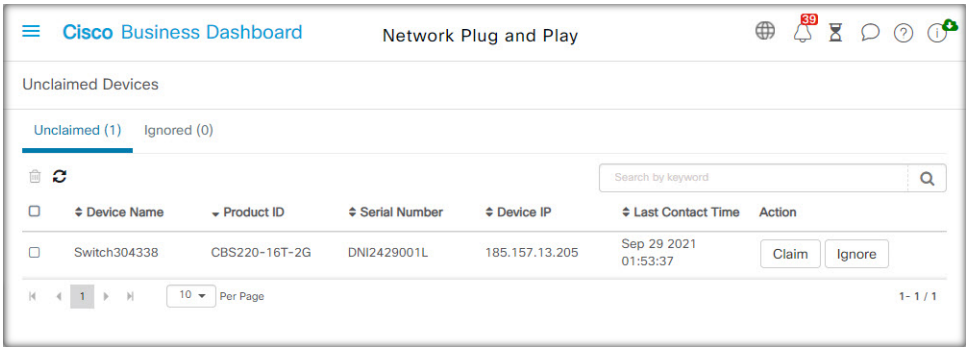
有効なデバイスを削除するには、次の手順に従います。

1. **[Network Plug and Play]** > **[Enabled Devices]** に移動します。
2. 削除するデバイスのチェックボックスを 1 つ以上オンにして、[Delete] アイコンをクリックします。

（注） 削除しなければそのデバイスが Dashboard に認識される場合に対応デバイスを削除し、そのデバイスがオンラインだった場合は、そのデバイスのイメージファイルまたは構成ファイルの設定のみが削除されます。他の管理対象デバイスと同様にそのデバイスはインベントリに残ります。その後、デバイスが PnP を使用して Dashboard に接続されると、新しいエントリが [Enabled Devices] テーブルに追加されます。

要求されていないデバイス

（注） [Unclaimed Devices] ページは、管理者のみが使用できます。



要求されていないデバイスとは、サービスに接続済みである一方で、そのデバイスに一致するデバイスレコードがインベントリにないデバイスです。要求されていないデバイスのリストを表示し、要求されていないデバイスをネットワーク プラグ アンド プレイを使用して管理できるように要求するには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Unclaimed Devices]** に移動し、[Unclaimed] タブを選択します。
2. 管理するデバイスの要求ボタンをクリックします。
3. デバイスが所属する組織、ネットワーク、デバイスグループなど、要求されたパラメータを [Unclaimed Device] フォームに入力し、[Next] をクリックします。
4. 必要に応じて、デバイスに適用するファームウェアイメージを選択します。イメージに [Default] を選択した場合、そのデバイスはサーバに接続するときにその製品の ID のデフォルトとして指定されたイメージを使用します。
5. または、デバイスに適用する設定とともに、複数のバージョンがある場合はその設定のバージョンも選択します。設定がプレースホルダを含むテンプレートである場合は、このデバイスに使用する値の入力を求めるフォームが表示されます。必要に応じて、これらのフィールドに値を入力します。

   システムで定義されたパラメータがテンプレートに使用されている場合は、チェックボックスをオンにして、使用される値を表示することができます。
6. [Next] をクリックして、[Summary] 画面に進みます。入力したデータが正しいことを確認します。下部の [Preview] ウィンドウで、最終的なデバイス設定を確認することもできます。問題がなければ、[Finish] をクリックします。

プロビジョニングせずに未要求リストからデバイスを削除するには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Unclaimed Devices]** に移動し、[Unclaimed] タブを選択します。
2. リストから削除するデバイスに対して [Ignore] をクリックします。

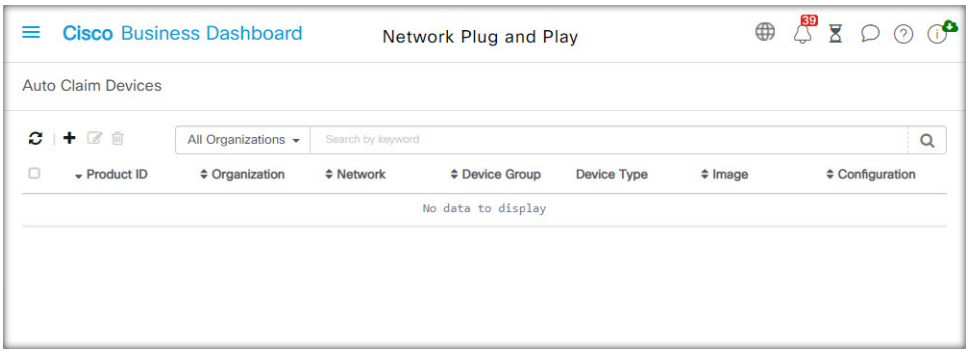
デバイスが [Ignored] リストに移動され、それ以上アクションは実行されません。無視されたデバイスを再利用するには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Unclaimed Devices]** に移動し、[Ignored] タブを選択します。
2. 再要求するデバイスの[Unignore] ボタンをクリックします。

デバイスが [Unclaimed] リストに移動され、デバイスを上で説明したように要求できるようになります。

自動要求のデバイス

（注） [Auto Claim] ページは管理者のみが使用できます。



デバイスの製品 ID に対して自動要求ルールを作成することで、サーバーで要求されていないデバイスが自動的に要求され、プロビジョニングされるようにすることができます。自動要求ルールを作成するには、次の手順に従います。

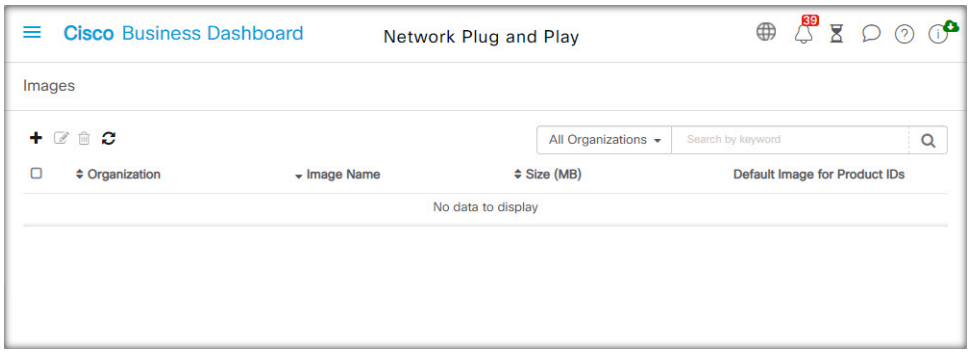
1. **[Network Plug and Play]** > **[Auto Claim Devices]** に移動します。
2. [+]（プラス）アイコンをクリックして、新しい**自動要求**ルールを作成します。
3. 照合する製品 ID（PID）と、新たに要求されたデバイスが所属する組織、ネットワーク、およびデバイスグループなど、要求されたパラメータを [Auto Claim Device] フォームに入力し、[Next] をクリックします。
4. 必要に応じて、デバイスに適用するファームウェアイメージを選択します。イメージに [Default] を選択した場合、そのデバイスはサーバに接続するときにその製品の ID のデフォルトとして指定されたイメージを使用します。
5. または、デバイスに適用する設定とともに、複数のバージョンがある場合はその設定のバージョンも選択します。設定がプレースホルダを含むテンプレートである場合は、このデバイスに使用する値の入力を求めるフォームが表示されます。必要に応じて、これらのフィールドに値を入力します。

   システムで定義されたパラメータがテンプレートに使用されている場合は、チェックボックスをオンにして、使用される値を表示することができます。
6. [Next] をクリックして、[Summary] 画面に進みます。入力したデータが正しいことを確認します。下部の [Preview] ウィンドウで、最終的なデバイス設定を確認することもできます。問題がなければ、[Finish] をクリックします。

インベントリに存在しない新しいデバイスは、自動要求ルールのリストと比較照合されます。一致がある場合、**自動要求**ルールで定義されているイメージと構成ファイルで新しいデバイスレコードがインベントリ内に作成されます。その後、デバイスがそれに応じてプロビジョニングされます。デバイスが**自動要求**ルールに一致しない場合、そのデバイスは [Unclaimed] リストに追加され、以後アクションは実行されません。

デバイスのファームウェア イメージ

[Images] ページでは、ファームウェアイメージをアップロードできます。アップロード後、イメージをデバイスに展開できます。



ファームウェアイメージは、各プラットフォームのデフォルトイメージとして指定でき、それにより、デバイスファミリ全体に対してファームウェアを非常に簡単にアップデートできます。ファームウェアイメージは組織固有のものであり、同じ組織に関連付けられているプロビジョニングデバイスにのみ使用できます。

ファームウェアイメージをアップロードするには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Images]** に移動します。
2. ✚（プラス）アイコンをクリックします。
3. イメージの組織をドロップダウンから選択します。
4. ご使用の PC からファームウェア イメージをドラッグし、[Upload File] ウィンドウのターゲット領域にドロップします。または、ターゲット領域をクリックし、アップロードするファームウェア イメージを選択します。
5. [Upload] をクリックします。

1つ以上のデバイスタイプに対してイメージをデフォルトイメージとして指定できます。イメージをデフォルトのイメージとして指定するには、以下の手順に従います。

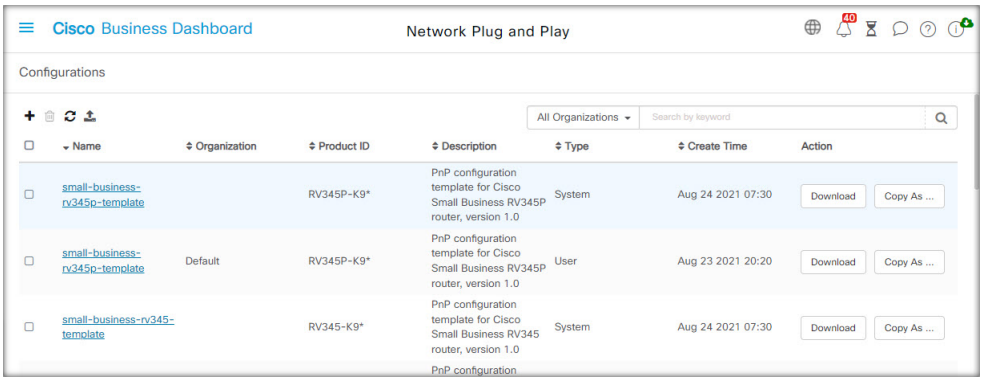
1. **[Network Plug and Play]** > **[Images]** に移動します。
2. [Images] テーブルでイメージのオプション ボタンを選択し、[edit] をクリックします。
3. [Default Image for Product IDs] フィールドに、製品 ID のカンマ区切りリストを入力します。製品 ID には、単一文字を表すワイルドカード文字の「?」、および文字列を表すワイルドカード文字の「*」を含めることができます。
4. [Save] をクリックします。

イメージを削除するには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Images]** に移動します。
2. 削除するイメージのオプションボタンを選択し、[delete] をクリックします。

デバイスの設定ファイル

[Configurations] ページでは、構成ファイルをアップロードまたは作成できます。アップロード後、構成ファイルをデバイスに展開できます。構成ファイルは組織固有のものであり、同じ組織に関連付けられているプロビジョニングデバイスにのみ使用できます。



構成ファイルは、単純なテキストファイルの場合もあれば、複数のデバイスで同じ構成ファイルを使用できるようにするためのプレースホルダや関連付けられたメタデータが含まれている場合もありますが、デバイスごとに一意のパラメータを設定することができます。たとえば、1 つの設定テンプレートを複数のデバイスに適用できますが、デバイスごとにホスト名を個別に指定することもできます。

ダッシュボードアプリケーションには、いくつかの設定テンプレートがシステムテンプレートとして含まれており、すべての組織で使用できます。これらのテンプレートを使用すると、一般的に変更される設定を変更することもそのまま使用することもでき、新しいテンプレートのベースとしてコピーして使用することも可能です。

新しい構成を手動で作成するには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Configurations]** に移動します。
2. ✚（プラス）アイコンをクリックします。
3. テンプレートエディタが開くと、左側に設定用の空白の領域、右側にそのテンプレートに関連付けられたメタデータを管理するためのフォームが表示されます。

   左上のフィールドに設定の名前を入力します。組織を選択し、この設定をサポートする製品 ID のカンマ区切のリストを右側のフィールドに入力します。必要に応じて、説明を入力します。製品 ID には、単一文字を表すワイルドカード文字の「?」、および文字列を表すワイルドカード文字の「*」を含めることができます。
4. 左側のテキスト領域にテキストを入力するか、または貼り付けて、設定を作成します。必要に応じて、右側のコントロールを使用してメタデータに適切な変更を加えます。

   [Preview] ボタンを使用すると、デバイスに割り当てられたときに設定テンプレートがどのように表示されるかを確認できます。
5. 設定に問題なければ、[Save] をクリックします。

構成ファイルをアップロードするには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Configurations]** に移動します。
2. [Upload] アイコンをクリックします。
3. ドロップダウンから設定に組織を選択します。設定の名前を指定し、必要に応じて説明を追加します。
4. ご使用の PC から設定ファイルをドラッグし、[Upload File] ウィンドウのターゲット領域にドロップします。または、ターゲット領域をクリックし、アップロードする設定ファイルを選択します。
5. [Upload] をクリックします。

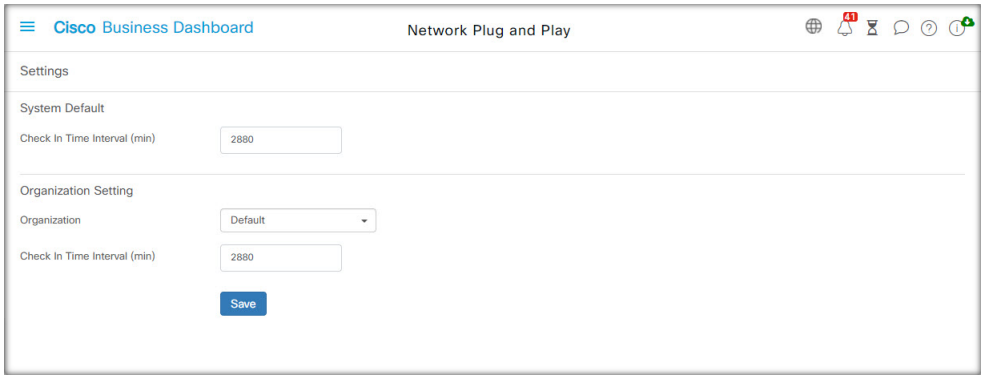
構成ファイルの内容を確認する必要がある場合、アップロードした構成ファイルのファイル名をクリックすると、テンプレートエディタに内容を表示できます。

構成を削除するには、次の手順に従います。

1. **[Network Plug and Play]** > **[Configurations]** に移動します。
2. 削除する設定のチェックボックスを 1 つ以上オンにして、[Delete] アイコンをクリックします。

設定の管理

[Network Plug and Play Settings] ページでは、ネットワーク プラグアンドプレイ プロトコルの動作を制御できます。



[Check In Time Interval] では、初回プロビジョニングの後にデバイスがネットワーク プラグアンドプレイ サービスに接続する頻度が制御されます。このパラメータを変更するには、以下の手順に従います。

1. **[Network Plug and Play]** > **[Settings]** に移動します。
2. 表示されるフィールドに、目的の接続間隔を入力します。時間は分単位で、デフォルトは 2880 分（2 日）です。
3. [Save] をクリックします。

[Check In Time Interval] はシステム全体に対して設定されますが、組織レベルでオーバーライドできます。組織に間隔が設定されていない場合は、システム値が使用されます。

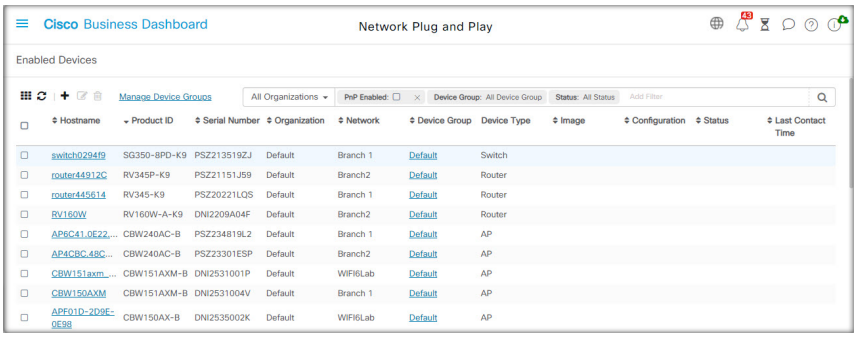
証明書の設定

最初の起動時に Cisco Business ダッシュボード によって自動的に生成された証明書は自己署名証明書です。ほとんどの場合、ネットワーク プラグアンドプレイ クライアントが証明書を受け入れるにはこれでは十分でなく、新しい証明書を生成する必要があります。新しい自己署名証明書または証明書署名要求（CSR）を生成する場合、Dashboard は、GUI の [Subject Alternative Name] フィールドに指定された値の他に、[Common Name] フィールドの内容を [Subject Alternative Name] フィールドに含めます。

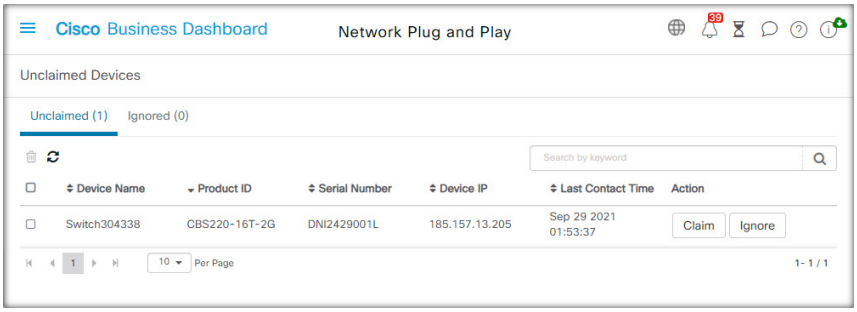
Dashboard の証明書の設定に関する詳細については、証明書の管理 （116 ページ） を参照してください。

ネットワーク プラグ アンド プレイのモニタリング

ネットワーク プラグ アンド プレイ サービスで認識されている各デバイスは、[Enabled Devices] ページ



または [Unclaimed Devices] ページにステータス表示付きで表示されます。

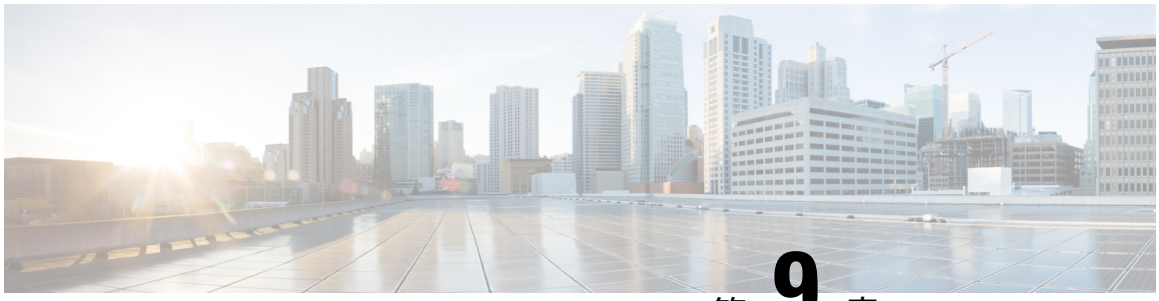


また、このステータスは、[PnP Status] 列の表示を可能にすることで、[Inventory] ページに表示することもできます。ステータス フィールドには、デバイスの現在の状態が表示され、次の表にリストされている値のいずれかが含まれます。ステータス フィールドをクリックすると、そのデバイスの時間経過に伴う状態変化の履歴など、詳細を表示できます。

表 *6:* ネットワーク プラグ アンド プレイ：デバイス ステータス

ステータス	説明
Pending	デバイスが定義されている一方で、サービスには未接続。

ステータス	説明
Provisioning	デバイスがサービスに対して初回接続を実行済み。
Provisioning_Image	デバイスによってファームウェア イメージが適用中。
Provisioned _Image_Rebooting	新しいファームウェアを実行するためにデバイスがリブート中。
Provisioned_Image	新しいファームウェアの適用が正常に完了。
Provisioning_Config	デバイスに設定ファイルを適用中。
Provisioned_Config	デバイスへの設定ファイルの適用が正常に完了。デバイスの種類によっては、設定を適用するためにリブートする場合があります。
Error	エラーが発生しました。ログ ファイルで詳細を確認できます。
Provisioned	デバイスのプロビジョニング プロセスが完了。



第 9 章

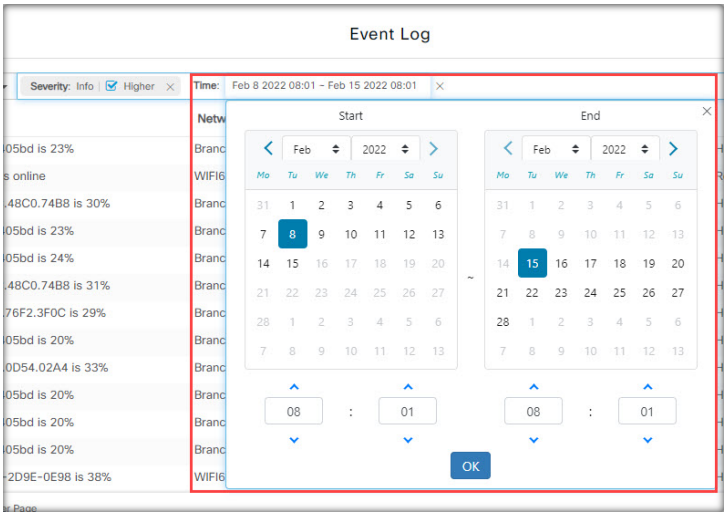
イベント ログ

この章は、次の項で構成されています。

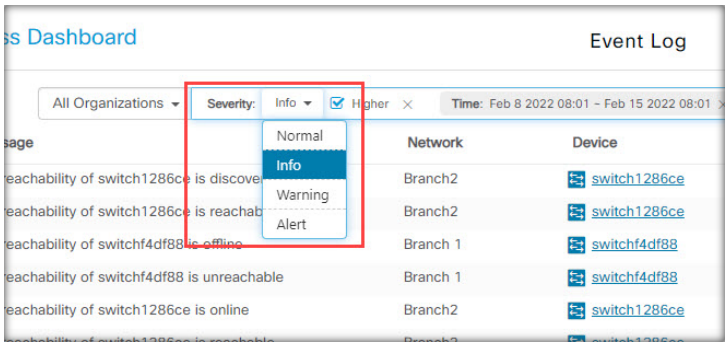
イベント ログについて

[Event Log] 画面を開いて、ネットワーク全体で発生したイベントを検索します。この画面は、ネットワーク全体で生成されたイベントを検索およびソートできるインターフェイスを提供します。これらのイベントが最大 500,000 件、最大 90 日間保存されます。提供されるフィルタコントロールを使用して、次のパラメータの組み合わせに基づいて表示されたイベントを制限することができます。

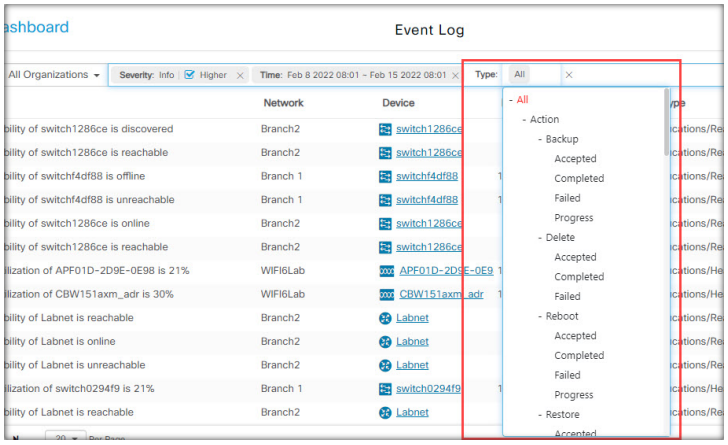
[Time] を追加し、目的の期間を示す開始時刻と終了時刻を指定します。この期間内に発生したイベントのみが表示されます。



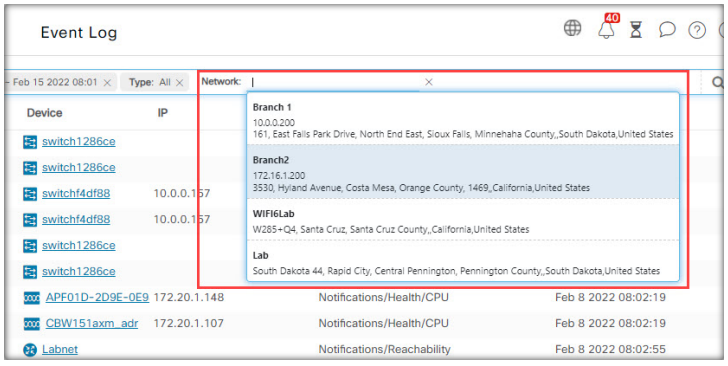
[Severity] フィルタを追加し、表示するイベントのレベルを選択します。[Higher] チェックボックスを選択して、より高いレベルの重大度のイベントを含めることもできます。



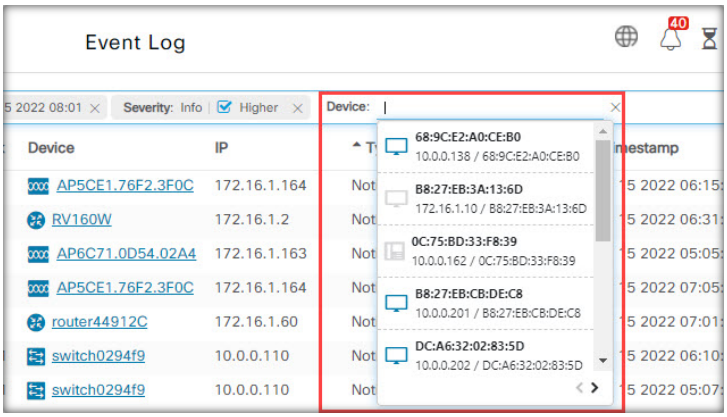
[Type] フィルタを追加し、表示するイベントタイプを 1 つ以上選択します。タイプはツリー構造で配置され、タイプを選択すると選択したタイプの下のすべてのイベントタイプが自動的にツリーに含まれます。



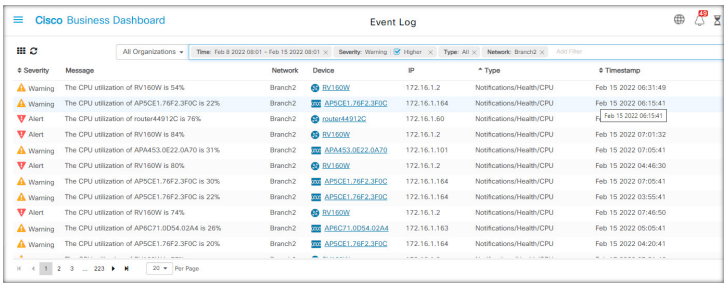
[Network] フィルタを使用して、1 つ以上のネットワーク別にイベントを表示します。入力すると、一致したサイトが表示されます。

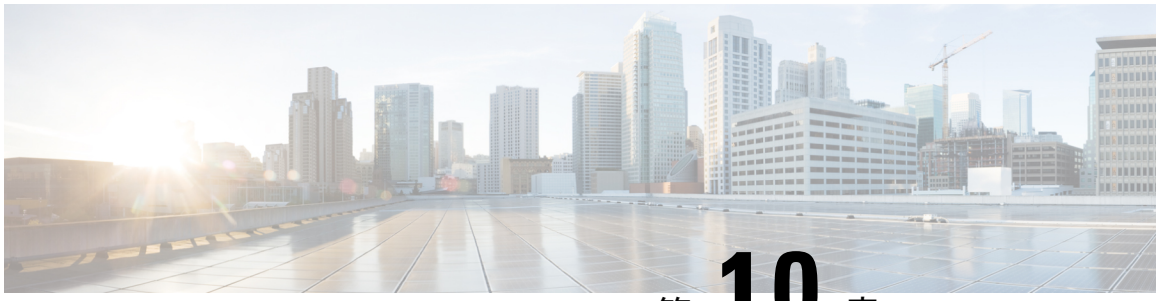


[Device] フィルタを使用して、1 つ以上のデバイス別にイベントを表示します。入力すると、一致したデバイスが表示されます。名前、IP アドレス、または MAC アドレスでデバイスを指定することもできます。



フィルタ条件に一致するイベントは、次の例のようなテーブルに表示されます。列見出しを使用して、テーブル内の情報を並べ替えることもできます。





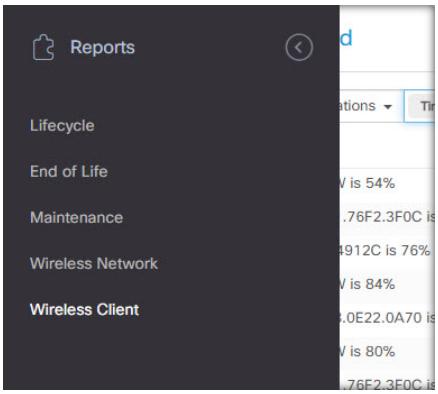
第 10 章

レポート

この章は、次の項で構成されています。

レポートの概要

Cisco Business ダッシュボード の [Reports] オプションは、ネットワークに関する一連のレポートを提供します。以下のものを含むレポートが用意されています。

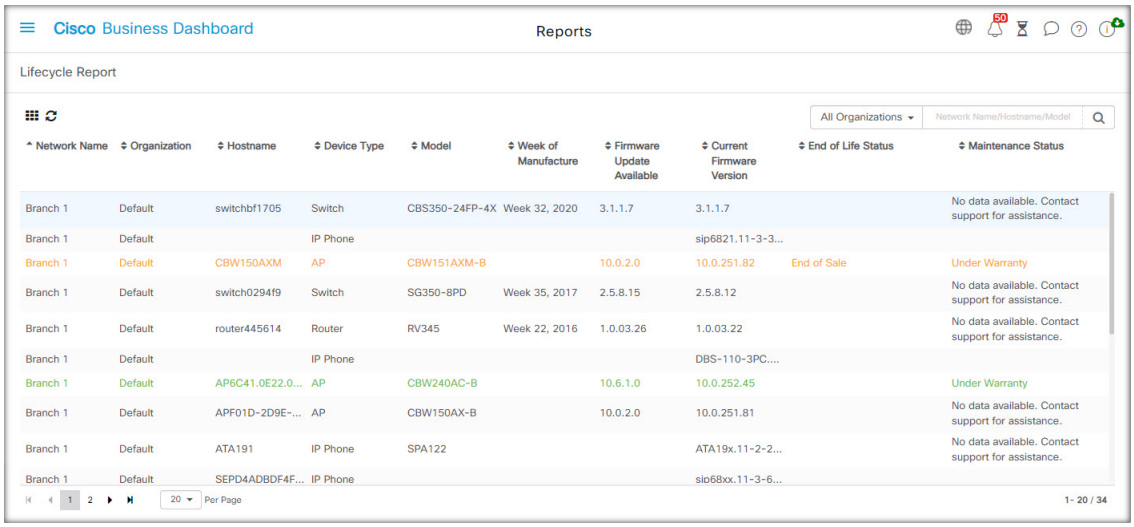


- [Lifecycle]：ネットワーク内のデバイスのライフサイクルステータスの要約を提供します。
- [End of Life]：サービス終了案内が発行されているすべてのデバイスを示します。
- [Maintenance]：すべてのデバイスとその保証状態、デバイスに有効なサポート契約があるかどうかが一覧表示されます。
- [Wireless Network]：SSID、アクセスポイント、およびスペクトル使用状況などワイヤレス環境に関する情報が表示されます。

- [Wireless Client]：ネットワークに表示されるワイヤレスクライアントに関する詳細が表示されます。

ライフサイクルレポートの表示

ライフサイクルレポートは、ソフトウェアとハードウェアの両方のライフサイクルステータスを考慮した、ネットワークデバイスのステータスの概要ビューを提供します。



次の表に、このレポートで提供される情報を示します。

フィールド	説明
Network Name	デバイスがあるネットワークの名前。
Organization	デバイスが属する組織。
Hostname	デバイスのホスト名。
Device Type	デバイスのタイプ。
Model	デバイスのモデル番号。
Week of Manufacture	デバイスの製造日を、週番号と年で表示します。
Firmware Update Available	デバイスに対して利用できる最新のファームウェア バージョンを表示するか、デバイスのファームウェアが現在最新であることが示されます。
Firmware Version	デバイス上で動作している現在のファームウェア バージョンを表示します。

フィールド	説明
End of Life Status	デバイスに対してサポート終了案内が発行されているかどうかと、サポート終了プロセス中の次の主なマイルストーンの日付を示します。
Maintenance Status	デバイスが現在保証対象か、またはサポート契約の対象になっているかを示します。

デバイスに対する表の中で注意が必要な行は、緊急度を示すために色付けされています。たとえば、サポート終了案内が発行されているデバイスは、サポート終了マイルストーンに達していない場合はオレンジ色で表示され、デバイスがシスコによってサポートされなくなった場合は赤く表示されます。

レポートの上部にある [Search] ボックスを使用すると、結果をフィルタ処理できます。[Search] ボックスにテキストを入力すると、表示されるエントリの数が一致するテキストに制限されます。結果は、[Organization] ドロップダウンを使用して特定の組織に制限することができます。

レポートの左上にある [column selection] アイコンを使用すると、表示される情報をカスタマイズできます。アイコンをクリックして、表示されるチェックボックスを使用すると、レポートに含める列を選択できます。

サポート終了レポートの表示

サポート終了レポートには、**サポート終了**案内が発行されているすべてのデバイスと、サポート終了プロセスの主な日付、推奨される後継プラットフォームが一覧表示されます。

次の表に提供される情報を示します。

フィールド	説明
Network Name	デバイスがあるネットワークの名前。
Organization	デバイスが属する組織。
Product ID	デバイスの製品 ID またはパーツ番号。

フィールド	説明
Hostname	デバイスのホスト名。
Device Type	デバイスのタイプ。
Current Status	製品のサポート終了プロセスの段階。
Date of Announcement	サポート終了案内が発行された日付。
Last Date of Sale	製品がシスコによって販売されなくなる日付。
Last Date of Software Releases	その製品に対してそれ以上ソフトウェア バージョンがリリースされなくなる日付。
Last Date for New Service Contract	デバイスに対して新たなサポート契約を結ぶ最終日付。
Last Date for Service Renewal	デバイスに対して既存のサポート契約を更新する最終日付。
Last Date of Support	シスコが製品に対するサポートを提供しなくなる日付。
Recommended Replacement	推奨される後継製品。
Product Bulletin	製品案内番号と、シスコの Web サイト上の案内へのリンク。

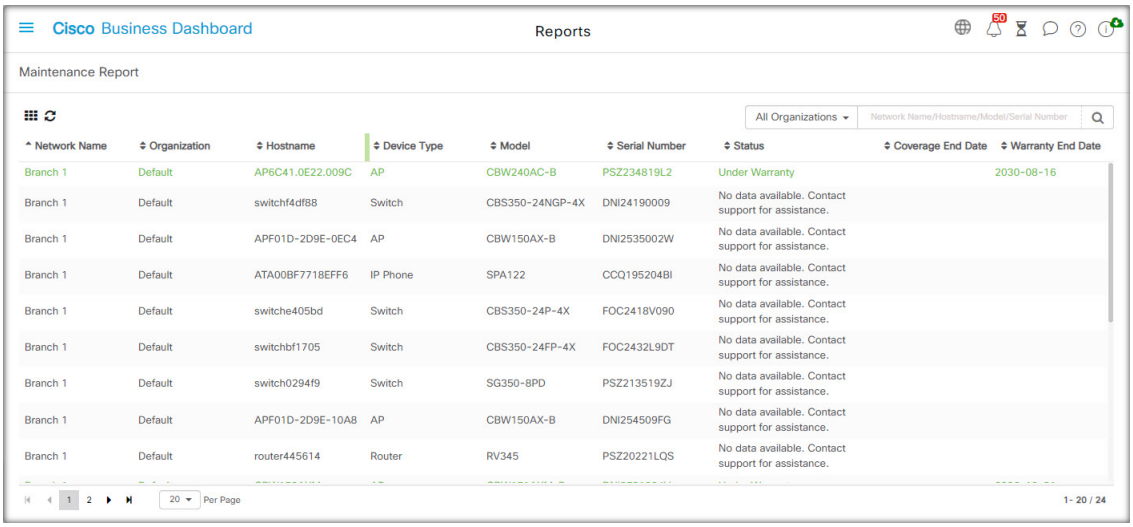
表の各行は、デバイスのサポート終了プロセスの段階を示すために色分けされています。たとえば、販売最終日を過ぎているものの、サポートの最終日に達していないデバイスはオレンジ色で表示され、サポートの最終日を過ぎたデバイスは赤で表示されます。

レポートの上部にある [Search] ボックスを使用すると、結果をフィルタ処理できます。[Search] ボックスにテキストを入力すると、表示されるエントリの数が一致するテキストに制限されます。結果は、[Organization] ドロップダウンを使用して特定の組織に制限することができます。

レポートの左上にある [column selection] アイコンを使用すると、表示される情報をカスタマイズできます。アイコンをクリックして、表示されるチェックボックスを使用すると、レポートに含める列を選択できます。

メンテナンス レポートの表示

メンテナンス レポートには、各デバイスに対する保証およびサポート契約ステータス情報が含まれているすべてのネットワーク デバイスが一覧表示されます。



次の表に、このレポートで提供される情報を示します。

フィールド	説明
Network Name	デバイスがあるネットワークの名前。
Organization	デバイスが属する組織。
Hostname	デバイスのホスト名。
Device Type	デバイスのタイプ。
Model	デバイスのモデル番号。
Serial Number	デバイスのシリアル番号。
Status	デバイスの現在のサポート ステータス。
Coverage End Date	現在のサポート契約が切れる日付。
Warranty End Date	デバイスに対する保証が切れる日付。

表の各行は、デバイスのサポート ステータスを示すために色分けされています。たとえば、保証またはサポート契約の期限に近づいているデバイスはオレンジ色で表示され、保証が切れ現在サポート契約が結ばれていないデバイスは赤で表示されます。

レポートの上部にある [Search] ボックスを使用すると、結果をフィルタ処理できます。[Search] ボックスにテキストを入力すると、表示されるエントリの数が一致するテキストに制限されます。結果は、[Organization] ドロップダウンを使用して特定の組織に制限することができます。

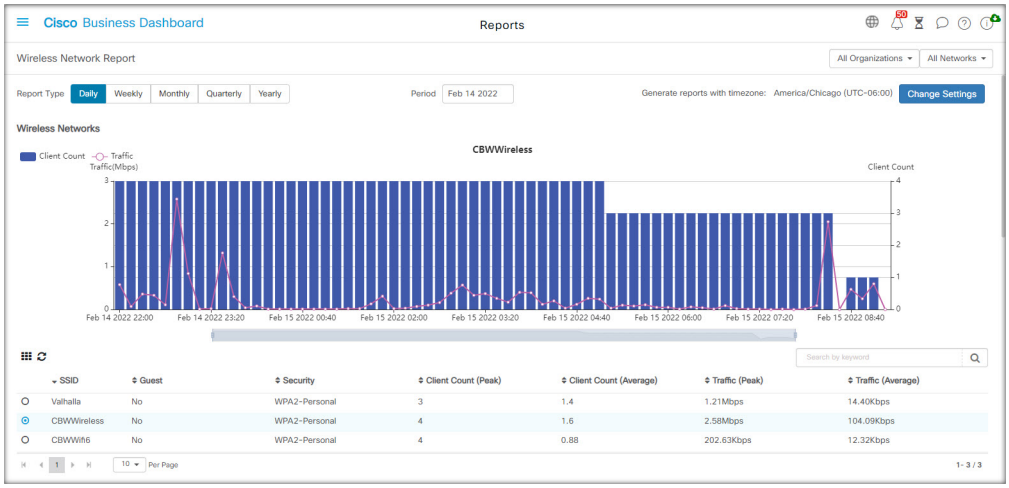
レポートの左上にある [column selection] アイコンを使用すると、表示される情報をカスタマイズできます。アイコンをクリックして、表示されるチェックボックスを使用すると、レポートに含める列を選択できます。

ワイヤレス ネットワーク レポートの表示

ワイヤレス ネットワーク レポートには、SSID、ワイヤレス スペクトルの使用、およびアクセス ポイントごとに分類されたワイヤレス ネットワークの詳細が表示されます。また、検出された不正なアクセス ポイントのリストも表示されます。ページの上部にあるコントロールを使用して、日別から年別までの時間範囲でレポートを生成できます。

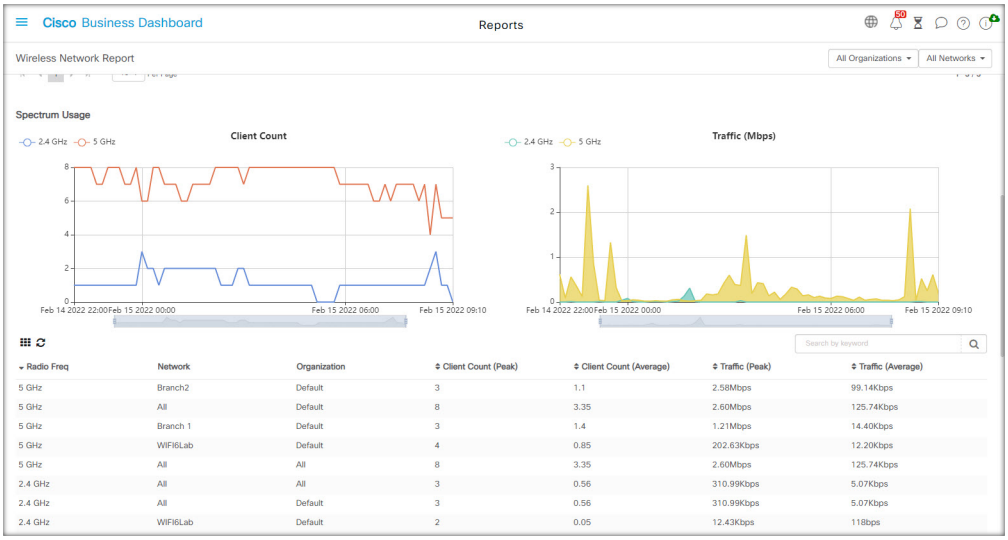
いくつかのデータセットには、選択した行の時間の経過に伴う内訳を示すグラフが含まれています。グラフ上の凡例のラベルをクリックするとデータの各セットの表示を切り替えられます。

次の表で、レポートのさまざまなセクションに表示される情報について説明します。

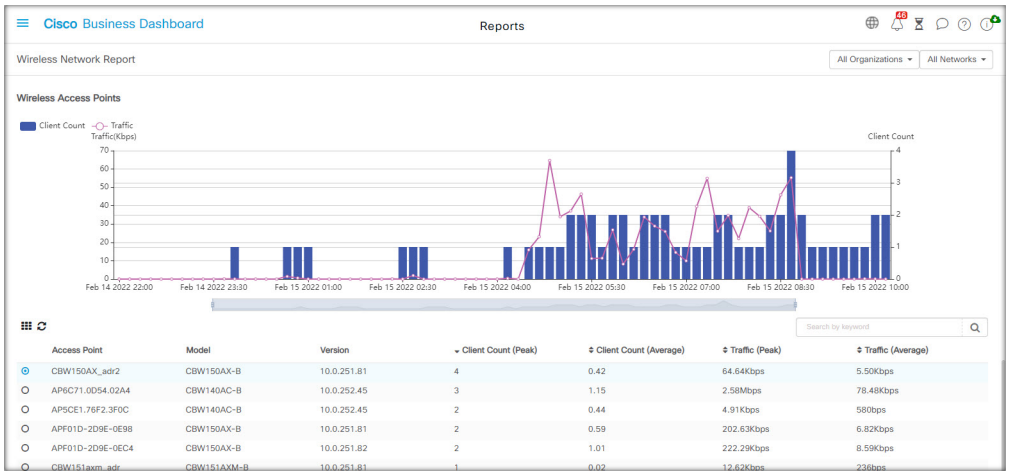


ワイヤレス ネットワーク テーブル	
SSID	ワイヤレスネットワーク名。
Network（デフォルトでは非表示）	SSID があるネットワーク。
Organization（デフォルトでは非表示）	SSID が属する組織。
Guest	SSID がゲストアクセス用に設定されているかどうか。
Security	SSID 用に設定されたセキュリティ方式。
Client Count (Peak)	レポートの対象期間に SSID に関連付けられたクライアントの最大数。
Client Count (Average)	レポートの対象期間に SSID に関連付けられたクライアントの平均数。

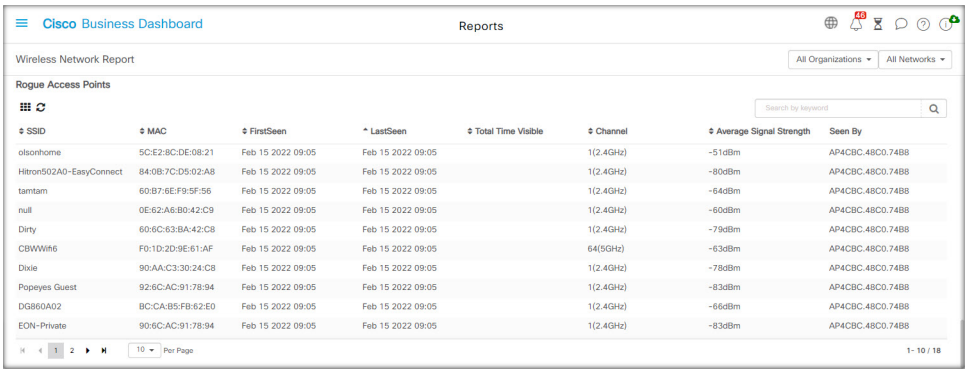
ワイヤレス ネットワーク テーブル	
Traffic (Peak)	レポートの対象期間に SSID を介した最大集約トラフィック レート。
Traffic (Average)	レポートの対象期間に SSID を介した平均集約トラフィック レート。



スペクトル使用状況テーブル	
Radio Freq	使用中の無線周波数帯（2.4 GHz または 5 GHz）。
Network	表示されるスペクトル使用状況データが適用されるネットワーク。
Organization	スペクトル使用状況データが適用される組織。
Client Count (Peak)	レポートの対象期間に周波数帯を使用したクライアントの最大数。
Client Count (Average)	レポートの対象期間に周波数帯を使用したクライアントの平均数。
Traffic (Peak)	レポートの対象期間に周波数を介した最大合計トラフィック レート。
Traffic (Average)	レポートの対象期間に周波数を介した平均合計トラフィック レート。



ワイヤレス アクセス ポイント テーブル	
Access Point	アクセス ポイントの名前。
Network（デフォルトでは非表示）	アクセスポイントがあるネットワーク。
Organization（デフォルトでは非表示）	アクセスポイントが属する組織。
Model	アクセスポイントのモデル。
Version	アクセスポイントで実行しているファームウェアバージョン。
Client Count (Peak)	レポートの対象期間にアクセスポイントに関連付けられたクライアントの最大数。
Client Count (Average)	レポートの対象期間にアクセスポイントに関連付けられたクライアントの平均数。
Traffic (Peak)	レポートの対象期間にアクセスポイントを介した最大合計トラフィックレート。
Traffic (Average)	レポートの対象期間にアクセスポイントを介した平均合計トラフィックレート。



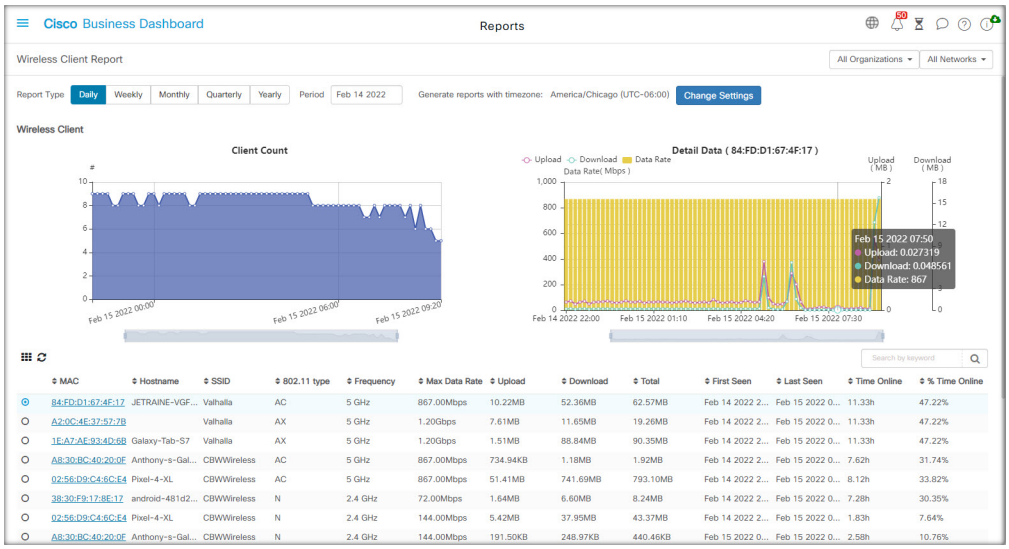
不正なアクセスポイントテーブル	
SSID	検出された SSID。
Network（デフォルトでは非表示）	検出アクセスポイントがあるネットワーク。
Organization（デフォルトでは非表示）	検出アクセスポイントが属する組織。
MAC	不正アクセスポイントの MAC アドレスの検索。
First Seen	不正アクセスポイントが最初に検出された時刻。
Last Seen	不正アクセスポイントが最後に表示された時刻。
Total Time Visible	不正アクセスポイントがオフラインだった合計時間。
Channel	不正アクセスポイントが使用したワイヤレスチャネル。
Average Signal Strength	アクセスポイントの検出により検出された不正アクセスポイントの平均信号強度。
Seen By	不正アクセスポイントが検出されたアクセスポイント。

ワイヤレス クライアント レポートの表示

ワイヤレス クライアント レポートには、ネットワーク上のワイヤレス クライアントの詳細が表示されます。ページの上部にあるコントロールを使用して、日別から年別までの時間範囲でレポートを生成できます。

各データセットには、選択した行の時間の経過に伴う内訳を示すグラフが含まれています。グラフ上の凡例のラベルをクリックするとデータの各セットの表示を切り替えられます。

次の表は、各レポートで提供される情報を示しています。



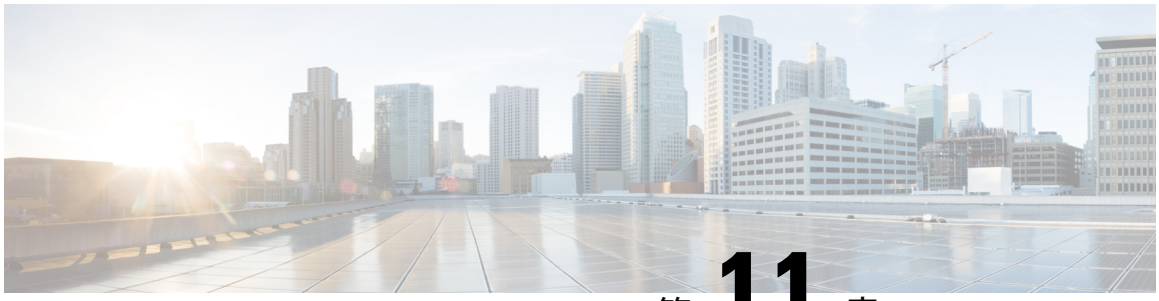
ワイヤレス クライアント テーブル	
MAC	クライアントの MAC アドレス
Hostname	クライアントのホスト名（使用可能な場合）。
Organization	クライアントで最後に表示された組織。
Network	クライアントで最後に表示されたネットワーク。
SSID	クライアントが最後に関連付けられた SSID。
802.11 Type	クライアントで使用される 802.11 変種。
Frequency	クライアントで使用される周波数帯域。
Max Data Rate	クライアントで使用された最大データ レート。
Upload	クライアントでアップロードされたデータの量。
Download	クライアントでダウンロードされたデータの量。
Total	クライアントで送受信されたデータの総量。
First Seen	クライアントが最初に検出された時刻。
Last Seen	クライアントが最後に表示された時刻。
Time Online	クライアントがオンラインだった合計時間。
% Online Time	クライアントがネットワークで認識されていた合計時間内にクライアントがオフラインだった時間の割合。

表 *7:* ワイヤレスゲストテーブル

ワイヤレスゲストテーブル	
MAC	クライアントの MAC アドレス。
Hostname	クライアントのホスト名（使用可能な場合）。
Username	ゲストポータルにクライアントが入力したユーザ名。
Organization	クライアントで最後に表示された組織。
Network	クライアントで最後に表示されたネットワーク。
SSID	クライアントが最後に関連付けられた SSID。
802.11 Type	クライアントで使用される 802.11 変種。
Frequency	クライアントで使用される周波数帯域。
Max Data Rate	クライアントで使用された最大データレート。
Upload	クライアントでアップロードされたデータの量。
Download	クライアントでダウンロードされたデータの量。
Total	クライアントで送受信されたデータの総量。
First Seen	クライアントが最初に検出された時刻。
Last Seen	クライアントが最後に表示された時刻。
Time Online	クライアントがオンラインだった合計時間。

ワイヤレスゲストテーブル	
% Online Time	クライアントがネットワークで認識されていた合計時間内にクライアントがオフラインだった時間の割合。

（注） [First Seen] タイムスタンプと [Last Seen] タイムスタンプは、アクセスポイントによって報告された時刻です。Network Time Protocol（NTP）などのメカニズムを使用して、すべてのネットワークデバイスにクロック同期を実装することをお勧めします。



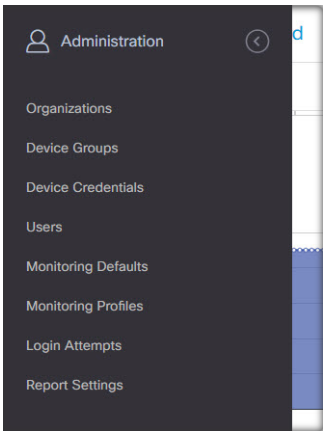
第 11 章

管理

この章は、次の項で構成されています。

管理について

Cisco Business ダッシュボード の [Administration] オプションを使用すると、組織レベルでアプリケーションの動作を制御できます。



このオプションは、次のページに分かれています。

- [Administration]：Cisco Business ダッシュボード に組織を作成し、管理します。

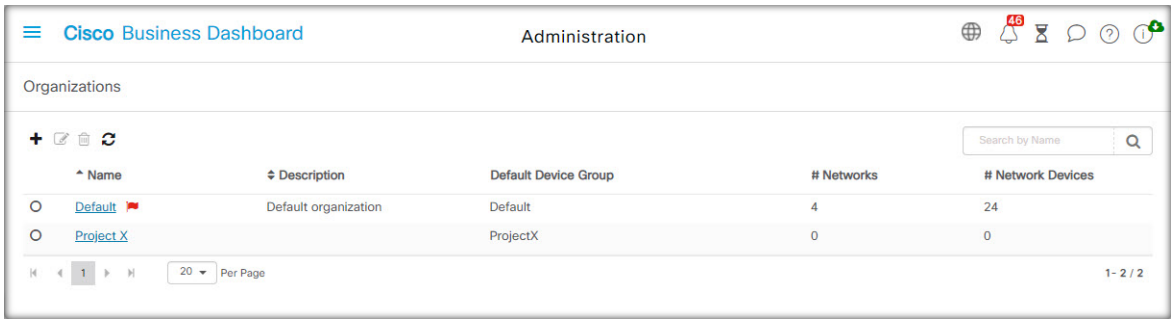
- [Device Groups]：ネットワークデバイスをグループに割り当てて、容易に管理できるようにします。
- [Device Credentials]：ネットワークデバイスにアクセスするときに使用するログイン情報を入力します。
- [Users]：Cisco Business ダッシュボード へのユーザアクセスを定義します。
- [Notification Defaults]：Cisco Business ダッシュボード のデフォルトの通知動作を変更します。
- [Notification Defaults]：Cisco Business ダッシュボード へのすべてのユーザアクセスのログを提供します。
- [Report Settings]：レポートの生成方法を制御する設定を変更します。

すべてのロールにすべてのページが表示されるわけではありません。オペレータはユーザ設定を管理できません。[Notification Defaults] と [Report Settings] は、管理者にのみ表示されます。

組織

組織は、ネットワーク、ユーザー、およびデバイスを、通常は個別に管理するグループに分割するために Cisco Business ダッシュボード で使用されます。各ネットワークまたはデバイスは 1 つの組織に属し、各ユーザーは 1 つ以上の組織を管理できます。組織は、顧客、部門または地域（会社にとって最も適切なもの）を表すことがありますが、どのような場合も、複数の組織を使用して、ネットワークのさまざまな部分を誰が表示し、管理できるかをより細かく制御できます。Cisco Business ダッシュボード のインストール時に、デフォルトと呼ばれる組織が 1 つ作成されます。

新しい組織を作成



1. **[Administration]** > **[Organizations]** に移動します。
2. テーブルの上部にある [+]（プラス）アイコンをクリックします。
3. 組織の名前を指定し、必要な詳細情報を入力します。
4. 新たに検出されたデバイスのデフォルトグループとして使用する必要がある新しいデバイスグループの名前を入力します。新しいデバイスグループが組織とともに作成されます。

5. 組織の変更期間の開始時刻と期間を指定します。
6. [Save] をクリックします。
7. 作成する組織ごとに上記の手順を繰り返します。

既存の組織を変更

1. **[Administration]** > **[Organizations]** に移動します。
2. 変更する組織のオプションボタンを選択し、[Edit] アイコンをクリックします。
3. 必要に応じて変更を加え、[Save] をクリックします。

組織の削除

1. **[Administration]** > **[Organizations]** に移動します。
2. 変更する組織のオプションボタンを選択し、[Deletion] アイコンをクリックします。

組織のモニタリングプロファイルを管理

モニタリングプロファイルを使用して、組織全体でのネットワーク デバイス モニタリングの実行方法を制御できます。組織レベルで選択されるプロファイルは、組織内のすべてのネットワークに適用されます。

組織のモニタリングプロファイルを変更するには、次の手順を実行します。

1. **[Administration]** > **[Organizations]** に移動します。
2. 変更する組織の名前をクリックし、[Monitoring Profiles] タブを選択します。
3. ドロップダウンを使用して、対応するタイプのデバイスに適用する適切なモニタリングプロファイルを選択します。モニタリングプロファイルの作成の詳細については、モニタリングプロファイル （106 ページ） を参照してください。

   また、個別のデバイスタイプまたは組織全体の [Inherit from Monitoring Defaults] チェックボックスをオンにして、システムレベルで定義されている動作に従うよう選択することもできます。
4. [Save] をクリックします。

（注） 実行可能なモニタリングのタイプとその管理方法の詳細については、「モニタリングプロファイル」を参照してください。システムレベルでのモニタリングプロファイルの変更に関する詳細については、モニタリングのデフォルト値（105ページ） を参照してください。

組織に関連付けられているユーザーを管理

組織管理者またはその下位のロールを持つユーザは、組織内のデバイスを表示または管理できるように、その組織に明示的に関連付ける必要があります。

ユーザーを組織に関連付けるには、以下の手順に従います。

1. **[Administration]** > **[Organizations]** に移動します。
2. 変更する組織の名前をクリックし、[Users] タブを選択します。
3. ✚（プラス）アイコンをクリックします。ドロップダウンリストからユーザーを選択します。

（注） [Administrator] レベルのユーザーは、すべての組織に暗黙的に関連付けられていて、ドロップダウンリストには表示されません。

組織からユーザーを削除するには、次の手順に従います。

1. **[Administration]** > **[Organizations]** に移動します。
2. 変更する組織の名前をクリックし、[Users] タブを選択します。
3. テーブル内のユーザの横にある [Delete] アイコンをクリックします。

組織に関連付けられているネットワークを管理

Cisco Business ダッシュボード 内のすべてのネットワークが単一の組織に属しています。[Organization Detail] ページの [Networks] タブを選択すると、組織に関連付けられているネットワークのリストを表示できます。

ネットワークと組織の関連付けは、ネットワークが最初に作成されたときに行われます。ネットワークが関連付けられている組織を変更するには、次の手順に従います。

1. [Network] に移動し、変更するネットワークを選択します。[More] をクリックして [Network Detail] パネルを表示します。
2. ネットワーク名の横にある [Edit] アイコンをクリックします。
3. ドロップダウンリストから新しい組織を選択します。
4. [OK] をクリックします。

このビューから、組織の新しいネットワークを作成できます。[+]（プラス）アイコンをクリックして新しいネットワークを作成し、表示されるフォームに適切な値を入力します。

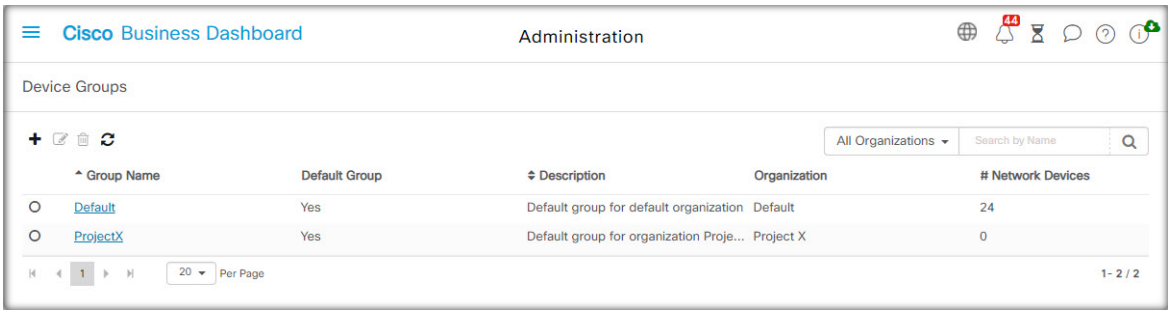
デバイスグループ

Cisco Business ダッシュボード は、ほとんどの設定タスクの実行にデバイスグループを使用します。複数のネットワークデバイスがグループ化されているため、デバイスのサブセットに対してのみ VLAN または WLAN を作成するなどの単一のアクションで構成できます。

各デバイス グループは複数の種類のデバイスを含むことができ、デバイス グループに設定が適用されると、その設定はグループ内のその機能をサポートするデバイスのみに適用されます。たとえば、デバイスグループにワイヤレスアクセスポイント、スイッチ、ルータが含まれている場合、新しいワイヤレス SSID の設定はワイヤレスアクセスポイントのみに適用され、ルータにはそれがワイヤレスルータである場合のみ適用されます。

デバイスグループには、複数のネットワークのデバイスが含まれている場合がありますが、すべてのデバイスが 1 つの組織に属している必要があります。デバイスグループは、組織またはネットワークのデフォルトのグループとして指定され、そのネットワークまたは組織で新たに検出されたデバイスがデフォルトのデバイスグループに配置されます。

デバイスグループの作成



1. **[Administration]** > **[Device Groups]** に移動します。
2. ✚（プラス）記号をクリックして新しいグループを作成します。
3. グループの組織、名前、および説明を入力します。[Save] をクリックします。
4. 必要に応じて、[+]（プラス）アイコンをクリックし、グループに追加するデバイスを検索ボックスを使用して選択し、デバイスをデバイス グループに追加します。デバイスは、個別に追加することも、ネットワーク別に追加することもできます。選択したデバイスがすでに別のグループのメンバーになっている場合は、そのグループから削除されます。各デバイスは、1 つのグループのみのメンバーになることができます。

デバイスグループの変更

1. **[Administration]** > **[Device Groups]** に移動します。
2. 変更するグループの横にあるオプション ボタンを選択し、[Edit] アイコンをクリックします。

3. 必要に応じて、名前と説明を変更します。[Save] をクリックします。
4. 必要に応じてデバイスをグループに追加または削除します。以前グループに追加したデバイスを削除するには、デバイスの横の**ゴミ箱**アイコンをクリックします。デバイスがネットワークまたは組織の [Default] グループに移動されます。

（注） [Default] グループからデバイスを削除することはできません。[Default] グループからデバイスを削除するには、デバイスを新しいグループに追加する必要があります。

デバイスグループの削除

1. **[Administration]** > **[Device Groups]** に移動します。
2. 削除するデバイスグループのオプションボタンをクリックし、[Delete] アイコンをクリックします。

（注） [Default] グループは削除できません。

デバイスのクレデンシャル

Cisco Business ダッシュボード がネットワークを完全に検出して管理するには、ネットワークデバイスで認証されるためのクレデンシャルが必要です。デバイスが最初に検出されたときに、Probe がデフォルトのユーザ名（cisco）、パスワード（cisco）、SNMP コミュニティ（public）を使用して、デバイスを認証しようとします。この試みに失敗すると通知が生成され、ユーザが有効なクレデンシャルを指定する必要があります。有効なログイン情報を提供するには、以下の手順に従ってください。

1. **[Administration]** > **[Device Credentials]** に移動します。このページの最初のテーブルには、クレデンシャルが必要な検出済みのすべてのデバイスのリストが表示されます。
2. [Username] / [Password] フィールド、[SNMP Community] フィールド、および [SNMPv3] クレデンシャル フィールドのいずれかまたはすべてに、有効なクレデンシャルを入力します。対応するフィールドの横の ✚（プラス）アイコンをクリックして、種類ごとのクレデンシャルを 3 つまで入力できます。パスワードがプレーンテキストを使用して入力されていることを確認します。

（注） [SNMPv3] クレデンシャルの場合、サポートされている認証プロトコルは None、MD5、および SHA であり、サポートされている暗号化プロトコルは None、DES、および AES です。

3. [Apply] をクリックします。Probe は各クレデンシャルを、その種類のクレデンシャルが必要な各デバイスに対してテストします。クレデンシャルが有効な場合、そのデバイスに対して後で使用するためにクレデンシャルが保存されます。
4. 必要に応じて、すべてのデバイスに有効なクレデンシャルが保存されるまで、手順 2 から 3 を繰り返します。

特定のデバイスの単一のクレデンシャルを入力するには、以下の手順に従います。

1. 検出済みデバイスのテーブル内のデバイスに対して表示されている [Edit] アイコンをクリックします。ポップアップが表示され、選択したクレデンシャルの種類に対応するクレデンシャルを入力するよう求められます。
2. ユーザ名とパスワードか、SNMP クレデンシャルをフィールドに入力します。
3. [Apply] をクリックします。適用せずにウィンドウを閉じるには、ポップアップの右上隅にある ✖ をクリックします。

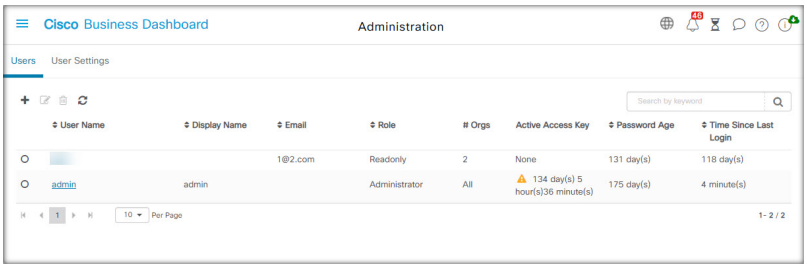
[Add New Credential] セクションの下には、Probe に有効なクレデンシャルが保存されている各デバイスの ID と、クレデンシャルが最後に使用された時刻を示す表が表示されます。保存されているデバイスのクレデンシャルを表示するには、デバイスの横にある [Show Password] アイコンをクリックします。クレデンシャルを再度非表示にするには、[Hide Password] ボタンをクリックします。また、デーブルの上部にあるボタンを使用すると、すべてのデバイスのクレデンシャルを表示したり、非表示にしたりできます。不要になったクレデンシャルを削除することもできます。保存されているクレデンシャルを削除するには、以下の手順に従います。

1. **[Administration]** > **[Device Credentials]** に移動します。
2. [Saved Credentials] 表で、削除する 1 つ以上のクレデンシャルのチェックボックスをオンにします。表の一番上にあるチェックボックスをオンにして、すべてのクレデンシャルを選択することもできます。
3. [Delete Selected Credentials] をクリックします。

また、1 台のデバイスのクレデンシャルを削除するには、そのデバイスの横にある [Delete] ボタンをクリックします。

ユーザー

[User Management] ページでは、ユーザーが Cisco Business ダッシュボードにアクセスする方法を制御したり、それらのユーザーとダッシュボードが通信する方法に影響する設定を変更したりすることができます。また、ユーザーベースのネットワーク認証を実行するときに、それらのユーザーにネットワークへのアクセスも許可するかどうかも制御できます。これは、ネットワークに対して新しいユーザーを追加または削除する必要がある場合に便利なツールです。



Cisco Business ダッシュボードには、[Dashboard Access] ドロップダウンリストを使用して利用可能なダッシュボード機能を制御する設定と、ユーザーベースのネットワークアクセス時にユーザーがネットワークにアクセスできるかどうかを制御する設定（[Network Access] チェックボックス）があります。これらの設定で使用できるオプションは次のとおりです。

- [Administrator]：管理者は、システムを保守する機能を含めて、Dashboard のすべての機能にアクセスできます。
- [Organization Administrator]：組織管理者は 1 つ以上の組織の管理に限定されていて、システムに変更を加えることはできません。
- [Operator]：オペレータは組織管理者と同様の権限を持ちますが、ユーザーを管理することはできません。
- [Readonly]：読み取り専用ユーザーは、ネットワーク情報を表示することはできますが、変更を加えることはできません。
- [No Access]：アクセス権なしのユーザーは、ダッシュボード機能を使用できません。ただし、ダッシュボードにログオンして自身のユーザープロファイルを管理することはできます。
- [Network Access]：この設定は、ユーザーベースのネットワークアクセスの使用時に、ユーザーがネットワークにアクセスできるかどうかを制御します。ダッシュボードアクセス設定が組織管理者以下に設定されている場合、ユーザーの組織リスト内の組織にのみアクセスが許可されます。

Cisco Business ダッシュボードを使用すると、ユーザがローカルユーザデータベースに対して認証されます。リリース 2.2.1 以降、ユーザは Microsoft Azure Active Directory インスタンスに対しても認証されます。

（注） ユーザーベースのネットワークアクセスの認証を実行する場合、ローカルユーザーのみがチェックされます。

Cisco Business ダッシュボードを最初にインストールすると、デフォルトの**管理者**ユーザが、ユーザ名とパスワードの両方が `cisco` に設定された状態でローカルユーザデータベースに作成されます。

（注） ユーザ設定は、**管理者**と**組織管理者**のみが管理できます。

ローカル ユーザー データベースに新しいユーザーを追加する

1. [Administration] > [Users] に移動し、[Users] タブを選択します。
2. ✚（プラス）アイコンをクリックして新しいユーザを作成します。
3. 各フィールドにユーザー名、表示名、電子メールアドレス、およびパスワードを入力し、ダッシュボードアクセスおよびネットワークアクセスの設定を指定します。また、ユーザの連絡先の詳細情報を入力することもできます。
4. [Save] をクリックします。

ユーザが**管理者**でない場合は、そのユーザを1つ以上の組織に追加する必要があります。これを行うには、[Organizations] タブを選択し、[+]（プラス）アイコンをクリックします。ドロップダウンリストから目的の組織を選択します。

ユーザーを変更

1. [Administration] > [Users] に移動し、[Users] タブを選択します。
2. 変更する必要があるユーザの横にあるオプションボタンを選択し、[Edit]アイコンをクリックします。
3. 必要に応じて変更を加えます。
4. [Save] をクリックします。

ユーザを新しい組織に追加するには、[Organizations] タブを選択し、[+]（プラス）アイコンをクリックします。ドロップダウンリストから目的の組織を選択します。組織から削除するには、テーブル内の組織の横にある [Delete] アイコンをクリックします。

ユーザーの削除

1. [Administration] > [Users] に移動し、[Users] タブを選択します。
2. 削除する必要があるユーザの横にあるオプションボタンを選択し、テーブルの上部にある [Delete] をクリックします。

パスワードの複雑さを変更

パスワードの複雑さの要件を有効または変更するには、次の手順に従います。

1. [Administration] > [Users] に移動し、[User Settings] タブを選択します。
2. [Authentication Source] の [Local] タブを選択し、必要に応じて [User Password Complexity] の設定を変更して、[Save] をクリックします。

（注） Azure Active Directory インスタンスに対して認証する場合、パスワードの複雑性は Active Directory で管理されます。

Azure Active Directory 認証を有効化

Cisco Business ダッシュボード は、Microsoft Azure Active Directory のインスタンスを使用したユーザ認証をサポートしています。Active Directory ユーザには、ユーザがメンバーになっている Active Directory グループに基づいてロールと組織リストが割り当てられます。

Azure Active Directory を認証ソースとして有効にするには、次の手順に従います。

1. **Azure Active Directory** で、Cisco Business ダッシュボード の新しいアプリケーション登録を作成し、**Microsoft Graph API** から User.Read および Domain.Read.All の委任権限を割り当て、**クライアントシークレット**を作成します。アプリケーション（クライアント）ID、クライアントシークレット、ディレクトリ（テナント）ID をメモします。
2. Cisco Business ダッシュボード Web GUI を開き、[Administration] > [Users] に移動します。[User Settings] タブを選択し、[Authentication Source] の [Azure AD] タブを選択します。
3. [Enable] チェックボックスをクリックします。
4. 手順 1 で収集した**クライアント ID**、**クライアントシークレット**、および**テナント ID** を所定のフィールドに入力します。
5. オプションで、ダッシュボードへのアクセスを許可するドメインのカンマ区切りリストを指定します。[Save] をクリックします。
6. [User Group Mappings] ヘッダーの下にある [+]（プラス）アイコンをクリックして、新しいグループマッピングを作成します。表示されたフィールドに Active Directory グループの**オブジェクト ID**を入力し、このグループのユーザに適用するロールと組織リストを選択します。マッピングする必要のあるすべてのグループに対してこの手順を繰り返します。

   ユーザーが複数のグループに一致する場合、最初に一致したロールと組織のマッピングが使用されます。
7. [Enable] チェックボックスの下に表示される**リダイレクト URL**をメモします。Azure Active Directory に戻り、メモした URL をアプリケーション登録用のリダイレクト URI のリストに追加します。

（注） リダイレクト URL に表示されるホストとポートは、ダッシュボードにアクセスするユーザの Web ブラウザから到達可能である必要があります。現在表示されている値に到達できない場合は、[System] > [Platform Settings] ページの [Systems Variables] タブの該当するフィールドを更新します。

ローカル認証を管理

ローカルユーザデータベースに対する認証は、デフォルトで有効になっています。ローカル認証を無効にするには、次の手順に従います。

1. Azure Active Directory に対する認証が上記のように設定されていることを確認します。Active Directory によって認証された管理者アカウントを使用してダッシュボードにログオンします。
2. [Administration] > [Users] に移動し、[User Settings] タブを選択します。[Authentication Source] で、[Local] タブを選択します。
3. [Enable] チェックボックスをオフにして、[Save] をクリックします。

ローカル認証を再度有効にするには、次の手順に従います。

1. **[Administration]** > **[Users]** に移動し、**[User Settings]** タブを選択します。[Authentication Source] で、[Local] タブを選択します。
2. [Enable] チェックボックスをオンにして、[Save] をクリックします。

すべての管理アクセスが失われた場合のアクセスを復元

Cisco Business ダッシュボード アプリケーションへの管理アクセスが失われた場合は、次の手順に従って同じアクセスを回復します。

1. SSH またはコンソールを使用して、ホスト オペレーティング システムにログオンします。
2. **cisco-business-dashboard recoverpassword** コマンドを入力します。

コマンドを入力すると、ローカルユーザ認証が有効になり、ユーザ名が **cisco** でパスワードが **cisco** のデフォルトの管理者が復元されます。

セッションタイムアウトを変更

ユーザーセッションのアイドルタイムアウトと絶対タイムアウトを変更するには、次の手順に従います。

1. [Administration] > [Users] に移動し、[User Settings] タブを選択します。
2. 必要に応じて、[User Settings] パラメータを変更し、[Save] をクリックします。ヘルプ アイコンにマウス オーバーするとこれらのパラメータの許容範囲が表示されます。

モニタリングのデフォルト値

モニタリングプロファイルを使用して、ネットワークで実行されるデバイスモニタリングを制御できます。モニタリングプロファイルは、組織レベルまたはシステムレベルで適用できます。システムレベルのモニタリングプロファイルの継承を選択した組織は、[Monitoring Defaults] ページで動作を制御します。

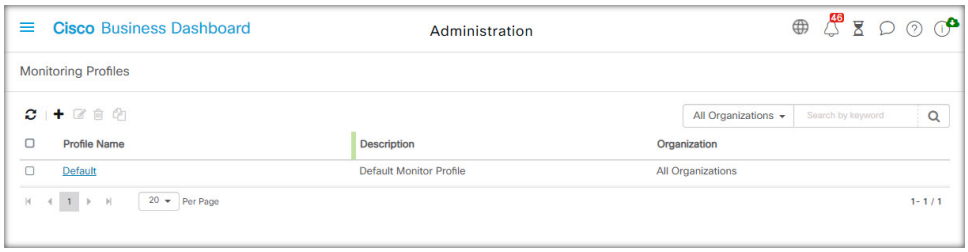
システム全体に適用される [Monitoring Profiles] を変更するには、以下の手順に従います。

1. **[Administration]** > **[Monitoring Defaults]** に移動します。
2. ドロップダウンを使用して、対応するタイプのデバイスに適用する適切なモニタリングプロファイルを選択します。モニタリングプロファイルの作成の詳細については、「モニタリングプロファイルの管理」を参照してください。
3. [Save] をクリックします。

実行可能なモニタリングのタイプとその設定方法の詳細については、「モニタリングプロファイル」を参照してください。組織レベルでのモニタリング設定の変更に関する詳細については、組織 （96 ページ） を参照してください。

モニタリングプロファイル

モニタリングプロファイルは、デバイスから収集されるデータと生成される通知を制御します。



プロファイルは、組織内またはシステム内のさまざまなタイプのデバイスに適用できます。たとえば、デバイスによっては、場所やセキュリティ要件に応じて異なる監視要件が必要になる場合があります。プロファイル内では、**通知モニタ**と**レポートモニタ**の 2 種類のモニタがサポートされています。

通知モニタは、通常、デバイスの状態の変化またはしきい値を超えるパラメータに起因して、通知およびアラートを生成します。通知には、情報、警告、およびアラートの重大度レベルがあり、次のチャネルで配信されます。

- Web UI のポップアップ通知。
- 電子メール。これには、電子メール設定が正しく設定されている必要があります。詳細については、電子メール設定の管理 （121 ページ）を参照してください。
- ヘルプデスクチケット。これには、ヘルプデスクサービスを提供するアプリケーションとの統合が必要です。詳細については、統合設定の管理 （135ページ）を参照してください。
- コラボレーションメッセージ。これには、コラボレーションアプリケーションとの統合が必要です。詳細については、統合設定の管理 （135 ページ）を参照してください。

（注） モニタリングプロファイルを設定して、チケットまたはコラボレーションメッセージの平均レートが 1 時間あたり 60 を超えないようにすることをお勧めします。外部アプリケーションと通信する場合、これを超えるレートが持続すると、API の輻輳とイベントの損失が発生する可能性があります。

アクティブな通知は [Notification Center] にも表示され、デバイス情報ビューにも表示されます。通知の変更も [Event Log] に記録されます。

レポートモニタは、監視ダッシュボードのワイヤレスレポートおよびトラフィックグラフで使用されるデータを収集します。

複数のモニタリングプロファイルを作成し、システムレベルで、または組織ごとに、異なるデバイスタイプに異なるプロファイルを割り当てることができます。プロファイルへのテンプレートの割り当てに関する詳細については、組織 （96 ページ） と モニタリングのデフォルト値 （105 ページ） を参照してください。

新しいモニタリングプロファイルを追加

1. **[Administration]** > **[Monitoring Profiles]** に移動します。
2. [+]（プラス）アイコンをクリックして新しいプロファイルを作成します。
3. プロファイルの名前と、プロファイルを関連付ける組織を指定します。ここで [All Organizations] を指定して、プロファイルを任意の組織で使用できるようにしたり、システムレベルのデフォルトとして使用したりすることもできます。
4. プロファイルの説明と、通知を受信する電子メールアドレスのカンマ区切りリストを指定することもできます。
5. [Save] をクリックします。
6. 画面が更新され、さまざまな通知モニタとレポートモニタが表示されます。用意されているコントロールを使用して、個々のモニターを有効または無効にすることができます。
7. 通知モニターには、[Edit] アイコンをクリックして変更できる追加の設定があります。設定はモニタによって異なりますが、生成される通知タイプ、通知のシビラティ（重大度）、通知をトリガーするしきい値が含まれます。

既存のモニタリングプロファイルをコピー

既存のモニタリングプロファイルをコピーするには、以下の手順に従います。

1. [Administration] > [Monitoring Profiles] に移動します。
2. コピーするプロファイルの横にあるチェックボックスを選択し、[Save As] アイコンをクリックします。
3. 必要に応じてプロファイル名、説明、組織、電子メールアドレスを更新してから、[Save] をクリックします。

4. 必要に応じて、通知モニタとレポートモニタを変更します。[Reset to defaults] ボタンをクリックすると、モニター設定をデフォルトに戻すことができます。

モニタリングプロファイルを変更

既存のモニタリングプロファイルを変更するには、以下の手順に従います。

1. [Administration] > [Monitoring Profiles] に移動します。
2. コピーするプロファイルの横にあるチェックボックスを選択し、[Edit] アイコンをクリックします。
3. 必要に応じてプロファイル設定と電子メールアドレスを更新してから、[Save] をクリックします。
4. 必要に応じて、通知モニタとレポートモニタを変更します。[Reset to defaults] ボタンをクリックすると、モニター設定をデフォルトに戻すことができます。

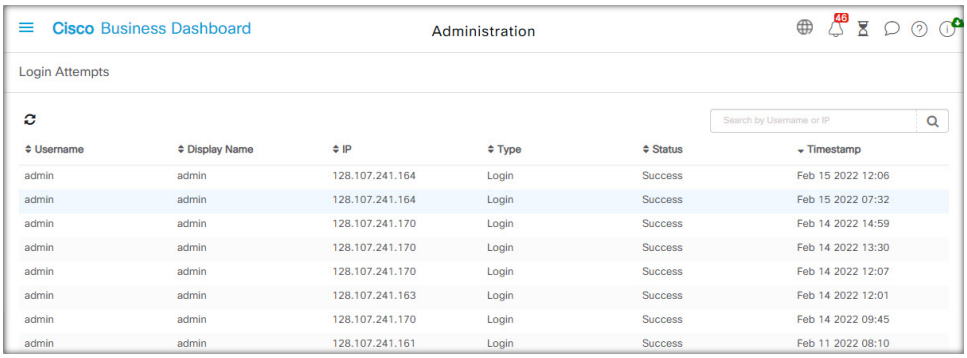
モニタリングプロファイルを削除

1. [Administration] > [Monitoring Profiles] に移動します。
2. コピーするプロファイルの横にあるチェックボックスをオンにして、[Delete] アイコンをクリックします。

（注） プロファイルが組織レベルのモニタリングプロファイルとして使用されている場合は、対応する組織とデバイスタイプがシステムレベルの設定を継承するように更新されます。システムレベルのモニタリングプロファイルとして使用されているプロファイルは削除できません。プロファイルを削除する前に、そのプロファイルを [Administration] > [Monitoring Defaults] ページから削除します。

ログイン試行の表示

Cisco Business ダッシュボードは、システムへのログインとシステムからのログアウトが成功したか失敗したかを記録します。



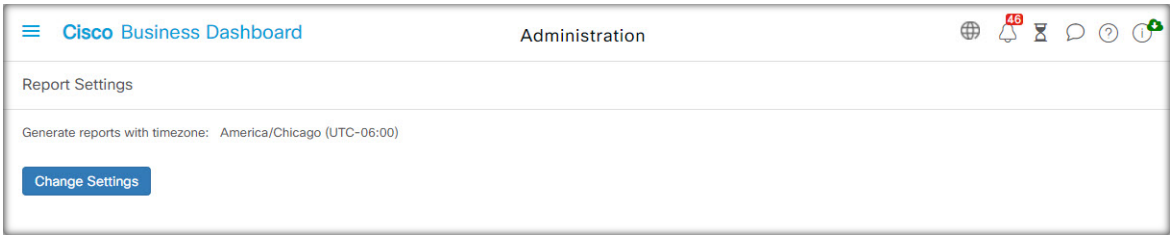
ログを表示するには、[Administration] > [Login Attempts] に移動します。テーブルに表示される情報は次のとおりです。

フィールド	説明
Username	イベントに関連付けられているユーザ名。
Display Name	ユーザの表示名。
IP	ユーザのログイン元であるデバイスの IP アドレス。
Type	イベントのタイプ。次の項目があります。 • LOGIN • LOGOUT
Status	試行が成功したか失敗したかを示します。
Timestamp	イベントが発生した日時。

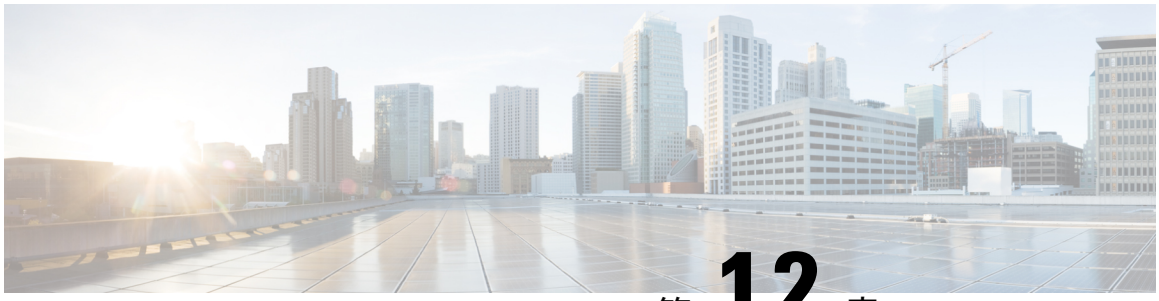
テーブルの上の検索ボックスを使用すると、特定のユーザまたは IP アドレスに一致するエントリのみを表示できます。

レポート設定の管理

[Report Settings] ページを使用し、レポートを生成するタイムゾーンを設定できます。



レポート期間の開始時間と終了時間は、設定したタイムゾーンの現地時間になります。



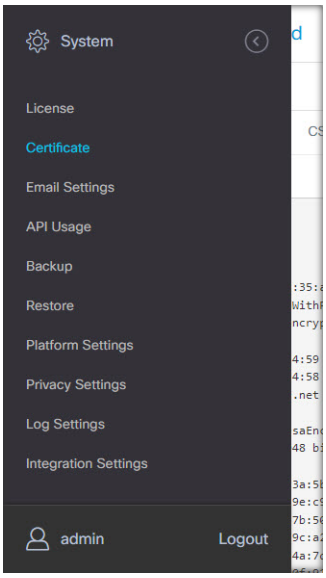
第 12 章

システム

この章は、次の項で構成されています。

システムについて

Cisco Business ダッシュボード の [System] オプションを使用すると、プラットフォームの動作を管理できます。



このセクションは、次のページに分かれています。

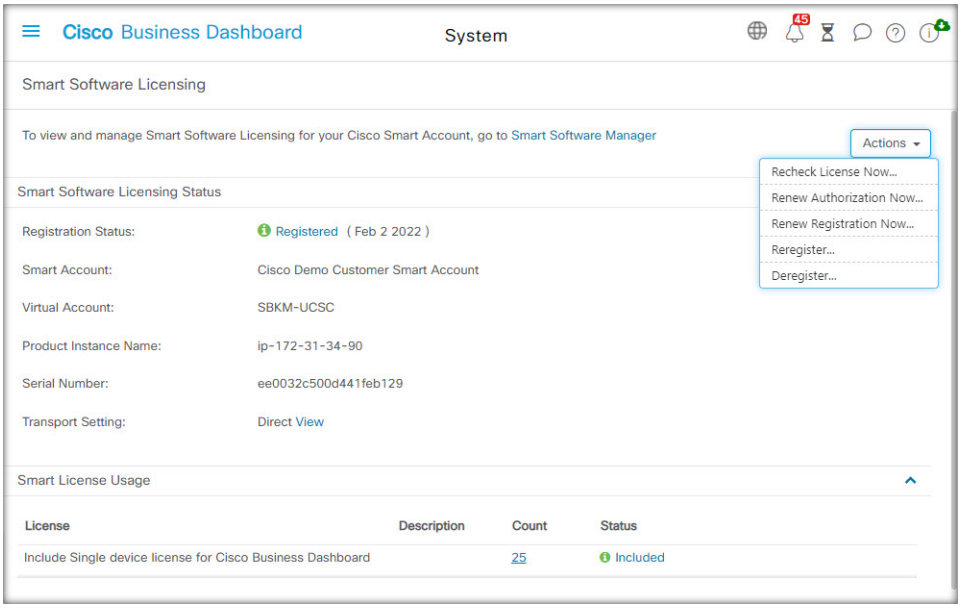
ページ名	ページ機能
ライセンス（License）	Dashboard のソフトウェアライセンスを管理します。
証明書（Certificate）	Dashboard でセキュリティ証明書を管理します。
電子メール設定（Email Settings）	電子メールを設定し、設定を管理します。
API の使用状況（API Usage）	Cisco Business ダッシュボード API の使用状況を監視します。
バックアップ（Backup）	Dashboard 用の設定とその他のデータをバックアップします。
Restore（復元）	Dashboard 用の設定とその他のデータを復元します。
プラットフォームの設定（Platform Settings）	Dashboard のネットワーク設定を管理します。
プライバシー設定（Privacy Settings）	シスコと共有できるデータを制御します。
ログ設定（Log Settings）	Dashboard のログ設定を変更します。
ローカルプローブ（Local Probe）	Dashboard にホストされた Probe を管理します。
統合設定（Integration Settings）	Cisco Business Dashboard と外部アプリケーションの統合を管理します。

（注） これらのページは、**管理者**のみが使用できます。

ライセンスの管理

（注） このページは、Cisco Business ダッシュボード for AWS の従量制課金バージョンには表示されません。

[License] ページでは、ネットワークで必要なライセンスの数とタイプを確認すること、および **Dashboard** を Cisco Smart Licensing システムに接続することができます。デバイス数が 25 以下の場合、追加のライセンスは必要ありません。このページには、次の 2 つの情報パネルがあります。



- **スマート ソフトウェア ライセンシングのステータス**

  このパネルには、スマート ライセンス クライアントの登録状態と使用中のスマートアカウントに関する情報が表示されます。

- **スマート ライセンスの使用状況**

  このパネルには、ネットワークの現在の状態に基づいて必要なライセンスの数と種類が一覧表示されます。この情報は、ネットワークが変更されると自動的に更新されます。また、Dashboard でスマートアカウントから要求されるライセンスの数が更新されます。[Status] フィールドにより、必要な数のライセンスが正常に取得されたかどうかが示されます。

また、このページには、スマートアカウントに対して Dashboard を登録および登録解除するためのコントロールも含まれます。

Dashboard がネットワークを管理するための十分なライセンスを取得できない場合、Dashboard は評価モードで実行され、Dashboard のユーザインターフェイスのヘッダーにメッセージが表示されます。評価モードで実行する場合、状況を改善するための猶予期間は 90 日です。90 日以内に問題が解決されない場合、問題が解決されるまで Dashboard の一部の機能が制限されます。問題を解決するには、追加ライセンスを取得するか、管理対象デバイスの数を減らす必要があります。

スマートアカウントへの Dashboard の登録

Dashboard をスマートアカウントに登録するには、次の手順に従います。

1. *https://software.cisco.com* にあるスマート アカウントにログオンします。

   [License] セクションの下にある [Smart Software Licensing] リンクを選択します。

2. [Inventory] ページを選択し、必要に応じて、選択した仮想アカウントをデフォルトから変更します。
3. [General] タブをクリックします。
4. [New Token…] ボタンをクリックして、新しい**製品インスタンス登録トークン**を作成します。オプションで、説明を追加し、[Expire After] の時間を変更します。
5. [Create Token] をクリックします。
6. トークンの右にある [Actions] ドロップダウンから [Copy] を選択して、新しく作成したトークンをクリップボードにコピーします。
7. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
8. [Register] ボタンをクリックし、表示されるフィールドにトークンを貼り付けます。
9. [OK] をクリックします。

Dashboard が Cisco Smart Licensing に登録され、管理対象ネットワークデバイスの数に見合う十分なライセンスが要求されます。使用可能なライセンスが不十分である場合、ユーザインターフェイスにメッセージが表示され、十分なライセンスを取得するための 90 日の期間が与えられます。この期間が経過すると、システムの機能が制限されます。

スマートアカウントから Dashboard を削除

スマートアカウントから Dashboard を削除し、割り当てられたライセンスをプールに戻すには、次の手順に従います。

1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。

2. 右上にあるドロップダウンリストから [Deregister…] を選択します。ポップアップで [Deregister] をクリックして確定します。

ライセンスを今すぐ確認

Cisco Business ダッシュボードは、毎日チェックを実行して、ネットワークに対して使用できる十分なライセンスがその時点で存在するかどうか確認し、必要なライセンスの数が減少している場合にはただちに更新を行います。ただし、必要なライセンスの数が増加している場合、またはプールに対してライセンスが追加または削除された場合、Dashboard が更新されるまでに最大で 1 日かかる場合があります。Dashboard にライセンス割り当てをすぐに更新させるには、以下の手順に従います。

1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
2. 右上のドロップダウンリストから [ReCheck License Now…] を選択します。 Cisco Business ダッシュボードは Cisco Smart Licensing にただちに問い合わせて、Dashboard の稼働に使用できる十分なライセンスがあるかどうか確認します。

認証を今すぐ更新

[Renew Registration Now] アクションを使用すると、Dashboardは Cisco Smart Licensing との通信を認証するために使用される証明書を更新します。通常、これは、拡張された通信の停止を回避する場合に、シスコ サポートの要求でのみ必要になります。登録を更新するには、以下の手順に従います。

1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
2. 右上にあるドロップダウンリストから [Renew Authorization Now…] を選択します。

登録を今すぐ更新

[Renew Registration Now] アクションを使用すると、Manager は Cisco Smart Licensing との通信を認証するために使用される証明書を更新します。通常、これは、拡張された通信の停止を回避する場合に、シスコ サポートの要求でのみ必要になります。登録を更新するには、以下の手順に従います。

1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
2. 右上にあるドロップダウンリストから [Renew Registration Now…] を選択します。

異なるアカウントへの Dashboard の移動

Dashboard を再登録すると、一方の仮想アカウントから別の仮想アカウントに Dashboard を移動できます。アカウント間で Dashboard を移動するには、以下の手順に従います。

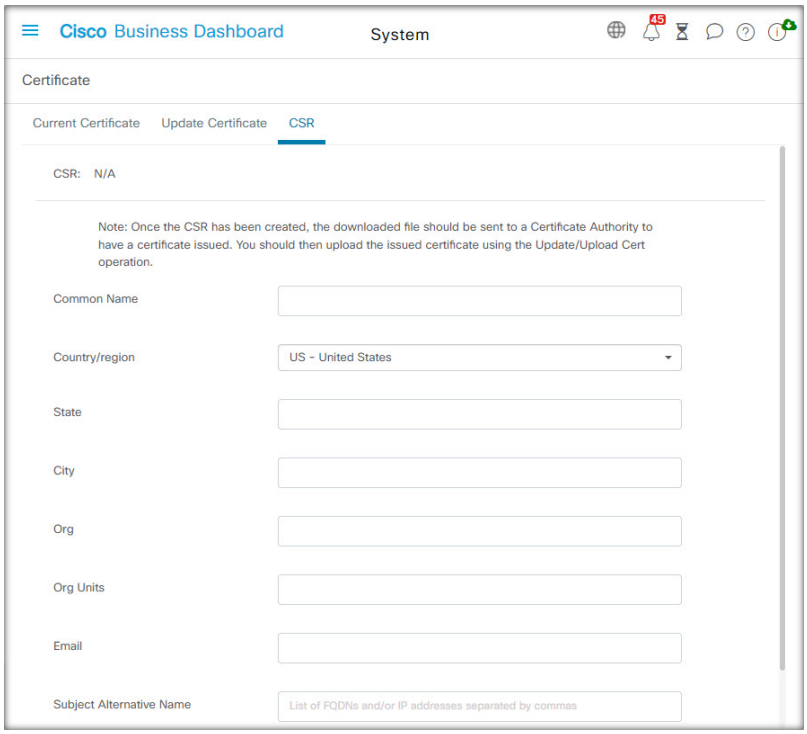
1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
2. 右上にあるドロップダウンリストから [Reregister...] を選択します。
3. 表示されるボックスに新しい登録トークンを入力します。Dashboard が別のアカウントに現在登録されている場合、[Reregister this product instance if it is already registered] チェックボックスが選択されていることを確認し、[OK] をクリックします。

証明書の管理

Cisco Business ダッシュボード のインストール時に、サーバとの Web 通信その他の通信を保護するために自己署名証明書が生成されます。この証明書は、信頼される認証局（CA）が署名した証明書に置き換えることができます。これを行うには、CA による署名のための証明書署名要求（CSR）を生成する必要があります。

また、Dashboard とは完全に独立した証明書と対応する秘密キーを生成することもできます。これを行う場合、アップロードの前に、証明書とプライベート キーを PKCS#12 形式のファイルに結合することができます。

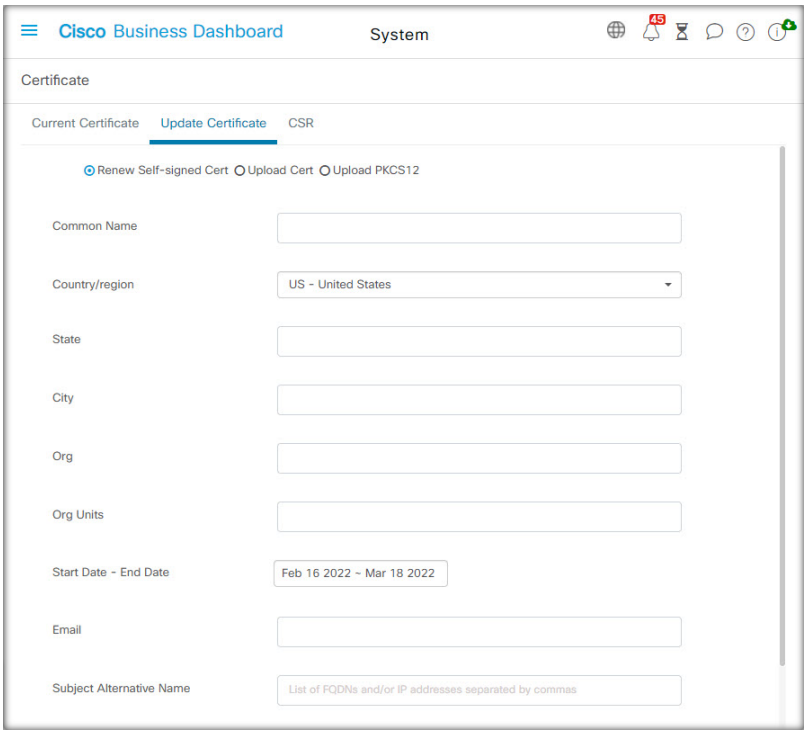
証明書署名要求（CSR）の生成



1. **[System]** > **[Certificate]** に移動し、[CSR] タブを選択します。

2. 表示されるフォームにあるフィールドに適切な値を入力します。これらの値は、CSR を生成するために使用され、CA から受信する署名証明書に組み込まれます。
3. [Create] をクリックします。これにより、CSR が PC に自動的にダウンロードされます。また、CSR ラベルの横にある [Download] をクリックすることで、後日 CSR をダウンロードすることもできます。
4. 必要に応じて手順 2 に戻ることで、CSR を変更できます。

新しい証明書をアップロード



管理 GUI を使用して新しい証明書をアップロードするには、以下の手順に従います。

1. **[System]** > **[Certificate]** に移動し、[Update Certificate] タブを選択します。
2. [Upload Cert] オプション ボタンを選択します。証明書を含むファイルはターゲット領域で廃棄してかまいません。また、ターゲット領域をクリックすると、ファイルシステムをブラウズできます。ファイルは PEM 形式でなければなりません。

   また、代わりに [Upload PKCS12] オプションを選択することで、PKCS#12 形式で証明書と関連するプライベート キーをアップロードできます。用意されているフィールドに、ファイルをロック解除するためのパスワードを指定する必要があります。
3. [Upload] をクリックしてファイルをアップロードし、現在の証明書を置き換えます。

コマンドラインを使用して新しい証明書をアップロードするには、次の手順を実行します。

1. SCP などを使用して、証明書と秘密キーファイルを Cisco Business Dashboard ファイルシステムにコピーします。秘密キーは機密情報であるため、これらのファイルへのアクセスは、承認された担当者のみに制限してください。
2. コンソールまたは SSH を使用して、オペレーティングシステムにログオンします。
3. コマンド **cisco-business-dashboard importcert -t pem -k <private key file> -c <certificate file>** を使用して、ダッシュボードアプリケーションに証明書を適用します。証明書と秘密キーがダッシュボードアプリケーションにロードされ、現在の証明書が新しいものに置き換えられます。このコマンドとそのオプションの詳細については、**cisco-business-dashboard importcert -h** と入力してください。

（注） 一部のブラウザでは既知の認証局によって署名された証明書に証明書の警告が生成される場合がありますが、他のブラウザでは警告なしに証明書が受け入れられる場合もあります。ネットワーク プラグアンドプレイ クライアントも証明書の受け入れに失敗する場合があります。これは、認証局がブラウザまたは PnP クライアントの信頼された認証局ストアに含まれていない中間証明書を使用して証明書に署名しているためです。このような状況では、認証局は、Dashboard にアップロードする前にサーバ証明書と連結させる必要のある一連の証明書を提供します。サーバ証明書は、連結されたバンドルの最初に表示する必要があります。

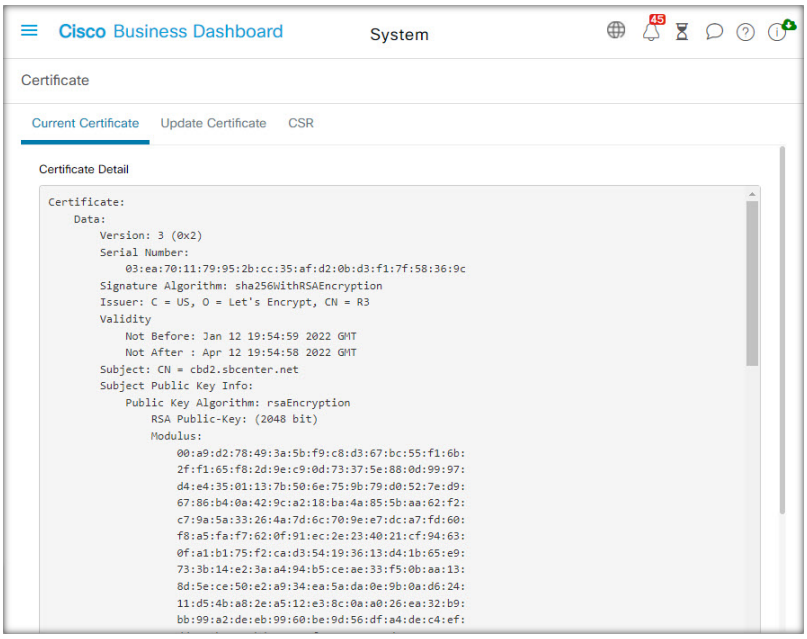
自己署名証明書を再生成

自己署名証明書を再生成するには、以下の手順に従います。

1. **[System]** > **[Certificate]** に移動し、[Update Certificate] タブを選択します。
2. [Renew Self-Signed Cert] をクリックします。表示されるフォームにあるフィールドに適切な値を入力します。これらの値は、証明書の作成に使用されます。
3. [Save] をクリックします。

現在の証明書を表示

現在の証明書を表示するには、次の手順に従います。



1. **[System]** > **[Certificate]** に移動し、[Current Certificate] タブを選択します。
2. 証明書がプレーン テキスト形式でブラウザに表示されます。

現在の証明書のダウンロード

現在の証明書のコピーをダウンロードするには、次の手順に従います。

1. **[System]** > **[Certificate]** に移動し、[Current Certificate] タブを選択します。
2. ページ下部にある [Download] をクリックします。証明書がブラウザにより PEM 形式でダウンロードされます。

Let's Encrypt からの証明書の自動インストール

リリース 2.2.1 以降、Cisco Business Dashboard は、**Let's Encrypt Certificate Authority**（https://letsencrypt.org/ja/）からドメイン検証済み証明書を自動的に取得して更新できるようになり、リリース 2.5.0 では、これらの証明書を管理ページから管理することができます。

重要 登録済みの完全修飾ドメイン名と、パブリック IP アドレスを指す DNS レコードが必要です。詳細については、プラットフォーム設定の管理（126 ページ）を参照してください。

管理 GUI を使用して Let’s Encrypt 証明書をインストールするには、次の手順を実行します。

1. **[System]** > **[Certificate]** に移動し、[Update Certificate] タブを選択します。
2. [Let’s Encrypt Certificate] オプションボタンを選択します。
3. チェックボックスをオンにすると、Let's Encrypt 証明書の使用が有効になります。

4. 提示されたフィールドに 1 つ以上の完全修飾ドメイン名を入力します。名前はドメインネームシステム（DNS）で定義され、Cisco Business Dashboard サーバーのアドレスに解決される必要があります。
5. 緊急の更新およびセキュリティ通知に使用する電子メールアドレスを指定します。
6. 提示されたリンクを使用して Let's Encrypt 利用規約を確認し、チェックボックスをオンにして利用規約に同意します。
7. 必要に応じて、電子メールアドレスを電子フロンティア財団（https://www.eff.org）と共有するためのチェックボックスをオンにします。
8. [Get Certificate] ボタンをクリックします。

ダッシュボードが Let's Encrypt 認証局に接続され、HTTP 検証方法を使用して証明書が取得されます。ページが更新され、証明書の詳細が有効期限とともに表示されます。証明書は、有効期限の約 30 日前に自動的に更新されます。

任意の時点で証明書を更新する必要がある場合は、次の手順に従います。

1. **[System]** > **[Certificate]** に移動し、[Update Certificate] タブを選択します。
2. [Let’s Encrypt Certificate] オプションボタンを選択します。
3. 提示されているチェックボックスとフィールドを使用して、証明書に適用する名前を更新します。

   または、画面の下部で連絡先の詳細を更新できます。
4. [Get Certificate] ボタンをクリックします。

ページのフィールドを変更せず、[Force Renewal] ボタンをクリックすることで、通常の更新時間の前に証明書を強制的に再生成することもできます。

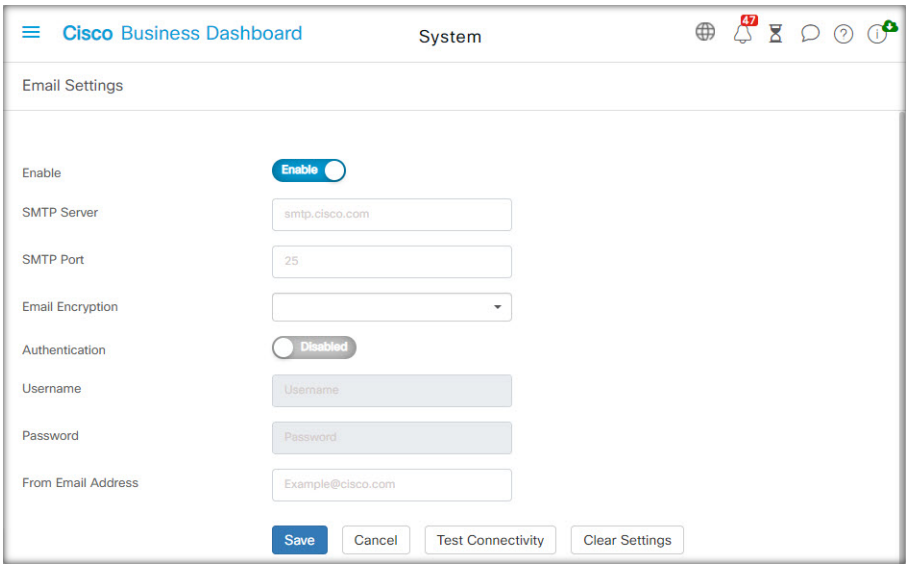
コマンドラインを使用して Let's Encrypt 証明書をインストールするには、次の手順を実行します。

1. SSH またはコンソールを使用して、ホストオペレーティングシステムにログオンします。
2. **cisco-business-dashboard letsencrypt** コマンドを実行し、**-d** オプションを使用して 1 つ以上の完全修飾ホスト名を指定します。（たとえば、**cisco-business-dashboard letsencrypt -d dashboard.example.com -d pnpserver.example.com** のように指定します。）コマンドに表示されるすべての名前は、ダッシュボードサーバの IP アドレスに解決される必要があります。
3. プロンプトに従って証明書を発行し、ダッシュボードアプリケーションに適用します。証明書は、有効期限が近づくとダッシュボードによって自動的に更新されます。

（注） **Let's Encrypt** サービスは、ダッシュボード Web サーバに接続してホスト名の所有権を確認する必要があります。これを可能にするには、ダッシュボードWebサーバーにインターネットからアクセスできる必要があります。ダッシュボードアプリケーションへのアクセスを許可された IP アドレスのみに制限する方法の詳細については、プラットフォーム設定の管理 （126 ページ） を参照してください。

電子メール設定の管理

[Email Settings] ページでは、電子メールが Cisco Business ダッシュボード によって送信される方法を制御できます。



このページにアクセスして、以下のパラメータを設定してください。

フィールド	説明
SMTP Server	使用する SMTP サーバのドメイン名または IP アドレス。
SMTP Port	メールを送信するために使用される TCP ポート。
Email Encryption	使用する暗号化方式には、次のものが含まれます。 • なし • TLS • SSL
Authentication	電子メール認証を有効または無効にします。

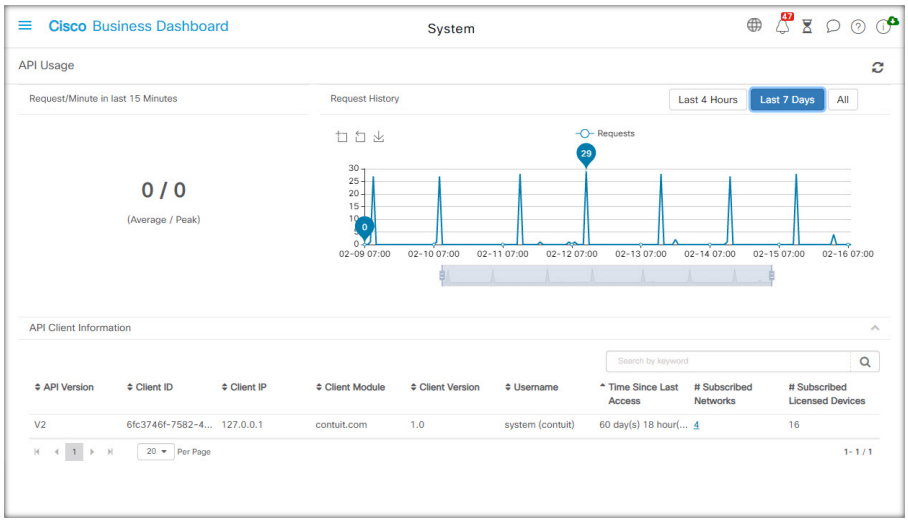
フィールド	説明
Username	認証が有効な場合に提示するユーザ名。
Password	認証が有効な場合に提示するパスワード。
From Email Address	メッセージの送信元の電子メール アドレス。

設定をテストするには、[Test Connectivity] をクリックします。これにより、ターゲットの電子メールアドレスの入力が要求され、指定されたアドレスにテスト用の電子メールが生成されます。

API 使用状況の表示

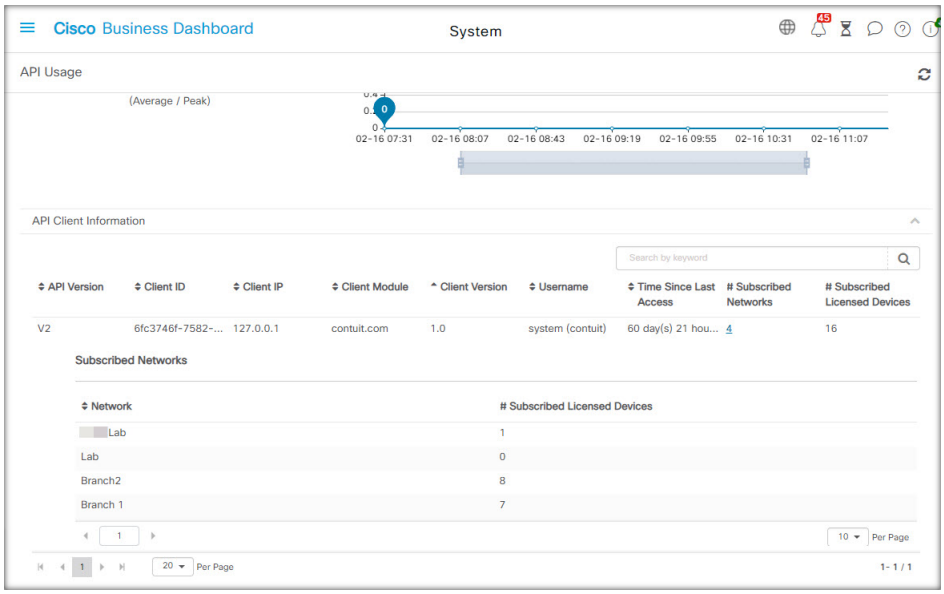
[API Usage] ページには、Cisco Business ダッシュボード と統合されているすべての外部アプリケーションに関する情報が表示されます。このレポートは次の 3 つのセクションに分かれています。

- [15-minute Request Monitor]：過去 15 分間の平均要求レートとピーク要求レートを表示します。
- [Request History] グラフ：時間の経過に伴う要求アクティビティのグラフを表示します。過去 4 時間、過去 7 日間、または使用可能なすべての情報の期間を選択できます。次に、グラフの下にあるスライダを使用して、グラフのフォーカスを特定の対象期間に絞り込むことができます。
- [API Client Information] テーブル：API を 1 回以上使用したすべてのクライアントのリストが表示されます。次の表で、[API Client Information] テーブルに表示される情報について説明します。



フィールド	説明
API Version	API にアクセスするときにクライアントが使用するバージョン。
Client ID	クライアント アプリケーションの特定のインスタンスの識別子。
Client IP	このクライアントに関連付けられている IP アドレス。また、API バージョンが v1 で通知が要求されたときに、Dashboard がイベント通知をポストする必要があるコールバック URL も表示されます。
Client Module	このクライアントに関連付けられているアプリケーションのタイプ。
Client Version	このクライアントに関連付けられているアプリケーションのバージョン。
Username	v1 API を使用するクライアントの場合、このフィールドには、Dashboard への認証時にアプリケーションによって提示されたユーザ名が表示されます。v2 API を使用するクライアントの場合、このフィールドには、クライアントが使用する**アクセス キー ID**と、キーが関連付けられているユーザ名が表示されます。
Time Since Last Access	このクライアントからの最後のアクティビティ以降の時間。
# Subscribed Networks	アプリケーションがイベント通知を要求したネットワークの数。この数値は、クリックすると、このクライアントの登録済みネットワークテーブルを表示するリンクです。次に、登録済みネットワークのテーブルについて説明します。
# Subscribed Licensed Devices	このクライアントにイベント通知を送信する管理対象デバイスの数。

クライアントが通知を要求したネットワークに関する情報を表示するには、[API Client Information] テーブルにあるクライアントの [# Subscribed Networks] リンクをクリックします。クライアントが通知を要求したネットワークのリストが含まれているクライアントの [Subscribed Networks] テーブルが表示されます。次のテーブルに、[Subscribed Networks] テーブルに表示される情報について説明します。



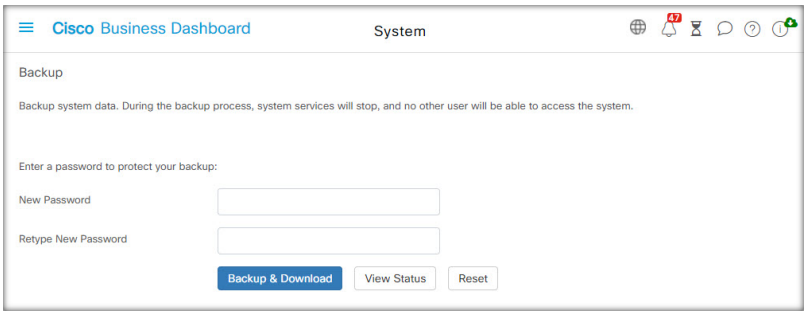
フィールド	説明
Network	クライアントによって監視されているネットワークの名前。
# Subscribed Licensed Devices	イベント通知を送信するこのネットワーク内の管理対象デバイスの数。

Dashboard 設定のバックアップと復元

ディザスタリカバリのために、または Dashboard を新しいホストに容易に移行するために、Cisco Business ダッシュボードが使用する設定などのデータをバックアップできます。機密データを保護するため、バックアップはパスワードで暗号化されます。

Cisco Business ダッシュボードバックアップファイルは、バックアップされたシステムと同じバージョンを実行しているシステム、または最大1つの新しいマイナーリリースを実行しているシステムに復元できます。たとえば、バージョン 2.2.0 を実行しているシステムから作成されたバックアップは、2.3.1 を実行しているシステムには復元できますが、2.4.0 を実行しているシステムには復元できません。

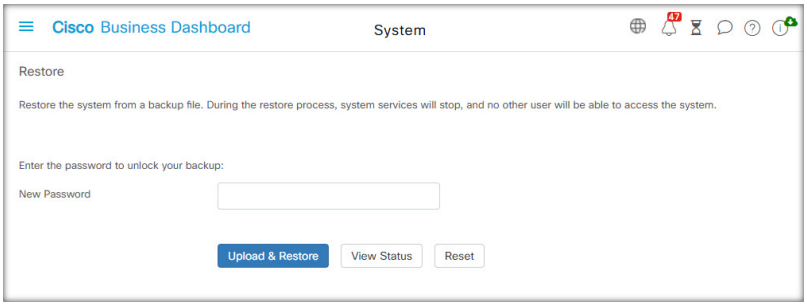
バックアップを実行するには、以下の手順に従います。



1. **[System]** > **[Backup]** に移動します。
2. バックアップを暗号化するためのパスワードを、[Password] および [Confirm Password] フィールドに入力します。
3. [Backup & Download] をクリックします。ポップアップウィンドウが表示され、バックアップの進行状況が表示されます。大規模なシステムでは、バックアップの完了までに時間がかかる可能性があるため、進行状況メーターを非表示にし、後で [View Status] アイコンを使用して再度表示こともできます。

完了すると、バックアップ ファイルが PC にダウンロードされます。

構成のバックアップを Dashboard に復元するには、以下の手順に従います。



1. **[System]** > **[Restore]** に移動します。
2. バックアップを暗号化するために使用したパスワードを、[Restore] フィールドに入力します。
3. [Upload & Restore] をクリックして続行します。ポップアップが表示され、PC からバックアップファイルをアップロードできるようになります。用意されたターゲット領域にバックアップファイルをドラッグアンドドロップするか、ターゲット領域をクリックして、PC のファイルシステム内のファイルを指定できます。[Restore] をクリックして続行します。

ダッシュボードのバージョンが 2.5.0 以降の場合、復元プロセスが完了するとアプリケーションが再起動します。

プラットフォーム設定の管理

[Platform Settings] ページでは、オペレーティングシステムに直接アクセスせずに主要なシステム設定を変更できます。Cisco Business ダッシュボードによってサポートされるプラットフォームにはさまざまな種類があるため、すべてのプラットフォームですべての設定を使用できるわけではありません。

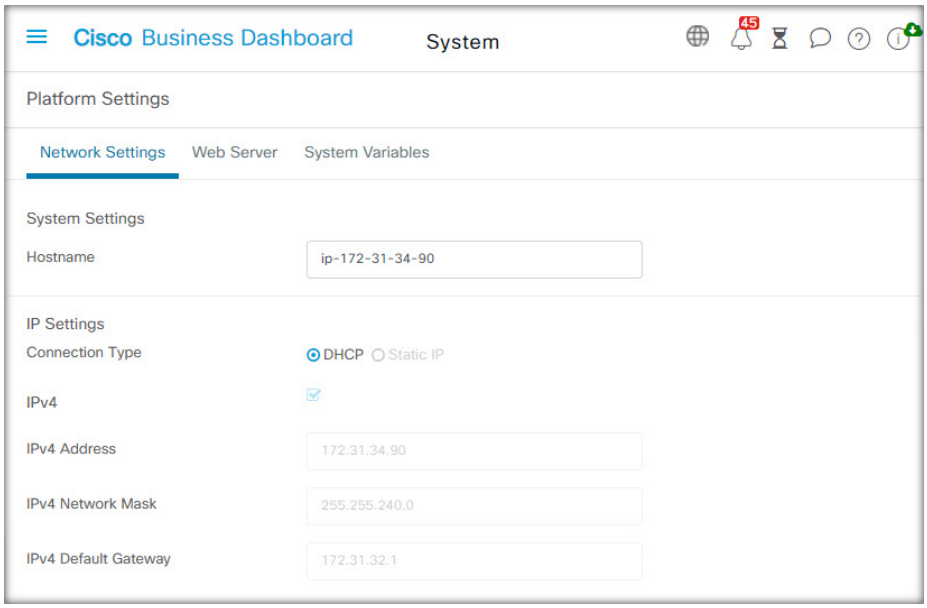
プラットフォーム設定は 3 つのグループに分かれています

- ネットワーク設定
- ウェブ サーバ
- システム変数

以下のセクションでは、各タブで実行可能な設定について説明します。

ホスト名の変更（[Network Settings] タブ）

ホスト名は、オペレーティングシステムがシステムを特定するために使用する名前で、Bonjour アドバタイズメントを生成する際、Cisco Business ダッシュボード が Dashboard を特定するために使用されます。

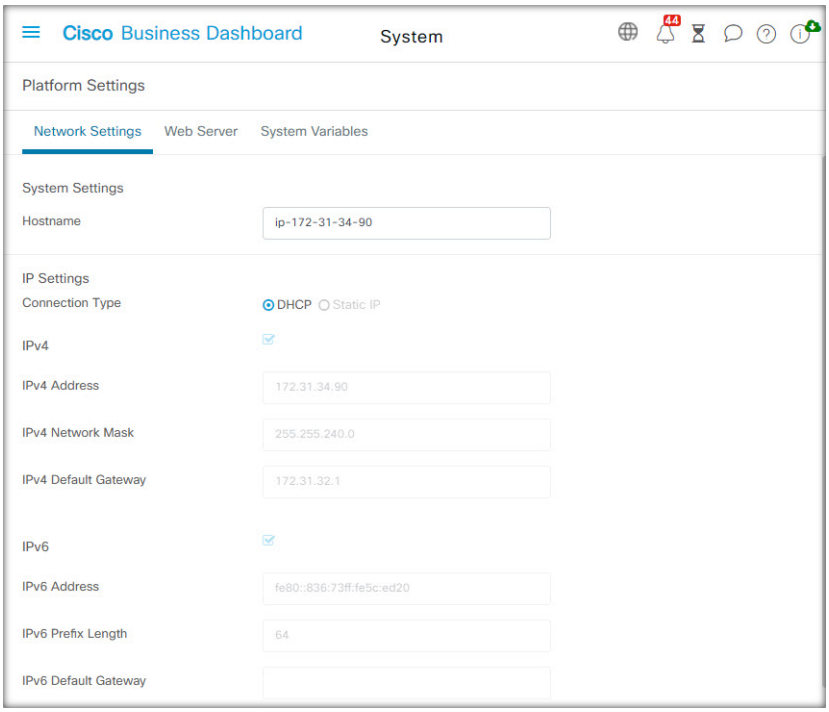


Dashboard のホスト名を変更するには、以下の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[Network Settings] タブを選択します。
2. 表示されたフィールドで、Dashboard のホスト名を指定します。
3. [Save] をクリックします。

ネットワーク設定の変更（[Network Settings] タブ）

（注） これは、AWS または Azure 用の Cisco Business ダッシュボードには適用されません。ネットワーク構成を変更するには、AWS インスタンスの場合は AWS の EC2 コンソールを使用し、Azure インスタンスの場合は Azure ポータルを使用します。

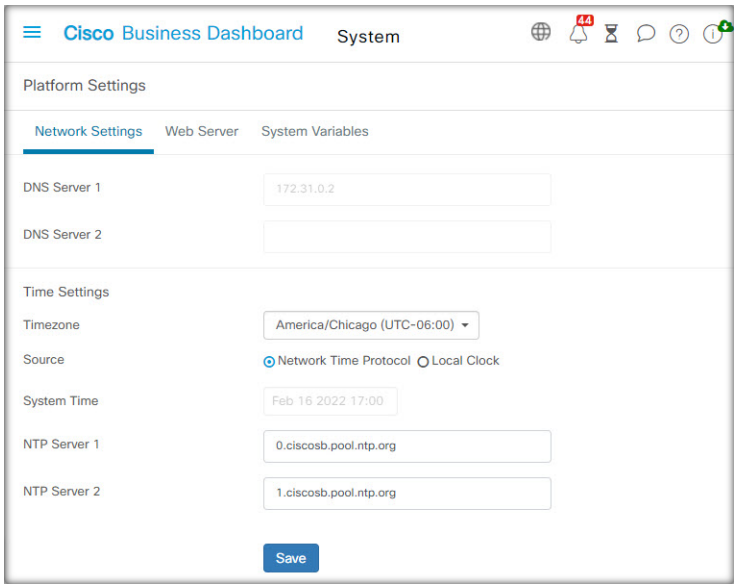


Dashboard のネットワーク構成を変更するには、以下の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[Network Settings] タブを選択します。
2. IP アドレスの割り当て方法を選択します。指定可能なオプションは、[DHCP]（デフォルト）と [Static IP] です。[Static IP] オプションを選択する場合は、アドレス、サブネット マスク、デフォルト ゲートウェイ、DNS サーバを適切なフィールドに指定します。
3. [Save] をクリックします。

時刻設定の変更（[Network Settings] タブ）

[Time Settings] では Dashboard のシステムクロックを管理します。システムクロックを調整するには、以下の手順に従います。



1. **[System]** > **[System Platform Settings]**に移動し、[Network Settings] タブを選択します。
2. Dashboard に適切なタイムゾーンを選択します。
3. 時刻同期の方法を選択します。指定可能なオプションは、[NTP]（デフォルト）と[ローカル クロック] です。[NTP] オプションを選択した場合は、同期に使用する NTP サーバを必要に応じて変更します。

   [Local Clock] が選択されている場合、表示されているコントロールを使用して手動で日付と時刻を調整できます。また、[Clock] をクリックして、PC の時刻と同期させます。
4. [Save] をクリックします。

（注） 仮想マシンがローカル クロックとホスト マシンと同期させるように設定されている場合、[Platform Settings] ページから行ったローカル クロックの変更は、ハイパーバイザにより上書きされます。

使用中のハイパーバイザが VirtualBox で、VirtualBox Guest Additions が VM にインストールされている場合、NTP サービス（timesyncd）は動作しません。

ポート設定の変更（[Web Server] タブ）

[Port Settings] では、Dashboard のユーザインターフェイスがホストされる TCP ポートを管理します。デフォルトの Web サーバーポートを変更するには、以下の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[Web Server] タブを選択します。
2. HTTP および HTTPS プロトコル用に Web サーバが使用するポートを変更します。

3. Cisco Business Dashboard を介してネットワークデバイスへのリモートアクセスを提供するために使用されるポートを変更します。
4. [Save] をクリックします。

Dashboard へのアクセスの制限（[Web Server] タブ）

[Access Control] 設定を使用して、Dashboard にアクセスできる IP アドレスを制限できます。Dashboard GUI、Dashboard API、およびプローブと管理対象デバイスからの接続に異なる IP 範囲を指定できます。

Dashboard へのアクセスを制限するには、次の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[Web Server] タブを選択します。
2. 表示されたフィールドにネットワークプレフィックスおよびマスクを入力します。いずれかのセクションに複数のプレフィックスが必要な場合は、[+]（プラス）アイコンをクリックしてエントリを追加します。同様に、ごみ箱アイコンをクリックして既存のエントリを削除することもできます。
3. [Save] をクリックします。

システム変数の管理（[System Variables] タブ）

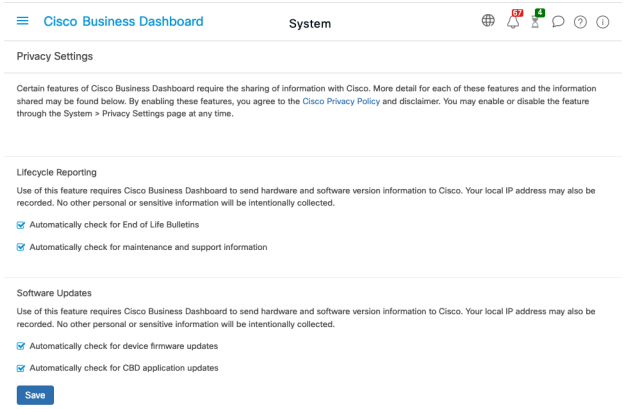
Cisco Business ダッシュボード 設定テンプレートやその他のタスクを生成するときに、システム変数を使用して、Dashboard に関連した特定のパラメータを入力します。一部のシステム変数は Dashboard によって自動的に決定されますが、ユーザ入力を必要とする変数もあります。特に、Dashboard が Web プロキシまたは NAT ゲートウェイの背後に展開されている場合、管理者は Dashboard の外部アドレッシング情報を提供する必要があります。

Dashboard の外部アドレス情報を更新するには、次の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[System Variables] タブを選択します。
2. 必要に応じて、[External System Settings] パラメータに IP アドレスとポート情報を入力します。空白のままにすると、Dashboard は、対応するシステム変数のプラットフォームアドレスとポート情報を使用します。
3. [Save] をクリックします。

プライバシーの管理

Cisco Business ダッシュボード の一部の機能には、シスコがホストするオンライン サービスを使用する必要があります。そのため、特定の情報をシスコと共有することになります。具体的には、次のようなサービスがあります。



- **Cisco Active Advisor**：Cisco Business ダッシュボードはネットワークインベントリ情報を Cisco Active Advisor サービス（*https://www.ciscoactiveadvisor.com*）にアップロードできます。この機能はデフォルトで無効に設定されています。
- **Lifecycle Reporting**：この機能には、Cisco Business ダッシュボードに**ライフサイクルレポート、サポート終了レポート、およびメンテナンスレポート**の生成が含まれています。ライフサイクルレポートはデフォルトで有効になっています。
- **Software Updates**：ネットワークデバイスのソフトウェア更新プログラムの可用性の通知と、それらの更新プログラムを自動的に適用する機能。ソフトウェアの更新はデフォルトで有効になっています。
- **Product Improvement**：この機能により、Cisco Business ダッシュボードは、シスコの製品ポートフォリオをさらに発展させる目的で、ネットワーク内のハードウェアとソフトウェアの使用状況に関する情報を送信できます。製品の改善はデフォルトで有効になっています。

これらの機能はすべてシスコのプライバシーポリシーの対象であり、いつでも有効または無効にすることができます。[Privacy Settings] ページは、Dashboard の初期セットアップ時に表示され、ネットワークデータが収集される前に、デフォルトで有効になっているどの機能も無効にすることができます。これらの機能と共有される情報の詳細については、以下を参照してください。

Cisco Active Advisor

Cisco Active Advisor（CAA）は、ネットワーク インベントリに関する必須のライフサイクル情報を提供するクラウドベースのサービスです。この機能を有効にすると、Dashboard がインベントリ情報を CAA に送信するようになるため、CAA ポータルにライフサイクル情報を表示できます。ユーザー名やパスワードなどの秘密情報は送信されません。

アップロードは、自動的に実行することも、オンデマンドで実行することもできます。オンデマンドアップロードを実行するには、次の手順を実行します。

1. [Network] ページに移動し、表示するネットワークを選択します。
2. [Network Actions] ドロップダウンから [Upload to CAA] を選択します。

3. プロンプトが表示された場合は、cisco.com のクレデンシャルを入力します。
4. 必要に応じて、アップロードに適用するラベルを選択します。
5. [Upload] をクリックします。また、[View inventory data before sending] をクリックして、アップロード前にデータを検査することもできます。

（注） 提供される cisco.com のクレデンシャルは、アップロードに使用する前に少なくとも 1 回は Cisco Active Advisor ポータル (*https://www.ciscoactiveadvisor.com*) へのログオンに使用する必要があります。

自動アップロードを有効にするには、以下の手順に従います。

1. [Network] ページに移動してネットワークを選択し、[More] をクリックします。次に、[CAA] タブを選択します。
2. 表示されたフィールドに cisco.com のクレデンシャルを入力します。

   または、アップロードに適用するラベルを選択できます。
3. [Automatically upload newly discovered devices] チェックボックスがオンになっていることを確認します。
4. [Save] をクリックします。また、このページのリンクをクリックして、アップロードするデータの例を表示することもできます。

自動アップロードを無効にするには、次の手順に従います。

1. [Network] ページに移動してネットワークを選択し、[More] をクリックします。次に、[CAA] タブを選択します。
2. [Automatically upload newly discovered devices] チェックボックスをオフにします。
3. [Save] をクリックします。

Lifecycle Reporting

Cisco Business ダッシュボードは、ネットワーク内の各シスコ デバイスのライフサイクル状態に関する情報を提供します。これを実行するには、Dashboard が各シスコデバイスの製品 ID、シリアル番号、ハードウェアおよびソフトウェアのバージョンをシスコに送信する必要があります。Dashboard の IP アドレスも記録されます。このプロセスの間に個人情報や機密情報が意図的に収集されることはありません。

ライフサイクルレポートの生成を無効にするには、以下の手順に従います。

1. **[System]** > **[Privacy Settings]** に移動します。
2. 無効にするレポートのチェックボックスをオフにします。
3. [Save] をクリックします。

Product Improvement

この機能を有効にすると、Cisco Business ダッシュボード からハードウェアおよびソフトウェア製品の使用状況情報が定期的にシスコに送信されます。Dashboard の IP アドレスも記録されます。このプロセスの間に個人情報や機密情報が意図的に収集されることはありません。

送信される情報の例を表示するには、以下の手順に従います。

1. **[System]** > **[Privacy Settings]** に移動します。
2. [Send product improvement data to Cisco] チェックボックスの横にある [View a Sample] リンクをクリックします。サンプルデータを使用したアップロードの例が表示されます。

製品改善データの生成を無効にするには、次の手順を実行します。

1. **[System]** > **[Privacy Settings]** に移動します。
2. [Send product improvement data to Cisco] チェックボックスをオフにします。
3. [Save] をクリックします。

Software Updates

この機能を使用するには、Cisco Business ダッシュボードが各デバイスの製品 ID とハードウェアおよびソフトウェアのバージョン情報をシスコに送信する必要があります。ローカル IP アドレスも記録される場合があります。このプロセスの間に個人情報や機密情報が意図的に収集されることはありません。

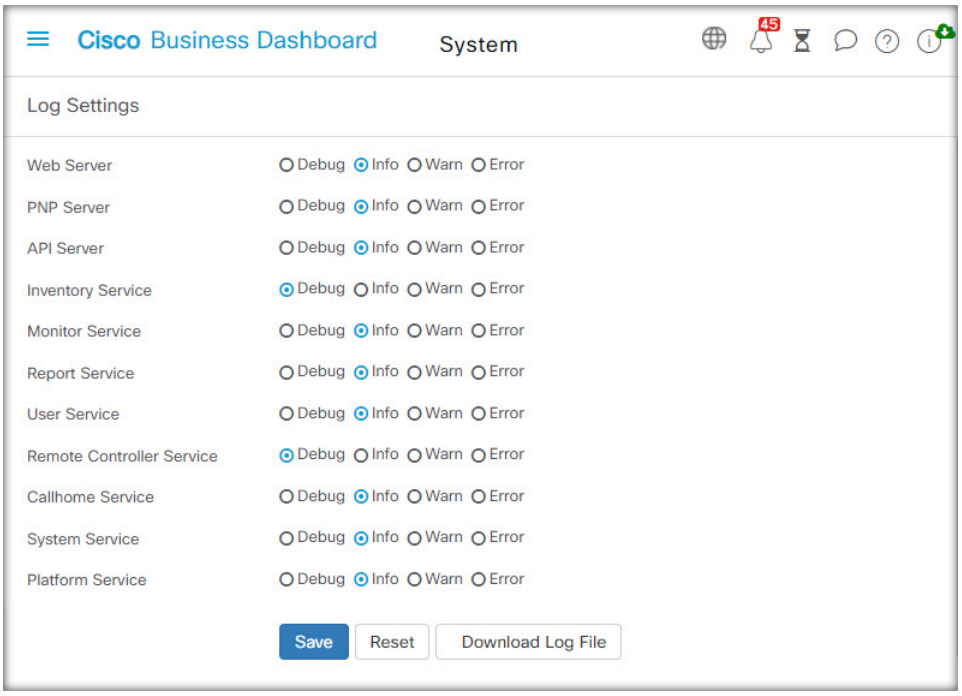
ソフトウェアの自動更新の使用を無効にするには、次の手順を実行します。

1. **[System]** > **[Privacy Settings]** に移動します。
2. デバイスファームウェアのチェックと Cisco Business ダッシュボード アプリケーションのチェックの両方のチェックボックスをオフにします。
3. [Save] をクリックします。

ログ設定の管理

[Log Settings] ページでは、各ソフトウェアモジュールによってログファイルに追加される詳細の量を制御できます。デフォルトのログ レベルは [Info] ですが、[Warn] または [Error] を選択することでログに記録されるメッセージの数を減らすことができ、また [Debug] を選択することでより多くの詳細を確認することができます。

Dashboard のログレベルを変更するには、以下の手順に従います。



1. **[System]** > **[Log Settings]** に移動します。
2. オプションボタンを使用して、各ソフトウェアモジュールの目的のログレベルを選択します。
3. [Save] をクリックします。

Dashboard のログファイルは、ローカルファイルシステムのディレクトリ `/var/log/ciscobusiness/dashboard/` で見つけることができます。[Download Log File] をクリックすると、このディレクトリのコンテンツのアーカイブをダウンロードできます。すべてのデータを収集するのに数分かかる場合があります。

syslog へのロギング

リリース2.2.1 以降、Cisco Business Dashboard アプリケーションログは、ホストの syslog サービスに送信され、そこから外部 syslog サーバに送信される場合があります。

ホスト syslog サービスへのファイルの送信を有効にするには、以下の手順に従います。

1. SSH またはコンソールを使用してホスト オペレーティング システムにログオンし、`/etc/ciscobusiness/dashboard/cisco-business-dashboard-logger.conf` ファイルを編集します。
2. `xxx.logger` 行を編集して、**file** または **syslog**、あるいはその両方を（カンマ区切りで）指定します。`redis`、`mongo`、`rabbitmq`、`nginx`、`cbd` の各モジュールを使用できます。`file` が指定されている場合、ログメッセージは `/var/log/ciscobusiness/dashboard/` ディレクトリのデフォルトログファイルに送信されます。**syslog** が指定されている場合、ログメッセージはホストの syslog サービスに送信されます。

（注） mongo モジュールは、複数のロギング先をサポートしません。複数の宛先がリストされている場合は、最初のエントリが優先されます。また、cbd モジュールは、ロガー設定の **file** キーワードの有無に関係なく、常にファイルシステムにログを記録します。

3. オプションで、`xxx.syslog.facility`行を変更して、各モジュールに使用される syslog ファシリティを指定できます。デフォルトでは、各モジュールは、個別のローカル <*n*> ファシリティにログを記録します（<*n*> の範囲は 1 ー 5 ）。
4. **cisco-business-dashboard stop** コマンドの後に **cisco-business-dashboard start** コマンドを使用して、Cisco Business Dashboard を再起動します。

ログメッセージを **syslog** に転送するようにロギング設定を変更したら、`/etc/rsyslog.conf` ファイルを更新してログを受信し、ダッシュボードのログメッセージを目的の宛先に転送します。設定ファイルの詳細については、https://www.rsyslog.com/doc/v8-stable/configuration/index.html [英語] を参照してください。

次の手順を実行します。

1. `/etc/rsyslog.conf`ファイルは、ループバック インターフェイスを介してログメッセージを受信できるように更新する必要があります。次の行が追加されるようにファイルを編集して、サーバがループバック インターフェイスのみでリッスンするように制限します。

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514" address="::1")
input(type="imudp" port="514" address="127.0.0.1")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514" address="::1")
input(type="imtcp" port="514" address="127.0.0.1")
```

2. ディレクトリ `/etc/rsyslog.d/` に新しいファイルを作成し、Cisco Business Dashboard に固有の設定ディレクティブを含めます。ファイル名は、`40-cisco-business-dashboard-syslog.conf`のような形式にする必要があります。
3. 手順 2 で作成したファイルを編集し、目的の宛先にログ出力を送信するためのディレクティブを含めます。たとえば、`cisco-business-dashboard-logger.conf` ファイルでデフォルトのファシリティを使用する場合、次の設定では、警告レベル以上のメッセージがダッシュボード アプリケーションから `logger.example.com` という名前の syslog サーバに送信されます。

```
local2.warning  @logger.example.com
```

4. **sudo systemctl restart rsyslog.service** コマンドを使用して rsyslog デーモンを再起動し、変更を適用します。

ローカル Probe の管理

（注） このページは AWS または Azure の Cisco Business ダッシュボード にはありません。

Cisco Business ダッシュボードプローブ は、Dashboard に対してローカルなネットワークのデバイスを管理するために、Cisco Business ダッシュボードと同じホストにインストールできます。Dashboard のシスコ仮想マシンイメージには Probe が含まれます。Dashboard に対してローカルなネットワークを管理しない場合、次の手順を使用して、同じ場所に配置されている Probe を無効にすることができます。

1. **[System]** > **[Local Probe]** に移動します。
2. トグル スイッチをクリックしてローカル Probe を無効にします。
3. [Save] をクリックします。

Dashboard から Probe ソフトウェア全体を削除するには、オペレーティングシステムにログオンし、`sudo apt-get --purge autoremove cbd-probe` コマンドを使用します。これにより、Probe ソフトウェア、設定、および他のアプリケーションが必要としない依存ファイルが削除されます。

統合設定の管理

Cisco Business Dashboard は、シスコおよびその他のベンダーが提供するさまざまなアプリケーションやサービスと統合することができます。アプリケーションと統合すると、アプリケーションと実行されるネットワークアクション間でデータとイベントが交換される場合があります。

統合は、次のアプリケーションとサービスでサポートされます。

- Connectwise Manage
- Webex

統合の設定および各アプリケーションと交換される情報の詳細については、次のセクションを参照してください。

Connectwise Manage

Connectwise Manage は、マネージドサービスプロバイダーが使用するために設計されたプロフェッショナルサービス自動化ツール（PSA）です。資産管理、アカウンティングおよび課金、ヘルプデスクサービスが機能の一部として含まれています。Cisco Business Dashboard と Connectwise Manage を統合することで、ネットワークデバイスの資産レコードを最新に保ち、ヘルプデスクチケットでイベントとネットワークアクションを管理できます。

サポートされる機能

Connectwise Manage と統合すると、Cisco Business ダッシュボードは資産管理、イベント管理、および自動化の 3 つの主要領域で追加機能を提供します。

資産管理の場合、Cisco Business ダッシュボードはダッシュボードで管理される各ネットワークデバイスの Connectwise Manage で設定レコードを自動的に作成し、定期的に更新します。設定レコードには、デバイスのタイプとモデル、シリアル番号、ソフトウェア情報、保証期限、ライフサイクル情報などの情報が含まれます。デバイスがダッシュボードインベントリから削除されると、設定は非アクティブとしてマークされますが、Connectwise Manage からは削除されません。

構成レコードの作成に加えて、ネットワークデバイスタイプを Connectwise Manage の特定の製品に関連付け、その製品とその顧客に関連付けられているデバイスの数量を含む Cisco Business ダッシュボード更新契約を設定することもできます。

ネットワークイベントを管理する場合、選択した通知が発生したときにダッシュボードがヘルプデスクチケットを作成するように、Cisco Business ダッシュボードモニタリングプロファイルを設定できます。これらの通知チケットには、イベントの詳細が含まれ、通知を生成したデバイスの設定レコードに関連付けられます。ファームウェア通知の場合、チケットは自動化チケットとして作成して、次の変更ウィンドウでファームウェア更新をデバイスに適用することもできます。

自動化チケットは、Cisco Business ダッシュボードがネットワークアクションを実行する特殊なチケットです。自動化チケットは、ダッシュボードが監視する専用のサービスボードで作成され、次のアクションを自動化するために使用できます。

- 設定のバックアップ
- 最新のファームウェアバージョンへのアップグレード
- デバイスの再起動
- 実行コンフィギュレーションの保存
- デバイスの削除

自動化チケットは、すぐに実行するように作成することも、次の変更時間帯に作成することもできます。実行前に承認を要求するように設定することもできます。チケットは、実行中の進捗情報と完了時のアクションの結果で更新されます。

前提条件

Connectwise Manage 統合を設定する前に、次の前提条件を満たす必要があります。

- 自動化チケットを使用する場合は、Connectwise Manage アプリケーションが Cisco Business Dashboard Web サーバーへの接続を確立できる必要があります。さらに、Cisco Business Dashboard には、Connectwise Manage によって信頼されている証明書が必要です。ほとんどの場合、これは、証明書が公的 CA によって署名される必要があることを意味します。Cisco Business Dashboard の証明書の設定の詳細については、証明書の管理 （116 ページ）を参照してください。

- ダッシュボードが NAT ゲートウェイまたはファイアウォールの背後にある場合は、**[System]** > **[Platform Settings]** の [System Variables] ページに、Connectwise Manage アプリケーションがダッシュボードへの接続に使用するホスト名と Web サーバーポートが入力されていることを確認してください。
- Cisco Business ダッシュボード用に一連の API キーを作成し、少なくとも次の表に示す権限が必要です。

表 *8 : API* キーに必要な権限

権限	追加レベル	編集レベル	削除レベル	問い合わせレベル
企業				
企業の保守	なし	なし	なし	すべて
コンフィギュレーション	すべて	すべて	すべて	すべて
ファイナンス				
契約	なし	すべて	なし	すべて
調達				
製品カタログ	なし	なし	なし	すべて
サービスデスク				
サービスチケット	すべて	すべて	すべて	すべて
システム				
テーブルの設定	すべて	すべて	すべて	すべて

- 自動化チケットに適したサービスボードを特定または作成する必要があります。このボードには、統合プロセス中に適用される多くの設定要件があります。このボードは、ネットワーク運用専用にすることをお勧めします。このボードの設定方法の詳細については、次のセクションを参照してください。
- 通知チケットに適したサービスボードを特定または作成する必要があります。このボードには特定の要件はなく、既存の汎用ボードを使用できます。通知ボードは、自動化チケットに使用されるものと同じサービスボードでもかまいません。

Connectwise Manage 統合の設定

Connectwise Manage 統合の設定には、いくつかの手順があります。

- Connectwise Manage サービスとの通信を確立します。

- Connectwise の企業を Cisco Business Dashboard 組織にマッピングします。
- アセットの同期プロセスを設定します。
- イベント通知と自動化のサービスボードを選択します。

ここでは、すべての設定を正しく行うための各プロセスの実行方法について説明します。

Connectwise Manageサービスとの通信の確立

1. [System] > [Integration Settings] の順に選択します。
2. Connectwise Manage 統合を表すタイルを特定し、トグルスイッチが [Enabled] に設定されていることを確認します。
3. [Settings] アイコンをクリックして [Connectwise Manage Settings] ページを表示し、[Connection] タブを選択します。
4. 表示されたフォームのフィールドに入力し、[Save] をクリックします。要求されたパラメータの詳細については、次の表を参照してください。

表 9 : [Connectwise Manage Connection] のパラメータ

パラメータ	説明
API Hostname	接続先の Connectwise Manage サービスのプロトコルとホスト名。デフォルトは https://na.connectwise.net です。
Company ID	Connectwise Manage の企業 ID。これは、Connectwise Manage GUI にログオンするときに使用される値と同じです。
Public key	Cisco Business Dashboard の Connectwise Manage で定義された API キーの公開キー。
Private key	Cisco Business Dashboard の Connectwise Manage で定義された API キーの秘密キー。

[Save] をクリックすると、Cisco Business ダッシュボードは接続をテストし、セットアッププロセスの後半で必要となる Connectwise Manage からの情報を読み取ります。この情報には、企業、設定タイプ、製品、契約タイプ、およびサービスボードのリストが含まれます。Connectwise Manage でこの情報のいずれかを変更した場合は、このページの [Refresh Connectwise Data] ボタンをクリックしてデータを再読み取りします。

Connectwise の企業をCisco Business ダッシュボード 組織にマッピングする

Cisco Business Dashboard と Connectwise Manage 間の接続を確立したら、Cisco Business Dashboard の組織を Connectwise Manage の企業にマッピングする必要があります。企業を組織にマッピングすると、Connectwise Manage でネットワークデバイスとイベントを正しい顧客に関連付けることができます。マッピングを完了するには、次の手順に従います。

1. [System] > [Integration Settings] の順に選択します。

2. [Connectwise Manage] タイルの [Settings] アイコンをクリックし、[Organization Mapping] タブを選択します。
3. [Import from Connectwise] ボタンをクリックします。これにより、会社のリストと組織のリストが比較され、企業名または企業 ID のいずれかが組織名と一致する場合にマッピングが作成されます。
4. 企業と組織間の任意のマッピングは、手動で行うことも、カンマ区切り値（CSV）ファイルを使用して行うこともできます。

   マッピングを手動で作成するには、次の手順を実行します。

   1. マッピングテーブルの上にある [✚]（プラス）アイコンをクリックして、テーブルに新しいエントリを作成します。
   2. ドロップダウンリストから、マッピングする企業名と組織名を選択します。

   （注） 目的の企業名がドロップダウンメニューに表示されない場合は、[Connect] タブに戻り、[Refresh Connectwise Data] ボタンをクリックして会社のリストを更新します。

   3. [Save] アイコンをクリックします。

   CSV ファイルを使用してマッピングを作成するには、次の手順を実行します。

   1. 組織と会社名の間の必要なマッピングを含む CSV ファイルを作成します。
   2. 既存のマッピングのリストを含むテンプレート CSV ファイルのマッピングテーブルの上にある [Download] アイコンをクリックします。
   3. テンプレートファイルが更新されたら、テーブルの上にある [Upload] ボタンをクリックして、ファイルで指定された新しいマッピングを作成します。

   既存のマッピングを変更するには、次の手順を実行します。

   1. マッピングの横にあるラジオボタンをクリックします。
   2. [Edit] アイコンをクリックします。
   3. 必要な変更を加えます。
   4. [Save] アイコンをクリックします。

   既存のマッピングを削除する

5. 1. マッピングの横にあるラジオボタンをクリックします。
   2. **削除**アイコンをクリックします。

アセットの同期プロセスを設定します

ネットワークデバイスを表す設定レコードをConnectwise Manageで作成することは、イベント管理および自動化機能が動作するための前提条件です。Cisco Business Dashboardは、Connectwise Manageの企業にマッピングされている組織内の各ネットワークデバイスの設定レコードを自動的に作成および更新します。アセットの同期を設定するには、次の手順に従います。

1. [System] > [Integration Settings] の順に選択します。
2. [Connectwise Manage] タイルの [Settings] アイコンをクリックし、[Asset Synchronization] タブを選択します。
3. [Createwise Configuration Types in Connectwise] ボタンをクリックします。

   これにより、3 つの設定タイプ（CBD 管理型ルータ、CBD 管理型スイッチ、および CBD 管理型 WAP）が作成され、ネットワークデバイスに適したフィールドと質問が表示されます。これらの設定タイプがすでに存在する場合は、フィールドと質問で更新されます。
4. [Save] アイコンをクリックします。

毎日午前 0 時に、Cisco Business ダッシュボードは企業にマッピングされた各組織のアセット同期を実行します。その組織内のネットワークデバイスごとに、そのデバイスに関する情報を含む設定レコードが作成されます。設定レコードがすでに存在する場合は、デバイス情報への変更で更新されます。Cisco Business ダッシュボードから削除されたデバイスに関連付けられている設定レコードは、**非アクティブ**としてマークされます。

同期プロセスの一環として、Cisco Business ダッシュボードは次のことも行います。

1. 各企業について、Cisco Businessダッシュボードは指定した契約タイプに一致する契約を特定します。
2. 各契約について、Cisco Businessダッシュボードは選択した製品に一致する追加を特定し、各デバイスタイプに関連付けます。
3. 追加ごとに、Cisco Business ダッシュボードは対応する製品が選択されているタイプのデバイスの数に基づいて数量を更新します。

これを実現するには、次の手順を実行します。

1. **[System]** > **[Integration Settings]** の順に選択します。
2. [Connectwise Manage] タイルの [Settings] アイコンをクリックし、[Asset Synchronization] タブを選択します。
3. デバイスタイプごとに、[Product] フィールドをクリックし、このタイプのデバイスに関連付ける 1 つ以上の製品を選択します。
4. [Agreement Type] 見出しで、更新する契約を特定する 1 つ以上の契約タイプを選択します。
5. [Save] アイコンをクリックします。

（注） 目的の製品または契約タイプがドロップダウンメニューに表示されない場合は、[Connect] タブに戻り、[Refresh Connectwise Data] ボタンをクリックします。

イベント通知と自動化のサービスボードを選択します。

これらの各機能に使用するサービスボードを指定して、イベント管理および自動化機能を有効にします。使用するサービスボードを指定するには、次の手順を実行します。

1. [System] > [Integration Settings] の順に選択します。
2. [Connectwise Manage] タイルの [Settings] アイコンをクリックし、[Ticket Settings] タブを選択します。
3. [Notification Board] ドロップダウンメニューから、ネットワークイベントに応じて作成されるチケットに使用する適切なサービスボードを選択します。
4. [Automation Board] ドロップダウンメニューから、自動化チケットを監視するサービスボードを選択します。

（注） 目的のサービスボードがドロップダウンメニューに表示されない場合は、[Connect] タブに戻り、[Refresh Connectwise Data] ボタンをクリックしてサービスボードのリストを更新します。

5. [Save] アイコンをクリックします。

   Cisco Business ダッシュボードは、自動化機能をサポートするために必要な適切なステータス値、タイプ、およびサブタイプを含むように、Connectwise Manage の自動化ボードの設定を更新します。作成されるステータス、タイプ、およびサブタイプの詳細については、自動化チケットを使用したネットワークアクションの自動化（143ページ）の表30ー32を参照してください。

Connectwise Manage 統合の使用

Connectwise Manage で提供される 3 種類の統合のうち、イベント管理と自動化では、ユーザがアクティブに機能を操作する必要があります。通常、アセットの同期には、ユーザの操作は必要ありません。次の項では、各機能の使用方法について詳しく説明します。

アセットの同期の使用

上記の初期設定以外のアセット同期には、特別なアクションは必要ありません。Cisco Business ダッシュボードのネットワークデバイスのインベントリは、次の表に示す情報を含むConnectwise Manage 設定レコードに自動的に同期されます。アセットの同期設定で指定されたタイプに一致する契約には、選択した製品に一致する追加の数量が更新され、ネットワークに存在する対応するタイプのデバイスの数が反映されます。

アセットの同期プロセスは、毎日午前0時に自動的に行われます。即時同期が必要な場合は、[Asset Synchronization] 画面の [Sync Assets] ボタンをクリックして開始できます。Cisco Business ダッシュボードとコラボレーションツールが統合されている場合は、コラボレーションツールから実行することもできます。

（注） 通常、アセットの同期プロセスには数分かかり、大規模なネットワークではさらに時間がかかることがあります。

表 *10 : Connectwise Manage Configuration* フィールドの使用方法

フィールド	説明
Configuration Name	デバイスのホスト名に設定します
コンフィギュレーションの詳細	
Type	設定タイプは、[Asset Synchronization] ページで設定されたデバイスタイプとマッピングに基づいて設定されます。
Status	デバイスがダッシュボードインベントリから削除された場合は [Inactive] に設定され、そうでない場合は [Active] に設定されます。
Model	デバイスのモデル番号。
Serial Number	デバイスのシリアル番号。
会社	
Company	[Organization Mapping] ページで定義されているデバイスの組織に対応する会社。
注記	
Vendor Notes	Cisco Business ダッシュボードによって設定が作成されたことを示すメモと、作成タイムスタンプが表示されます。
Configuration Questions	設定に関する質問には、次の情報が含まれています。 • デバイスの製品 ID：このフィールドはモデル番号に似ていますが、新しいデバイスを購入するときに使用される識別子です。 • ソフトウェアバージョン：この情報には、現在のバージョンと、リリースノート付きの最新バージョンが含まれます。 • ライフサイクル情報：保証終了日と適用されるサポート終了の詳細が含まれます。
デバイスの詳細	

フィールド	説明
IP Address	デバイスの管理 IP アドレス。
MAC Address	デバイスの基本 MAC アドレス

自動化チケットを使用したネットワークアクションの自動化

自動化チケットでを使用すると、特別にフォーマットされたチケットを開いて、ネットワークデバイス上でアクションを実行できます。

チケットでは、アクションをすぐに実行するか、次の変更ウィンドウで実行するかを指定できます。また、実行前に承認手順が必要な場合があります。すべての前提条件が満たされると、Cisco Business ダッシュボードはチケットで指定されたアクションを実行し、操作の成功または失敗でチケットが更新されます。

自動化チケットを作成するには、次の特性を持つ新しいチケットを作成します。

- サービスボードは、統合の設定時に作成された自動化ボードに設定する必要があります。
- チケットは、Cisco Business ダッシュボードが管理するネットワークデバイスを表す 1 つの設定にのみ関連付ける必要があります。
- タイプは、目的のアクションに設定する必要があります。使用可能なアクションのリストについては、表 11 : 自動化チケットのタイプ （144 ページ）を参照してください。
- サブタイプは、必要な実行時間と承認が必要かどうかに基づいて選択する必要があります。使用可能なオプションのリストについては、表 12 : 自動化チケットのサブタイプ （145 ページ）を参照してください。
- 自動化プロセスを開始するには、ステータスを [Start] に設定する必要があります。自動化を開始する前に追加の作業が必要な場合は、作業が完了するまでステータスを [Needs Attention] に設定できます。可能なステータス値の一覧については、表 13 : 自動化チケットのステータス （145 ページ）を参照してください。

自動化チケットが作成され、ステータスが [Start] の場合、Cisco Business ダッシュボードはチケットを制御し、次の手順を実行します。

1. CBD は、チケットをチェックして、必要な情報がすべて存在することを確認します。問題がある場合は、内部メモが更新され、ステータスが [Needs Attention] に変わります。
2. チケットの形式が正しい場合は、承認が必要かどうかを確認するためにサブタイプがチェックされます。その場合、ステータスは [Needs Approval] に変更されます。ステータスが [Approved] に更新されるまで、それ以上のアクションは実行されません。
3. サブタイプがチェックされ、アクションを実行するタイミングが確認されます。チケットが今すぐ実行するように設定されている場合、ダッシュボードはすぐにアクションを実行します。アクションが次の変更ウィンドウで実行するように設定されている場合、新しいスケジュールプロファイルが作成され、チケットステータスが更新されてジョブが保留中であることが示されます。

4. アクションが完了すると、ダッシュボードはチケットのメモを更新し、操作の成功または失敗を示します。アクションが正常に完了した場合、チケットはクローズされます。アクションが失敗した場合は、ステータスが [Needs Attention] に更新されます。失敗の理由が解決すると、ステータスを [Start] に変更してチケットを再スケジュールするか、アクションが不要になった場合にクローズすることができます。

自動化チケットの承認は、自動化プロセスにある程度の変更制御を挿入できるオプションです。承認を必要とする自動化チケットを指定することで、アクションが実行される前にアクションを検証し、検証がチケット履歴に記録されます。

Connectwise Manage の自動化チケットの承認は、承認が必要で許可されていることを示すステータス変更によって実装されます。

承認が必要なチケット（ステータスが [Needs Approval] のチケット）は、次のいずれかの方法で承認できます。

- チケットステータスは、Connectwise Manage インターフェイスを使用して直接更新できます。承認を記録すると同時にチケットにメモを追加することをお勧めします。ただし、承認の詳細はチケット監査証跡にも記録されます。
- チケットは、Cisco Business ダッシュボードと統合されたコラボレーションツールを介して承認される場合があります。この場合、承認と承認者の ID を記録するメモがチケットに追加されます。

（注） Connectwise Manage またはCisco Business ダッシュボードのどちらも、承認者がチケットの作成者とは別の人物でなければならないという要件を適用できます。承認者は、指定されたスタッフのリストに制限することはできません。チケットを編集できるユーザ、またはコラボレーションスペースにアクセスできるユーザは、チケットを承認できます。このような制限を実装するには、運用プロセスが必要です。

表 *11* : 自動化チケットのタイプ

タイプ	説明
Backup Configuration	デバイスの現在の実行設定のコピーを取得し、Cisco Business ダッシュボードに保存します。
Delete	Cisco Business ダッシュボードインベントリからオフラインのデバイスを削除します。
Reboot	デバイスの再起動
Save Running Config	起動時に使用するために、実行設定をデバイスに保存します。
Update Firmware to Latest	デバイスのソフトウェアを、シスコが公開している最新バージョンにアップグレードします。

表 *12 :* 自動化チケットのサブタイプ

サブタイプ	説明
Approval Required – Run During Change Window	このアクションは承認が必要であり、チケットが承認された後の次の変更ウィンドウで実行されるようにスケジュールする必要があります。
Approval Required – Run Now	このアクションは承認が必要であり、チケットが承認されたらすぐに実行する必要があります。
Run During Change Window	アクションは、次の変更ウィンドウで実行されるようにスケジュールする必要があります。
Run Now	アクションはすぐに実行する必要があります。

表 *13 :* 自動化チケットのステータス

ステータス	説明
Start	チケットで自動化の準備ができていることをダッシュボードに示します。
Needs Attention	手動による操作が必要であることを示します。このステータスは、自動化を開始する前に必要な作業がある場合に手動で設定でき、自動化アクションが失敗した場合にダッシュボードによって設定されます。
In Process	ダッシュボードはチケットをアクティブに処理しています。
Needs Approval	続行するには承認が必要な有効な自動化チケットを示します。続行するには手動による操作が必要です。
Approved	チケットが承認され、実行の準備ができていることを示します。チケットは、Connectwise Manage ユーザインターフェイスでこのステータスを選択するか、Cisco Business ダッシュボードと統合されたコラボレーションツールの承認コマンドによって承認されます。
Scheduled with CBD	Cisco Business ダッシュボードでジョブがスケジュールされていますが、まだ実行されていません。チケットはジョブが実行されると更新されます。
Complete (closed)	要求されたアクションは正常に完了しました。

通知チケット付きネットワークイベントの管理

ネットワークイベントに応答してチケットを作成できるようにするには、Cisco Business ダッシュボードモニタリングプロファイルを更新して、[Open Helpdesk Ticket] アクションを 1 つ以

上の通知モニタに追加する必要があります。モニタリングプロファイルの管理に関する詳細については、モニタリングプロファイル （106 ページ） を参照してください。

（注） モニタリングプロファイルを設定して、チケットまたはコラボレーションメッセージの平均レートが 1 時間あたり 60 を継続的に超えないようにすることをお勧めします。外部アプリケーションと通信する場合、これを超えるレートが持続すると、API の輻輳とイベントの損失が発生する可能性があります。

[Open Helpdesk Ticket] が有効になっているモニタリングプロファイルに一致する通知が発生すると、通知ボードで新しいチケットが開かれ、対応するデバイスの設定に関連付けられます。チケットの本文は、通知に関する関連情報で更新されます。

ほとんどの通知モニタでは、通知チケットのみを開くことができます。ただし、ファームウェア通知の場合は、追加のオプションを使用できます。デバイスの新しいファームウェアバージョンが検出されると、作成されたチケットを自動化チケットとして開くこともできます。これにより、次の変更期間でファームウェアの更新がデバイスに適用されます。

モニタリングプロファイルでファームウェア通知を設定する場合は、[With Automation] と [With Approval] の 2 つの追加オプションが提供されます。[With Automation] チェックボックスをオンにすると、通知チケットの代わりに自動化チケットが作成されます。チケットは、デバイス設定に関連付けられた自動化ボードで開かれ、タイプが [Upgrade Firmware to Latest] に設定されます。

最後に、次の変更期間でアップグレードが実行されるように、サブタイプが設定されます。[With Approval] チェックボックスがオンになっている場合、サブタイプは、アップグレードがスケジュールされる前に承認が必要になるように設定されます。自動化チケットで使用されるさまざまなサブタイプの詳細については、表 12 : 自動化チケットのサブタイプ （145 ページ） を参照してください。

Webex

Webex は、メッセージング、通話、および会議を含むコラボレーションツールおよびサービスのスイートです。Cisco Business ダッシュボード と Webex との統合により、重要なネットワークイベントを常に通知し、アクションを実行できます。デスクトップまたはモバイルデバイスで Webex アプリケーションを使用できます。

サポートされる機能

Cisco Business Dashboard を Webex と統合すると、コラボレーションスペースに通知を転送して、ユーザにネットワークイベントを通知できます。モニタリングプロファイルを更新して通知をカスタマイズし、転送するプロファイルを選択できます。

さらに、ユーザが Webex インターフェイスから特定のアクションを実行できる、制限された制御インターフェイスが提供されます。サポートされるアクションは次のとおりです。

- Cisco Business ダッシュボードによって作成されたオープンヘルプデスクチケットのリストを表示します。

- 承認が必要な自動化チケットのリストを表示します。
- 自動化チケットを承認します。
- 使用可能なファームウェアアップデートがあるネットワークデバイスのリストを表示します。
- ネットワークデバイスのアップグレードを開始します。

前提条件

Webex統合を設定する前に、Webexボットを作成し、コラボレーションスペースに招待する必要があります。ボットを設定するには、次の手順を実行します。

1. https://developer.webex.com/my-apps/new/bot に移動して Webex アカウントにログインします。
2. ボットを作成するためのフォームに入力します。ボットの名前、ユーザ名、説明を入力する必要があります。ボットのカスタムアイコンを提供するオプションもあります。

（注） Webex ではボット名に空白文字を含めることができますが、Cisco Business ダッシュボードではボット名を空白を含まない単一の単語にする必要があります。

3. [Add Bot] をクリックしてボットを作成します。 Webex 統合を設定するときに必要になるため、表示されるボットトークンをメモします。

メモ ボットトークンは一度だけ表示されるため、後で参照できるように安全な場所に記録することが重要です。

ボットが作成されたら、コラボレーションスペースに招待する必要があります。Cisco Business ダッシュボードとの統合用に専用のスペースを作成しますが、既存のスペースを使用することもできます。ただし、スペースのメンバーはすべてのイベントを表示でき、サポートされているすべてのコマンドを実行できるため、ネットワークを管理する権限を持つユーザのみがスペースを使用できるようにする必要があります。

スペースの作成とユーザの招待の詳細については、Webex ドキュメントまたは Webex アプリのオンラインヘルプを参照してください。

（注） ボットは、Cisco Business ダッシュボードと統合されている場合にのみ、単一のコラボレーションスペースに招待されます。複数のスペースに招待された場合、ボットの動作は予測できません。

ボットの作成に加えて、Webex インフラストラクチャが Cisco Business Dashboard Web サーバーへの接続を確立できることを確認する必要があります。ダッシュボードが NAT ゲートウェイまたはファイアウォールの背後にある場合は、**[System]** > **[Platform Settings]** の下の [System Variables] ページに、Webex インフラストラクチャがダッシュボードへの接続に使用するホスト名と Web サーバーポートが入力されていることを確認してください。

Webex の統合の設定

Webex の統合を設定するには、次の手順を実行します。

1. [System] > [Integration Settings] の順に選択します。
2. Webex 統合のタイルを特定し、トグルスイッチが [Enabled] に設定されていることを確認します。
3. [Settings] アイコンをクリックして、[Webex Settings] ページを表示します。
4. ボットの作成時に受け取ったボットトークンを所定のフィールドにコピーし、[Save] アイコンをクリックします。
5. ステータスフィールドに正しいボット名とコラボレーションスペースが表示されていることを確認します。

（注） ボットは、Cisco Business Dashboard の 1 つのインスタンスでのみ使用し、他のアプリケーションでは使用しないでください。複数のアプリケーションがボットに関連付けられている場合、動作は予測できません。

Cisco Business ダッシュボードにボットの詳細を設定したら、コラボレーションスペースに通知を転送するようにモニタリングプロファイルを設定できます。モニタリングプロファイルの設定の詳細については、モニタリングプロファイル （106 ページ）を参照してください。

Webex 統合の使用

Webex 統合の使用は、主に次の 2 つの領域に分類されます。

- ネットワークイベントの通知の設定と受信。
- 限定制御インターフェイスを介したCisco Business ダッシュボードとの連携動作。

次の項では、それぞれのアクティビティについて詳しく説明します。

ネットワークイベントの通知管理

ネットワークイベントに応答して Webex で通知を有効にするには、Cisco Business ダッシュボードモニタリングプロファイルを更新して、[Send To Collaboration Space] アクションを 1 つ以上の通知モニタに追加する必要があります。モニタリングプロファイルの管理に関する詳細については、モニタリングプロファイル （106 ページ） を参照してください。

（注） モニタリングプロファイルを設定して、チケットまたはコラボレーションメッセージの平均レートが 1 時間あたり 60 を継続的に超えないようにすることをお勧めします。外部アプリケーションと通信する場合、これを超えるレートが持続すると、API の輻輳とイベントの損失が発生する可能性があります。

[Send To Collaboration Space] が有効になっているモニタリングプロファイルと一致する通知が発生すると、メッセージがコラボレーションスペースにプッシュされます。メッセージには、通知の詳細などの通知に関する関連情報と、Cisco Business ダッシュボード でデバイスを表示するためのリンク、およびイベント用に作成されている場合は Connectwise Manager で関連するヘルプデスクチケットを表示するためのリンクが含まれます。

Webex を介した Cisco Business Dashboard との連動動作

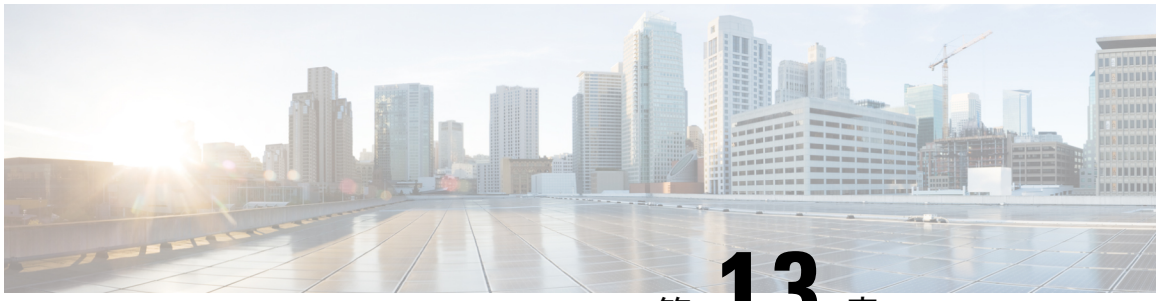
Webex と統合すると、Cisco Business ダッシュボード はダッシュボードのクエリとアクションを実行するために使用できる限定されたコマンドインターフェイスを提供されます。次の表に、使用可能なコマンドと関連アクションを示します。

このインターフェイスでは、ユーザがコマンドを受け入れるためにボットを指定する必要があります。インターフェイスは入力の柔軟性をある程度許容しますが、自然言語処理を提供するものではなく、定義済みコマンドのセットに制限されます。また、インターフェイスは部分的に大文字と小文字を区別し、一般的な使用法を認識しますが、一般的でない大文字化パターンを使用するコマンドは認識しません。

表 *14* : サポートされるコラボレーションコマンド

コマンド	説明
Menu Help ?	使用可能なすべてのコマンドのリストと説明を表示します。
Approvals	承認が必要な自動化チケットのリストを表示します。 このコマンドは、ダッシュボードが Connectwise Manage と統合されている場合にのみ使用できます。
Approve <Ticket#>	指定された自動化チケットを実行の承認済みとしてマークします。
Assets	アセットの同期プロセスを開始します。 このコマンドは、ダッシュボードが Connectwise Manage と統合されている場合にのみ使用できます。
Firmware	使用可能なファームウェアアップデートがあるすべてのネットワークデバイスのリストを表示します。

コマンド	説明
Upgrade <Serial#>	次の変更ウィンドウで指定されたデバイスのファームウェア更新を実行するようにスケジュールします。 ダッシュボードが Connectwise Manage と統合されている場合、承認を必要とする自動化チケットがこのタスク用に作成されるか、またはCisco Business ダッシュボードで直接スケジュールされます。



第 13 章

通知

この章は、次の項で構成されています。

通知について

Cisco Business ダッシュボードにより、Connectwise または Webex チームの統合通知など、ネットワークでさまざまなイベントが発生したときに通知が生成されます。通知は、電子メールか、ブラウザの右下隅に表示されるポップアップアラートを生成し、すべての通知は後で確認するためにログに記録されます。

通知は、関心がなくなったときに確認することもできます。デフォルトでは、これらの通知は [Notification Center] に表示されません。

サポートされる通知

次の表に、Cisco Business ダッシュボード でサポートされている通知のリストを示します

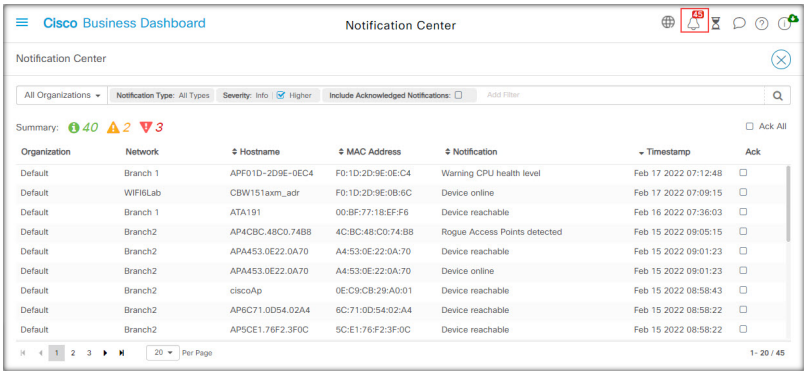


表 *15 :* サポートされる通知

イベント	レベル	説明	自動的にクリアされるか
アクセスポイント、ルータ、IP 電話、およびスイッチのデバイス通知			
到達可能性/デバイスが検出されました	Information	ネットワーク上に新しいデバイスが検出されました。	はい。デバイス検出の 5 分後。
到達可能性/デバイスが検出されませんでした	Warning	デバイスは検出プロトコルを通じて認識されていますが、IP を使用して到達できません。	はい（IP を介してデバイスに再度到達可能になったとき）
到達可能性/デバイスがオフラインです	Alert	デバイスはネットワーク上で検出されなくなりました。	はい（デバイスが再検出されたとき）
クレデンシャルが必要です/SNMP	Warning	Probe は、認証エラーによりデバイスにアクセスできません。	はい（Probe が認証されたとき）
クレデンシャルが必要です/ユーザ ID	Warning	Probe は、認証エラーによりデバイスにアクセスできません。	はい（Probe が認証されたとき）
ログイン情報が必要/パスワードが期限切れ	Warning	デバイスの管理者ユーザーのパスワードの有効期限が切れています。	はい（デバイスのパスワードがリセットされたとき）。
コンフィギュレーションの不一致	Alert	現在のデバイス設定が、Cisco Business Dashboard の設定プロファイルおよびデバイス設定で指定された設定と一致しません。	はい（設定の不一致が解決されたとき）。
デバイスサービス/SNMP	Warning	SNMP がデバイスで無効になっています。	はい（SNMP が有効になったとき）
デバイス サービス/Web サービス	Warning	Web サービスがデバイスで無効になっています。	はい（web サービス API が有効化されているとき）
状態	Warning/Alert	デバイスの稼働レベルが警告またはアラートに変化しました。	はい（デバイスの稼働状態が正常に戻ったとき）
シスコサポート通知			

イベント	レベル	説明	自動的にクリアされるか
ファームウェア	Information	新しいバージョンのファームウェアが cisco.com で入手できます	はい（デバイスが最新版にアップデートされたとき）
サポート終了	Warning/Alert	デバイスの サポート終了製品速報が検出されたか、またはサポート終了のマイルストーンに到達しました。	なし
メンテナンス有効期限	Warning/Alert	デバイスは保証対象外である、または現在有効な保守契約が結ばれていない、あるいはその両方です。	はい（新しい保守契約が結ばれた場合）
デバイスの健全性通知			
CPU	Warning/Alert	デバイスの CPU 使用率が最大しきい値を超えています。	はい（CPU 使用率が通常のレベルに戻った場合）
稼働時間	Warning/Alert	デバイスの稼働時間が最小しきい値を下回っています。	はい（デバイスの稼働時間が最小レベルを超えた場合）
接続クライアント数	Warning/Alert	接続されているクライアントの数が最大しきい値を超えています。	はい（接続されているクライアントの数が許容レベルに戻ったとき）

現在のデバイスの通知の表示とフィルタリング

単一のデバイスまたはすべてのデバイスの現在アクティブな通知を表示するには、以下の手順に従います。

1. [Home] ウィンドウで、グローバル ツールバーの右上隅にある [Notification Center] アイコンをクリックします。アイコンの番号バッジは未確認の通知の総数を示しており、バッジの色は現在未確認の最も高いシビラティ（重大度）を示しています。

   現在未処理になっている通知は、[Notification Center] アイコンの下に表示されます。シビラティ（重大度）アイコンの数字は、以下の各カテゴリの通知の総数を示しています。

アイコン	説明
	情報（緑色の円形のアイコン）

アイコン	説明
	警告（オレンジ色の三角形のアイコン）
	アラート（赤い逆三角形のアイコン）

2. [Notification Center] では、次のアクションを実行できます。
   - 通知の確認：通知のチェックボックスをオンにして、通知を確認します。表示内のすべての通知を確認するには、[ACK All] チェックボックスをオンにします。
   - 表示された通知をフィルタリングする：手順 3 を参照してください。

3. フィルタボックスは、テーブルに表示される通知を制限します。デフォルトでは、すべてのタイプとすべてのシビラティ（重大度）レベルの通知が表示されます。既存のフィルタを変更するには、そのフィルタをダブルクリックして設定を変更します。新しいフィルタを追加するには、[Add Filter] ラベルをクリックし、ドロップダウンリストからフィルタを選択します。以下の表に、使用可能なすべてのフィルタを示します。

フィルタ	説明
Notification Type	表示する通知のタイプ。たとえば、オフラインのデバイスに対する通知を表示するには、ドロップダウン リストから [Device Offline] を選択します。
Severity	表示される通知の重大度レベルには、次のものが含まれます。 • Info • Warning • Alert [Higher] チェックボックスをオンにすると、高いレベルの重大度を含めることができます。
Include Ack	確認応答済みの通知を含めます。
Network	指定したネットワークの通知を表示します。フィルタで入力を開始すると、一致するネットワークがドロップダウンに表示されます。該当するネットワークをクリックして選択します。 フィルタ内に複数のネットワークを含めることができます。

フィルタ	説明
Device	指定したデバイスの通知を表示します。フィルタで入力を開始すると、一致するデバイスがドロップダウンに表示されます。目的のデバイスをクリックして選択します。 フィルタに複数のデバイスを含めることができます。

（注） 個々のデバイスに対する通知は、デバイスの [Basic Info] パネルと [Detailed Info] パネルで確認できます。

通知の受信方法を制御するには、組織レベルまたはシステム レベルで通知設定を変更します。詳細については、「組織 （96 ページ）」または「モニタリングのデフォルト値」を参照してください。

デバイスの履歴通知の表示とフィルタリング

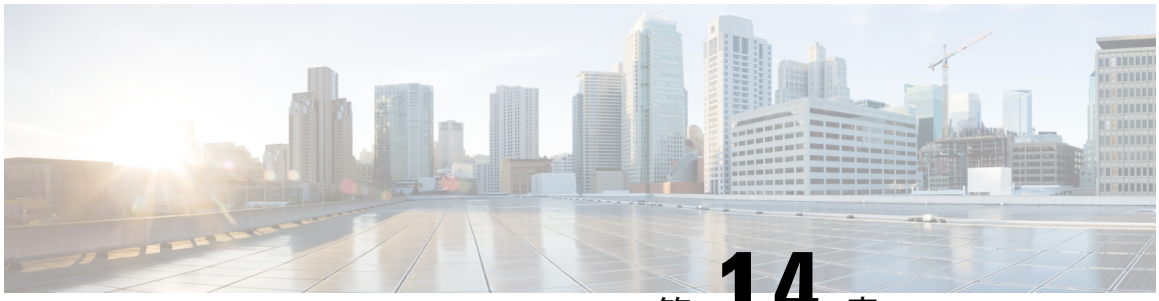
通知の発生または状態の変化は、Dashboard にイベントとして記録され、[Event Log] でも表示されます。イベントログのサブセットは、次のパネルで表示できます。

[Basic Info] パネルまたは [Device Detail] パネルには、個々のデバイスが表示されます。

[Basic Info] パネルには、過去 24 時間分のイベントのみが表示されます。

[Device Detail] パネルには、使用可能なデバイスのすべての履歴データが表示されます。

（注） [Device Detail] パネルは、フィルタ処理することで関心のあるイベントを特定することができます。履歴イベントの表示とフィルタ処理に関する詳細については、「イベント ログについて」を参照してください。



第 14 章

ジョブ管理

この章は、次の項で構成されています。

ジョブおよびジョブセンターについて

Cisco Business ダッシュボードによって実行されるタスクまたはアクションは、ジョブと呼ばれ、**ジョブセンター**で追跡されます。ジョブには、ユーザが開始したジョブと、システムによって自動的に開始されたジョブがあります。

ジョブセンターには、現在実行中または過去に発生したすべてのジョブが [Jobs] タブに表示されます。このタブには、ジョブのタイプ、影響を受けるデバイス、現在のステータス、ジョブが正常に完了したかどうかなどの詳細が示されます。

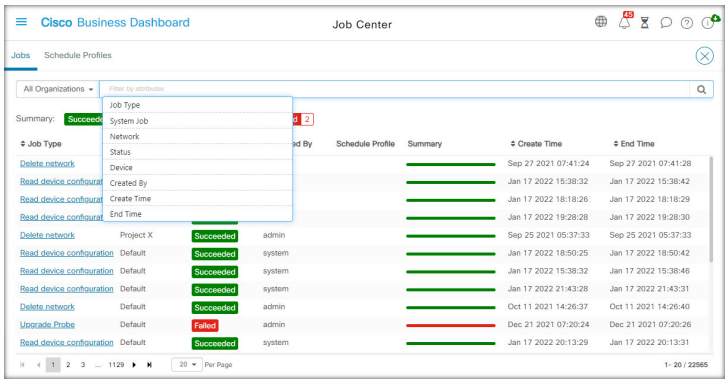
現在実行中のジョブと履歴ジョブの表示に加えて、ジョブセンターには [Schedule Profiles] の 2 番目のタブがあります。スケジュールプロファイルは、後の日付にスケジュールされているため、まだ発生していないジョブを表します。スケジュールプロファイルには、1 回だけ実行されるタスクと、定期的に実行するように定義されたタスクが含まれます。

ジョブおよびスケジュールプロファイルの表示およびフィルタリング

現在アクティブなジョブ、履歴ジョブ、およびまだ実行されていないジョブのスケジュールプロファイルを表示するには、以下の手順に従います。

ステップ 1 [Home] ウィンドウで、グローバルツールバーの右上隅にある [Job Center] アイコンをクリックします。

アイコンの番号バッジは、現在実行中のジョブの総数を示します。



現在アクティブなジョブと履歴ジョブはジョブセンターの [Jobs] タブに表示されますが、スケジュールプロファイルは [Schedule Profiles] タブに表示されます。ジョブタイプ、作成者、作成日時、ステータス情報などの情報がすべて表示されます。特定のジョブまたはスケジュールプロファイルの [Job Type] パラメータをクリックすると、詳細情報が表示されます。

ステップ 2 [Filter] ボックスは、テーブルに表示されるジョブまたはプロファイルを制限します。デフォルトでは、すべてのジョブとプロファイルが表示されます。既存のフィルタを変更するには、そのフィルタをダブルクリックして設定を変更します。新しいフィルタを追加するには、[Filter by attributes] ラベルをクリックし、ドロップダウンリストからフィルタを選択します。使用可能なフィルタは次のとおりです。

表 *16* : 使用可能なフィルタ

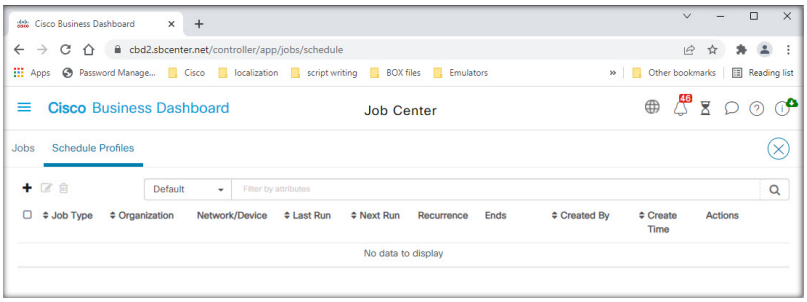
フィルタ	説明
Job Type	ドロップダウンリストから、表示するジョブまたはプロファイルのタイプを選択します。
System Job	このチェックボックスを使用して、システムによって開始されたジョブのみを表示するか、ユーザが開始したジョブのみを表示するかを制御します。このフィルタは、[Jobs] タブでのみ使用できます。
Status	ドロップダウンリストからステータス値を選択して、その状態のジョブのみに表示を制限します。このフィルタは、[Jobs] タブでのみ使用できます。
Device	選択したデバイスに影響するジョブまたはプロファイルのみに表示を制限します。
Created by	このフィルタを選択したときに表示されるフィールドにテキストを入力します。入力したテキストに一致する、ユーザが作成したジョブまたはプロファイルが表示されます。

フィルタ	説明
Create Time	このフィルタで提供される制御を使用して、時間間隔を指定します。この間隔で作成されたジョブまたはプロファイルが表示されます。
End Time	このフィルタで提供される制御を使用して、時間間隔を指定します。この間隔で実行を完了したジョブが表示されます。このフィルタは、[Jobs] タブでのみ使用できます。
Recurrence	ドロップダウンリストから、サポートされている頻度のいずれかを選択します。その頻度で繰り返されるように設定されたプロファイルが表示されます。このフィルタは、[Schedule Profiles] タブでのみ使用できます。
Network	選択したネットワークに影響するプロファイルのみに表示を制限します。
Next Run	このフィルタで提供される制御を使用して、時間間隔を指定します。この間隔で次に実行されるプロファイルが表示されます。このフィルタは、[Schedule Profiles] タブでのみ使用できます。

スケジュールプロファイルの管理

[Schedule Profiles] タブでは、定義済みのプロファイルを表示できるだけではありません。新しいプロファイルを作成し、既存のプロファイルを編集または削除することもできます。また、プロファイルによって作成されたすべてのジョブを検索することもできます。

新しいスケジュールプロファイルを作成するには、以下の手順に従います。



1. [Home] ウィンドウで、グローバルツールバーの右上隅にある [Job Center] アイコン

をクリックします。[Schedule Profiles] を選択します。

2. テーブルの左上にある [+]（プラス）アイコンをクリックします。
3. 表示されたフォームの [Job Detail] セクションで、ジョブタイプ、組織、およびターゲットデバイスまたはネットワークを選択します。選択したジョブタイプがネットワークに適用されない場合があります。
4. フォームの [Schedule] セクションで、繰り返しを選択し、ジョブの開始時刻を指定します。定期的なジョブの場合は、ジョブを終了するタイミングも指定します。

   ジョブは、次の変更ウィンドウまたは各変更ウィンドウで行われるようにスケジュールすることもできます。ジョブのタイミングは、ネットワークレベルまたは組織レベルで適用される変更ウィンドウ設定によって制御されます。変更ウィンドウの詳細については、変更期間の管理 （161 ページ）を参照してください。
5. 選択したジョブタイプによっては、追加情報が必要になる場合があります。その場合、追加のフィールドがフォームの [Schedule] セクションの下に表示されます。これらのフィールドに値を入力します。
6. 設定に問題なければ、[Save] をクリックします。

   新規アカウントを作成せずに終了する場合は、[Cancel] をクリックします。

既存のスケジュールプロファイルを編集するには、以下の手順に従います。

1. [Home] ウィンドウで、グローバルツールバーの右上隅にある [Job Center] アイコンをクリックします。[Schedule Profiles] タブを選択します。
2. 編集する必要のあるプロファイルを特定します。上記のフィルタを使用して、適切なプロファイルを特定できます。
3. テーブルの右端にある [Actions] 列を確認します。[Edit] アイコンをクリックします。
4. 提供されているフォームを使用してプロファイルを更新します。プロファイルのジョブタイプは変更できないことに注意してください。
5. 変更が完了したら、[Save] をクリックします。変更をキャンセルするには、[Cancel] をクリックします。

既存のスケジュールプロファイルを削除するには、以下の手順に従います。

1. [Home] ウィンドウで、グローバルツールバーの右上隅にある [Job Center] アイコンをクリックします。[Schedule Profiles] タブを選択します。
2. 削除するプロファイルを特定します。上記のフィルタを使用して、適切なプロファイルを特定できます。
3. プロファイルを削除するには [Action] 列の [Delete] アイコンをクリックします。

スケジュールプロファイルに関連付けられているすべてのジョブを表示するには、以下の手順に従います。

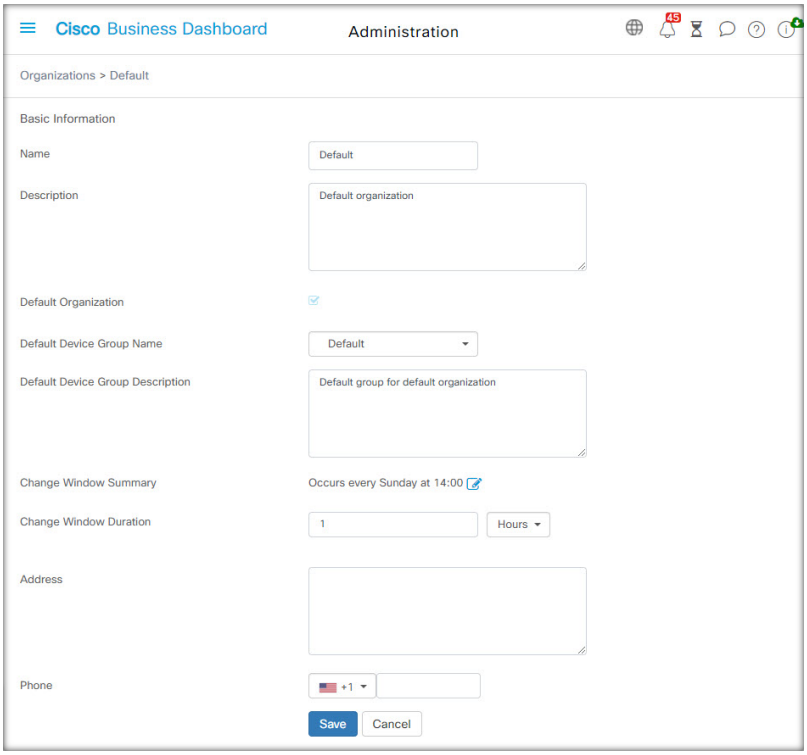
1. [Home] ウィンドウで、グローバルツールバーの右上隅にある [Job Center] アイコンをクリックします。[Schedule Profiles] タブを選択します。

2. 関連するジョブを検索するプロファイルを特定します。上記のフィルタを使用して、適切なプロファイルを特定できます。
3. [Actions] 列の [View Jobs] アイコンをクリックします。ビューが [Jobs] タブに切り替わり、このプロファイルに関連付けられているジョブのみが表示されます。

変更期間の管理

変更期間は、ユーザに影響を与えることなくネットワークを中断させる可能性のあるアクションを実行するために使用される期間です。通常、変更期間は週末または夜間の勤務時間外に発生するように定義されていますが、組織の要件に合わせて任意の時間に設定できます。変更期間は定期的な間隔であり、Cisco Business ダッシュボード のデフォルトでは毎週日曜日の午前 2 時から午前 3 時の間に発生するように設定されています。

変更期間は組織レベルで定義されますが、必要に応じてネットワークレベルで上書きできます。組織の変更ウィンドウを変更するには、以下の手順に従います。



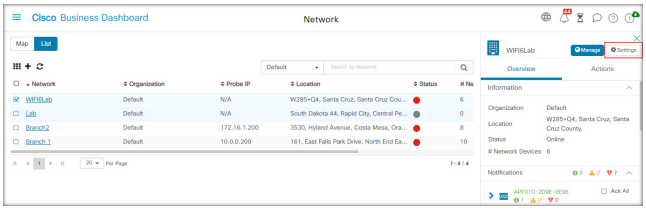
1. **[Administration]** > **[Organizations]** に移動します。
2. 変更する組織のオプションボタンを選択し、[Edit] アイコンをクリックします。
3. [Change Window Summary] パラメータの横にある [Edit] アイコンをクリックします。ポップアップウィンドウが開き、変更期間が表示される頻度と、期間を開始する日時を変更できます。適切なタイムゾーンを選択することで、開始時刻を組織のローカル時刻として指

定できるため、エラーが発生する可能性が低くなります。更新が完了したら、[Save] をクリックしてポップアップを閉じます。

4. 変更期間の時間も設定する必要があります。分単位または時間単位で指定でき、30分以上である必要があります。

5. 変更が完了したら、[Save] をクリックします。変更をキャンセルするには、[Cancel] をクリックします。

組織の変更ウィンドウとは異なる特定のネットワークの変更ウィンドウを設定するには、以下の手順に従います。



1. [Network] ページに移動します。

2. 変更するネットワークのチェックボックスを選択し、表示される [Network Info] パネルで [Settings] をクリックします。

3. 左上のネットワーク名の横にある [Edit] アイコンをクリックします。

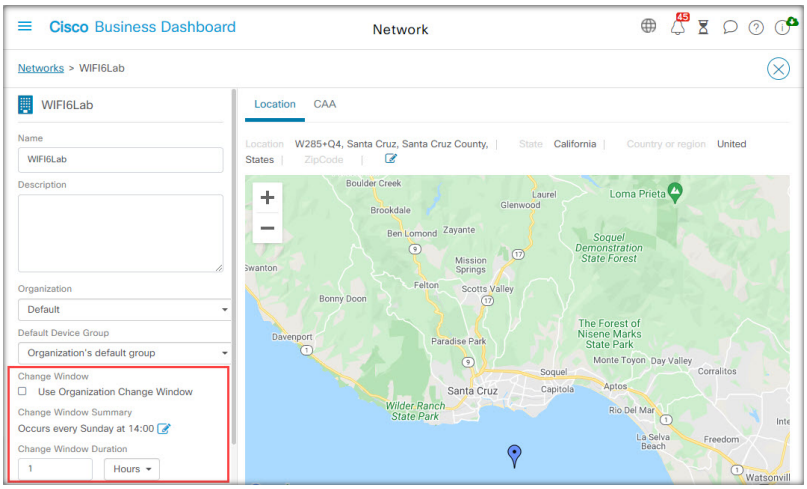
4. [Change Window] 見出しの下の、[Use Organization Change Window] チェックボックスをオフにします。

5. [Change Window Summary] パラメータの横にある [Edit] アイコンをクリックします。ポップアップウィンドウが開き、変更期間の実行頻度と開始時刻を変更できます。適切なタイムゾーンを選択することで、開始時刻を組織のローカル時刻として指定できるため、エラーが発生する可能性が低くなります。更新が完了したら、[Save] をクリックしてポップアップを閉じます。

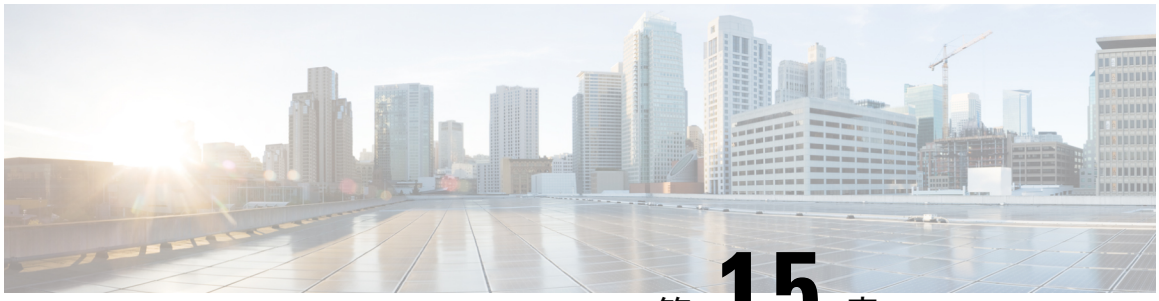
6. 変更期間の時間も設定する必要があります。分単位または時間単位で指定でき、30分以上である必要があります。

7. 変更が完了したら、[OK] をクリックします。変更をキャンセルするには、[Cancel] をクリックします。

組織変更ウィンドウを使用するようにネットワークを構成するには、以下の手順に従います。



1. [Network] ページに移動します。
2. 変更するネットワークのチェックボックスをオンにし、表示される [Network Info] パネルの [Settings] ボタンをクリックします。
3. 左上のネットワーク名の横にある [Edit] アイコンをクリックします。
4. [Change Window] 見出しの下の、[Use Organization Change Window] チェックボックスをオンにします。
5. 変更が完了したら、[OK] をクリックします。変更をキャンセルするには、[Cancel] をクリックします。



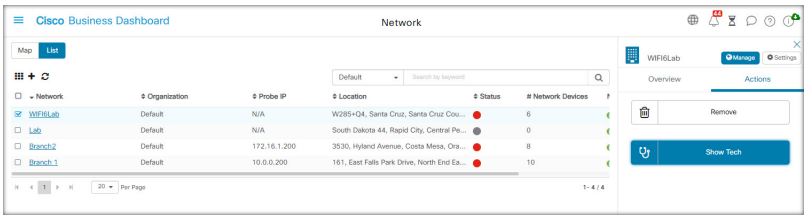
第 15 章

トラブルシューティング

この章は、次の項で構成されています。

ネットワーク診断情報の取得

Network Show Tech 機能を使用すると、ネットワークの診断情報を後で解析したり、サポートエンジニアに送信できる形式で容易にキャプチャできます。**Network Show Tech** は、Dashboard と Probe の接続の問題をトラブルシューティングしているイベントで、Dashboard UI から生成するか、Probe UI から直接生成することができます。**Network Show Tech** をキャプチャするには、次の手順に従います。



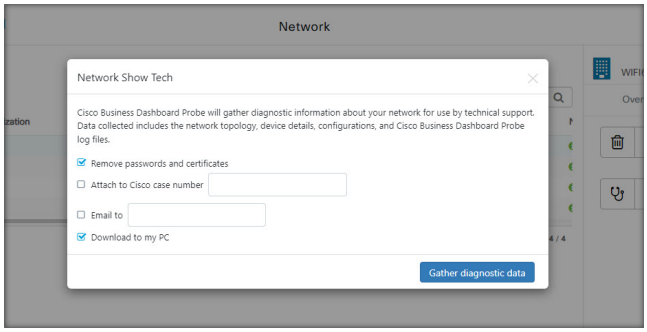
1. [Network] に移動し、チェックボックスをクリックし、診断情報を収集するネットワークを選択します。
2. [Actions] タブを選択し、[Show Tech] をクリックします。

   または、Probe の UI にログオンし、**[Troubleshooting]** > **[Network Show Tech]** に移動します。
3. チェックボックスを使用して、パスワードと証明書をデバイス設定から除外するかどうかと、診断情報をどこに送信するかを制御します。次のオプションを使用できます。
   - 診断情報を既存のシスコ サポート ケースに添付します。そのためには、フィールドにケース番号を入力します。
   - 電子メールを使用して診断情報を送信します。カンマ区切りの電子メールアドレスのリストをフィールドに入力します。

- 診断情報を PC にダウンロードします。

Probe から **Network Show Tech** を生成する場合は、サポートケースに電子メールを送信したり接続するオプションはありません。診断情報を PC にダウンロードする必要があります。

4. [Gather diagnostic data] をクリックします。



診断情報が zip ファイルとして配信され、収集したデータをナビゲートするための基本的な Web ページが含まれています。データにアクセスするには、以下の手順に従います。

1. 診断情報ファイルを PC に解凍します。
2. Web ブラウザを使用して、ディレクトリにある index.html ファイルを開きます。

Probe のログ設定の管理

Probe の [Log Settings] は、Dashboard と Probe の接続の問題をトラブルシューティングするイベントで、Dashboard UI から、または直接 Probe の UI から管理できます。ログ設定では、Probe がそのログファイルに保持する情報を制御します。

この情報は、Cisco Business ダッシュボード の問題を診断するエンジニアをサポートするために重要です。

特定のネットワークのログ設定を変更するには、次の手順に従います。

1. [Network] ページを開き、設定を変更するネットワークの横にあるチェックボックスをクリックします。
2. [Network overview] パネルの上部にある [Settings] ボタンをクリックします。
3. [Log Settings] タブを選択します。

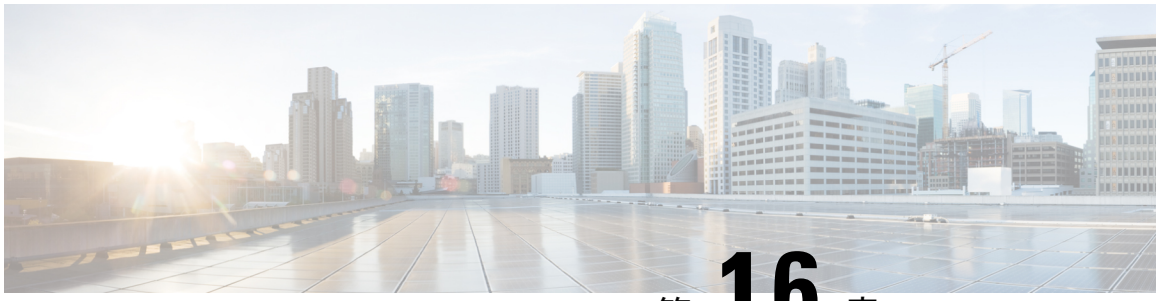
   または、Probe UI にログオンし、**[Administration]** > **[Log Settings]** に移動します。

使用可能な設定には以下のパラメータがあります。

表 *17 :* ログ設定

フィールド	説明
Log Level	ログに記録する詳細レベル。 • [Error]：エラー レベルのメッセージのみ • [Warning]：警告とエラー • [Info]（デフォルト）：情報メッセージ以上 • [Debug]：低レベルのデバッグ メッセージ含むすべてのメッセージ
Log Module	メッセージを保存するモジュール。 • [All]（デフォルト）：すべてのモジュール • [Call-home Agent]：Probe と Dashboard 間の通信 • [Discovery]：デバイス検出イベントとトポロジ検出 • [Northbound]：Dashboard と Probe 間の通信 • [Services]：ノースバウンドとサウスバウンド間のメッセージ変換 • [Southbound]：Probe とデバイス間の低レベル通信 • [System]：他のどのモジュールでも対象となっていないコア システム プロセス 必要に応じて複数のモジュールを選択できます。

Probe のログ ファイルは、[Network Show Tech] コンテンツに含まれます。[Network Show Tech] オプションの詳細については、ネットワーク診断情報の取得（165 ページ）を参照してください。



第 16 章

よく寄せられる質問

この章では、Cisco Business ダッシュボード の機能と、発生する可能性がある問題についてよく寄せられる質問に回答します。内容は次のカテゴリに分類されます。

一般的な FAQ

Q. Cisco Business ダッシュボード ではどのような言語がサポートされていますか。

A. Cisco Business ダッシュボード は以下の言語に翻訳されています。

- 中国語
- 英語
- フランス語
- ドイツ語
- 日本語

- スペイン語

検出の FAQ

Q. Cisco Business ダッシュボードはデバイスを管理するためにどのプロトコルを使用しますか。

A. Cisco Business ダッシュボードは各種のプロトコルを使用してネットワークを検出および管理します。特定のデバイスに対して正確にどのプロトコルが使用されるかは、デバイスの種類によって異なります。

使用されるプロトコルには以下のものがあります。

- Multicast DNS および DNS Service Discovery（*Bonjour* とも呼ぶ。*RFC 6762* と *6763* を参照）
- Cisco Discovery Protocol（CDP）
- Link Layer Discovery Protocol（『*IEEE specification 802.1AB*』を参照）
- 簡易ネットワーク管理プロトコル（SNMP）
- RESTCONF（*https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/* を参照）
- 独自の Web サービス API

Q. Cisco Business ダッシュボードはネットワークをどのように検出しますか。

A. Cisco Business ダッシュボード Probe は、CDP、LLDP、および mDNS アドバタイズメントをリッスンすることで、ネットワーク内のデバイスの初期リストを作成します。次に Probe は、サポートされているプロトコルを使用して各デバイスに接続し、CDP および LLDP 隣接テーブル、MAC アドレステーブル、関連するデバイス リストなどの追加情報を収集します。この情報はネットワーク内の追加のデバイスを識別するために使用され、すべてのデバイスが検出されるまでこのプロセスが繰り返されます。

Q. Cisco Business ダッシュボードはネットワークスキャンを行いますか。

A. Cisco Business ダッシュボードは広範囲のネットワークを積極的にスキャンすることはしません。Probe は ARP プロトコルを使用して直接接続されている IP サブネットをスキャ

ンしますが、その他のアドレス範囲をスキャンことはしません。Probe は検出されたデバイスごとに標準ポートの Web サーバと SNMP サーバの存在の有無もテストします。

設定の FAQ

Q. 新しいデバイスが検出されると何が起こりますか。その設定は変更されますか。

A. 新しいデバイスはデフォルト デバイス グループに追加されます。デフォルト デバイス グループに設定プロファイルが割り当てられている場合は、その設定が新たに検出されたデバイスに適用されます。

Q. デバイスをあるデバイス グループから別のデバイス グループに移動した場合、何が起こりますか。

A. 元のデバイス グループに現在適用されているプロファイルに関連付けられているすべての VLAN または WLAN 設定は削除され、元のグループに適用されない、新しいグループに適用されるプロファイルに関連付けられている VLAN または WLAN 設定がデバイスに追加されます。システム設定は、新しいグループに適用されるプロファイルによって上書きされます。新しいグループに対してシステム設定プロファイルが定義されていない場合、デバイスのシステム設定は変化しません。

セキュリティ上の留意事項の FAQ

Q. Cisco Business ダッシュボード ではどのポート範囲とプロトコルが必要ですか。

A. 以下の表に、Cisco Business ダッシュボード が使用するプロトコルとポートの一覧を示します。

表 *18 : Cisco Business* ダッシュボード：プロトコルとポート

ポート	方向	プロトコル	使用方法
TCP 22	着信	SSH	Dashboard へのコマンドラインアクセス。Cisco 仮想マシン イメージで SSH はデフォルトで無効になっています。
TCP 80	着信	HTTP	Dashboard への Web アクセス。セキュア Web サーバ（ポート 443）へのリダイレクト。
TCP 443	着信	HTTPS 多重化 TCP	Dashboard へのセキュア Web アクセス。 Probe と Dashboard 間の通信。

ポート	方向	プロトコル	使用方法
UDP 1812	着信	RADIUS	ユーザーアクセスを認証するときのダッシュボードへのデバイスアクセス。
TCP 50000 ～ 51000 （Microsoft Azure マーケットプレイスからデプロイされたシステムは TCP 50000 ～ 50049 を使用します）	着信	HTTPS	デバイスへのリモートアクセス。 この範囲は、[System] > [Platform Settings] ページを使用して制御できます。
UDP 53	発信	DNS	ドメイン名解決。
UDP 123	発信	NTP	時刻の同期。
TCP 443	発信	HTTPS	ソフトウェア アップデート、サポート ステータス、サービス終了通知などの情報を得るための、シスコ Web サービスへのアクセス。OS およびアプリケーション更新サービスへのアクセス。
UDP 5353	発信	mDNS	Dashboard をアドバタイズする、ローカルネットワークへのマルチキャスト DNS サービスアドバタイズメント。

Q. Cisco Business ダッシュボード Probe ではどのポート範囲とプロトコルが必要ですか。

A. 以下の表に、Cisco Business ダッシュボードプローブ が使用するプロトコルとポートの一覧を示します。

表 *19 : Cisco Business* ダッシュボード：プロトコルとポート

ポート	方向	プロトコル	使用方法
TCP 22	着信	SSH	Probe へのコマンドラインアクセス。Cisco 仮想マシン イメージで SSH はデフォルトで無効になっています。
TCP 80	着信	HTTP	Probe への Web アクセス。セキュア Web サーバ（ポート 443）へのリダイレクト。

ポート	方向	プロトコル	使用方法
TCP 443	着信	HTTPS	Probe へのセキュア Web アクセス。
UDP 5353	着信	mDNS	ローカル ネットワークからのマルチキャスト DNS サービス アドバタイズメントデバイス検出に使用。
UDP 53	発信	DNS	ドメイン名解決。
UDP 123	発信	NTP	時刻の同期
TCP 80	発信	HTTP	セキュア Web サービスが有効になっていないデバイスの管理。
UDP 161	発信	SNMP	ネットワーク デバイスの管理。
TCP 443	発信	HTTPS 多重化 TCP	セキュア Web サービスが有効になっているデバイスの管理ソフトウェア アップデート、サポート ステータス、サービス終了通知などの情報を得るための、シスコ Web サービスへのアクセス。 OS およびアプリケーション更新サービスへのアクセス。 Probe と Dashboard 間の通信。
UDP 5353	発信	mDNS	Probe をアドバタイズする、ローカルネットワークへのマルチキャスト DNS サービス アドバタイズメント。

Q. Cisco Business ダッシュボード はどのシスコサーバーと通信しますか。なぜですか。

A. 次の表に、Cisco Business ダッシュボード が通信するシスコサーバーとそのやり取りの目的を示します。

表 *20 : Cisco Business* ダッシュボード - シスコサーバー

ホストネーム	目的
tools.cisco.com	スマートライセンスで使用されます。スマートアカウントの Dashboard に十分なライセンスがあることを確認します。このサーバは、Dashboard インスタンスが Cisco Smart Licensing に登録されている場合にのみ使用されます。

ホストネーム	目的
api.cisco.com	ソフトウェア更新情報と製品ライフサイクル情報を取得するために使用されます。このサーバは、ソフトウェアの更新またはライフサイクルレポートが [System] > [Privacy Settings] で有効になっている場合にのみ使用されます。
dl.cisco.com download-ssc.cisco.com	シスコからソフトウェア更新ファイルをダウンロードするために使用されます。 これらのサーバは、[System] > [Privacy Settings] でソフトウェアの更新が有効になっているときに、ネットワークデバイスや Cisco Business ダッシュボードのアップグレード操作を実行する場合にのみ使用されます。
cloudsso.cisco.com	api.cisco.com との通信に先立つ Cisco Business ダッシュボードの認証に使用されます。このサーバは、ソフトウェアの更新またはライフサイクルレポートが [System] > [Privacy Settings] で有効になっている場合にのみ使用されます。
ciscoactiveadvisor.cisco.com	製品改善データを収集し、CAA へのアップロード機能をサポートするために使用されます。このサーバーは、製品の改善が [System] > [Privacy Settings] で有効になっている場合や、CAA へのアップロード機能を使用する場合にのみ使用されます。
www.cisco.com	ネットワーク通信の保護のためにシスコおよびサードパーティのサービスにより使用される X509 証明書を検証する目的で使用される、ルート認証局の署名証明書の更新を取得するために使用されます。

Q. Cisco Business ダッシュボードにはどのようなプロセスとシステムサービスが必要ですか。

A. 次の表に、Cisco Business ダッシュボードがシスコサーバで使用するプロセスとシステムサービスを示します。

表 *21 : Cisco Business* ダッシュボード - プロセスとシステムサービス

プロセス	詳細情報
Dashboard の必須プロセス	
/usr/lib/jvm/java-8-openjdk-amd64/bin/java … -jar /usr/lib/ciscobusiness/dashboard/lib/nm-aio-application-x.x.x-SNAPSHOT.jar	Dashboard のメインアプリケーション
/usr/lib/ciscobusiness/dashboard/bin/nginxsvc /usr/lib/ciscobusiness/dashboard/bin/nginx	ウェブ サーバ

プロセス	詳細情報
Dashboard の必須プロセス	
/usr/lib/ciscobusiness/dashboard/bin/mongosvc /usr/lib/ciscobusiness/dashboard/bin/mongod /usr/lib/postgresql/xx/bin/postgres postgres: xx/main:	データベース サービス
/bin/bash /usr/lib/ciscobusiness/dashboard/bin/freeradiussvc /usr/lib/ciscobusiness/dashboard/bin/freeradius	ユーザー認証サービス
/usr/lib/ciscobusiness/dashboard/bin/redissvc /usr/lib/ciscobusiness/dashboard/bin/redis-server	インメモリ キャッシュサービス
/usr/lib/ciscobusiness/dashboard/bin/rabbitmqsvc /usr/lib/ciscobusiness/dashboard/bin/rabbitmq-server /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd.smp erl_child_setup	メッセージブローカ
/usr/lib/ciscobusiness/dashboard/bin/bonjoursvc avahi-publish	マルチキャスト DNS アナウンスメント
/bin/sh /usr/share/contuit/contuit /bin/sh /usr/share/contuit-computations/contuit-computations /bin/sh /usr/share/contuit-monorepo/contuit-mop /bin/sh /usr/share/contuit-scheduler/contuit-scheduler /bin/sh /usr/share/contuit-shim/contuit-shim	外部アプリケーションとの統合が有効な場合にのみ必要
Dashboard の必須システムサービス	
/usr/sbin/rsyslog	ロギングサービス
/usr/sbin/cron	スケジューリングサービス
systemd-timesyncd	タイムサービス
avahi-daemon	マルチキャスト DNS リスナー

Q. Cisco Business ダッシュボード Probe にはどのようなプロセスとシステムサービスが必要ですか。

A. 次の表に、Cisco Business ダッシュボード Probe がシスコサーバで使用するプロセスとシステムサービスを示します。

表 *22 : Cisco Business* ダッシュボード - プロセスとシステムサービス

プロセス	詳細情報
Probe の必須プロセス	
/usr/lib/ciscobusiness/probe/bin/cbdprobe chagent	プローブのメインアプリケーション
/usr/lib/ciscobusiness/probe/bin/fpscan	デバイススキャンツール
/usr/lib/ciscobusiness/probe/bin/main /usr/lib/ciscobusiness/probe/bin/publish avahi-publish	マルチキャスト DNS アナウンスメント
nginx	Web サーバ Dashboard サーバに配置されている場合、プローブは Dashboard Web サーバを共有します。
Probe の必須システムサービス	
/usr/sbin/rsyslogd	ロギングサービス
/usr/sbin/cron	スケジューリングサービス
systemd-timesyncd	タイムサービス
avahi-daemon	マルチキャスト DNS リスナー
lldpd	LLDP ネイバー探索

Q. Cisco Business ダッシュボードと Probe 間の通信はどれほど安全ですか。

A. Dashboard と Probe 間の通信は、クライアントとサーバーの証明書で認証された TLS 1.2 セッションを使用して暗号化されています。セッションは Probe から Dashboard に対して開始されます。Dashboard と Probe 間の関連付けを最初に確立する際、ユーザは Probe 経由で Dashboard にログインする必要があります。

Q. Cisco Business ダッシュボードはデバイスに「バックドア」アクセスできますか。

A. いいえ。Cisco Business ダッシュボードは、サポートされているシスコデバイスを検出すると、検出されたデバイスの工場出荷時のログイン情報（ユーザー名/パスワード：cisco、SNMP コミュニティ：public）を使用してデバイスにアクセスしようとします。デバイス設定がデフォルトから変更されている場合は、ユーザーが正しいログイン情報を Cisco Business ダッシュボードに入力する必要があります。

Q. Cisco Business ダッシュボードに保存されているログイン情報はどの程度安全ですか。

A. Cisco Business ダッシュボードにアクセスするためのログイン情報は、SHA512 アルゴリズムを使用して不可逆的にハッシュ化されます。デバイスと、**Cisco Active Advisor** などの

その他のサービスのためのクレデンシャルは、AES-128アルゴリズムを使用して不可逆的に暗号化されます。

Q. Web UI 用のパスワードをなくした場合、どのようにすれば回復できますか。

A. Web UI のすべての admin アカウントのパスワードをなくした場合は、Probe のコンソールにログインして **cbdprobe recoverpassword** ツールを実行するか、Dashboard のコンソールにログインして **cisco-business-dashboard recoverpassword** ツールを実行することで、パスワードを回復できます。このツールは、ciscoアカウントのパスワードをデフォルトのciscoにリセットします。cisco アカウントが削除されている場合は、デフォルトのアカウントを使用してアカウントを作成します。以下に、このツールを使用してパスワードを回復するために実行するコマンドの例を示します。

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword Cisco Business Dashboard successful!
cisco@cisco-buisness-dashboard:~$
```

（注） Cisco Business ダッシュボード for AWS を使用する場合、パスワードは AWS インスタンス ID に設定されます。

Q. 仮想マシンブートローダーのデフォルトのユーザー名とパスワードは何ですか。

A. 仮想マシンブートローダーのデフォルトのログイン情報の場合、ユーザー名は **root** 、パスワードは **cisco**です。これらを変更するには、config_vm ツールを実行し、ブートローダーのパスワードを変更するかどうかを尋ねられたら、「yes」と応答します。

Q. ダッシュボードはネットワーク アクセス デバイスをどのように認証しますか。

A. ダッシュボードは 2 つのレベルの認証を使用します。

- まず、着信要求の送信元 IP アドレスが、NAT が使用されている場合はダッシュボードによって管理されるネットワークの外部 IP アドレスと比較され、NAT が使用されていない場合はネットワークの内部サブネットと比較されます。
- 次に、組織ごとに一意のランダム化されたRADIUSシークレットが作成され、ネットワーク アクセス デバイスによってその要求で使用される必要があります。

リモート アクセスの FAQ

Q. デバイスの管理インターフェイスに Cisco Business ダッシュボード から接続した場合、セッションはセキュリティ保護されますか。

A. Cisco Business ダッシュボード リモートアクセスセッションを、デバイスとユーザーの間でトンネリングします。Probe とデバイス間で使用されるプロトコルはエンドデバイスの設定によって変わりますが、Cisco Business ダッシュボード は、セキュアなプロトコルが有効になっていれば、必ずそのプロトコルを使用してセッションを確立します（たとえ

ば、HTTPS は HTTP よりも優先されます）。ユーザーが Dashboard を介してデバイスに接続している場合、セッションは、Dashboard と Probe の間を通過するときに、デバイスで有効になっているプロトコルにかかわらず、暗号化されたトンネルを通過します。ユーザーの Web ブラウザと Dashboard の間の接続は常に HTTPS になります。

Q. 別のデバイスとのリモート アクセス セッションをオープンしたときに、デバイスとのリモート アクセス セッションがすぐにログ アウトするのはなぜですか。

A. Cisco Business ダッシュボードを介してデバイスにアクセスすると、ブラウザは各接続を同じ Web サーバー（Dashboard）との接続であると見なすため、各デバイスからの cookie を他のすべてのデバイスに提供します。複数のデバイスが同じ cookie 名を使用する場合、あるデバイスの cookie が別のデバイスによって上書きされる可能性があります。これは、セッション cookie で最も頻繁に発生し、最後に訪れたデバイスに対してのみ cookie が有効であるという結果になります。同じ cookie 名を使用する他のすべてのデバイスはその cookie を無効と見なし、セッションをログアウトします。

Q. リモート アクセス セッションが以下のようなエラーで失敗するのはなぜですか。**アクセスエラー：リクエストエンティティが大きすぎます。**HTTP ヘッダーフィールドがサポートされているサイズを超えています。

A. 異なるデバイスと多数のリモートアクセスセッションを確立すると、ブラウザには Dashboard ドメイン用に大量の cookie が保存されます。この問題を回避するには、ブラウザ コントロールを使用してドメインの cookie をクリアしてから、ページを再ロードしてください。

ソフトウェア アップデートの FAQ

Q. Dashboard のオペレーティングシステムを最新に保つにはどうすればよいですか。

A. Dashboard は、オペレーティングシステムに Ubuntu Linux ディストリビューションを使用しています。パッケージとカーネルは、Ubuntu の標準的なプロセスを使用して更新できます。たとえば、手動更新を行うには、コンソールに cisco ユーザでログオンし、コマンド `sudo apt-get update` および `sudo apt-get upgrade` を実行します。システムを新しい Ubuntu リリースにアップグレードしてはならず、シスコによって提供されている仮想マシンに含まれているパッケージ、または最小限の Ubuntu インストールの一部としてインストールされたパッケージ以外の追加パッケージをインストールしないことを推奨します。

Q. Dashboard で Java を更新するにはどうすればよいですか。

A. Cisco Business ダッシュボードは Ubuntu リポジトリの OpenJDK パッケージを使用します。OpenJDK はコア オペレーティング システムの更新の一部として自動的に更新されます。

Q. Probe のオペレーティング システムを最新に保つにはどうすればよいですか。

A. Cisco Business ダッシュボードはオペレーティングシステムに Ubuntu Linux ディストリビューションを使用しています。パッケージとカーネルは、Ubuntu の標準的なプロセスを使用して更新できます。たとえば、手動更新を行うには、コンソールに cisco ユーザでログオンし、コマンド `sudo apt-get update` および `sudo apt-get upgrade` を実行します。システムを新しい Ubuntu リリースにアップグレードしてはならず、シスコによって提供されている仮想マシンに含まれているパッケージ、または最小限の Ubuntu インス

トールの一部としてインストールされたパッケージ以外の追加パッケージをインストールしないことを推奨します。

Q. Raspberry Pi を使用している場合に Probe のオペレーティングシステムを最新に保つにはどうすればよいですか。

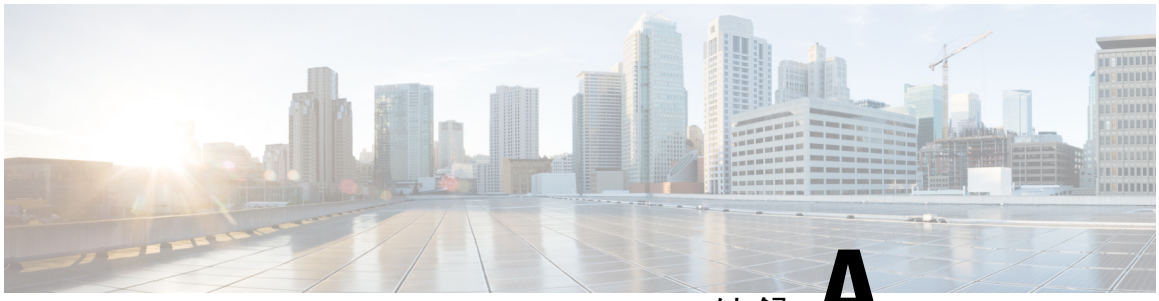
A. Raspbian パッケージおよびカーネルは、Debian ベースの Linux ディストリビューションに使用される標準プロセスを使用して更新できます。たとえば、手動更新を行うには、コンソールに cisco ユーザでログオンし、コマンド `sudo apt-get update` および `sudo apt-get upgrade` を実行します。システムを Raspbian の新しいメジャーリリースにアップグレードすることはできません。Raspbian ディストリビューションの「Lite」バージョンの一部としてインストールされているパッケージ、および Probe インストーラによって追加されたパッケージよりも新しいバージョンのパッケージを追加しないことを推奨します。

Q. Cisco Business Dashboard 2.3.0 に Ubuntu 20.04（Focal Fossa）のサポートが追加されました。システムを 2.3.0 にアップグレードした場合、オペレーティングシステムを Ubuntu 16.04 から Ubuntu 20.04 にアップグレードできますか。

A. 残念ながら、2 つのオペレーティング システム リリース間の変更は、インプレースアップグレードを実行するには大きすぎます。Ubuntu 16.04 を実行している既存のシステムがある場合は、Dashboard をリリース 2.3.0 にアップグレードしてから、**[System]** > **[Backup]** ページを使用して Dashboard のバックアップを作成する必要があります。次に、Ubuntu 20.04 を使用して Dashboard を再構築するか、Ubuntu 20.04 に基づいて新しい Dashboard インストールを実行します。その後、古い Dashboard から新しい Dashboard にバックアップを復元できます。

Q. Cisco Business Dashboard 2.3.0 に Ubuntu 20.04（Focal Fossa）のサポートが追加されました。システムを 2.3.0 にアップグレードした場合、オペレーティングシステムを Ubuntu 16.04 から Ubuntu 20.04 にアップグレードできますか。

A. 残念ながら、2 つのオペレーティング システム リリース間の変更は、インプレースアップグレードを実行するには大きすぎます。Ubuntu 16.04 を実行している既存のシステムがある場合は、Dashboard をリリース 2.3.0 にアップグレードしてから、**[System]** > **[Backup]** ページを使用して Dashboard のバックアップを作成する必要があります。次に、Ubuntu 20.04 を使用して Dashboard を再構築するか、Ubuntu 20.04 に基づいて新しい Dashboard インストールを実行します。その後、古い Dashboard から新しい Dashboard にバックアップを復元できます。



付録 A

付録 A：設定テンプレートの管理

この付録の内容は、次のとおりです。

設定テンプレートの管理

構成テンプレートは、複数のデバイスがあって構成要件が非常に似ているものの、少数のパラメータについてはデバイスごとに異なっている必要がある場合に使用できます。たとえば、ネットワークでは、すべてのスイッチに対して同一の設定を使用できますが、各スイッチには一意のホスト名と管理 IP アドレスが必要です。設定テンプレートを使用すると、すべての一般的な設定が含まれている単一の構成ファイルと、一意である必要がある設定要素のプレースホルダを使用できます。

設定テンプレートには2つの部分があります。設定自体と、デバイスレコードが作成されるときにユーザインターフェイスにどのようにプレースホルダを表示するかを制御するメタデータです。次の項では、それぞれについて詳しく説明します。

設定構文

設定テンプレートの設定部分は、通常のデバイス設定と非常によく似たテキストドキュメントです。設定テンプレートを作成する際は、テンプレートで有効にする必要がある機能と設定を使用してすでに設定されているサンプルデバイスから取得した設定のバックアップから始めることを推奨します。設定テンプレートは、デバイス固有のパラメータ（ホスト名など）がプレースホルダに置き換えられる点で、デバイス設定とは異なります。

新しいデバイスレコードを作成すると、設定テンプレートの各プレースホルダに正しい値を指定できるフォームが表示されます。これらの値は、デバイスに送信される実際の設定を生成するために、設定テンプレートとマージされます。

付録 A：設定テンプレートの管理

（注） プレースホルダ値は、設定がデバイスに送信されるときに設定テンプレートとマージされます。つまり、デバイスがマネージャに接続する前にシステム変数が変更された場合、最終的なデバイス設定はプレビューに表示されるものと異なる場合があります。

設定は、Mustache のテンプレート（*https://mustache.github.io/*）として作成されます。Mustache を使用すると、次のような、Mustache ドキュメントでタグと呼ばれるさまざまなプレースホルダを使用できます。

- 単純な変数。プレースホルダは、デバイスレコードで指定された値に置き換えられます。単純な変数の形式は **{{name}}** です。
- セクション。プレースホルダで設定のブロック（必要な場合は他のプレースホルダも含む）を囲みます。セクションの内容は、最終的な設定から除外するか、1回だけ含めるか、あるいは複数回繰り返すことができます。

  このタイプのプレースホルダの動作は、テンプレート内のメタデータと、デバイスレコードを作成するときにユーザーが指定する値によって定義されます。

  セクションの形式は **{{#name}}…{{/name}}** です。ここで、最初のタグでブロックの先頭を示し、2 番目のタグで末尾を示します。
- コメントは設定テンプレートをドキュメント化するために使用されることがあります。コメントの形式は {{**! This is a comment**}} です。

次に、単純なテンプレートの例を示します。

```
!
hostname {{hostname}}
!
{{! Insert a list of VLANs}}
{{#vlans}}
interface vlan {{vlan-id}}
 name {{vlan-name}}
!
{{/vlans}}
```

この例では、いくつかの異なるプレースホルダが使用されています。

- **{{hostname}}** は単純な変数です。これは、デバイスレコード内でホスト名に設定されている値に置き換えられます。
- ホスト名設定の直後にコメントがあります。このコメントは、デバイスに送信される設定には組み込まれません。
- **{{#vlans}}...{{/vlans}}** は、個々の VLAN のリストを保持するためにこの例で使用されているセクションです。デバイスレコードで定義されている各 VLAN について、このコンテナの内容のコピーがデバイス設定で作成されます。
- **{{vlan-id}}** と **{{vlan-name}}** はどちらも単純な変数であり、{{#vlans}} リスト内に含まれています。デバイスレコードが作成されると、 **{{vlan id}}** と **{{vlan name}}** に複数の値を指

付録 A：設定テンプレートの管理

定できます。これらの値は、これらの VLAN をそれぞれに作成するために必要な設定の生成に使用されます。

Mustache 構文の詳細については、*https://mustache.github.io/mustache.5.html* の Mustache man ページを参照してください。

テンプレートメタデータ

各設定テンプレートには、デバイスレコードの作成時に各プレースホルダをユーザに提示する方法を記述したメタデータが含まれています。このメタデータは、テンプレートエディタを使用してテンプレートを作成するときに生成されます。

設定テンプレートを作成または編集する際には、左側に設定自体が、右側に各プレースホルダのメタデータを設定できるフォームが表示されたテンプレートエディタが表示されます。

設定内の各プレースホルダは、次のコントロールとともに右側に表示されます。

- [Required] チェックボックス。このコントロールは、ユーザがこのプレースホルダの値を指定する必要があるかどうかを決定します。
- [Type] ドロップダウンリスト。このドロップダウンリストでプレースホルダのタイプを選択して、そのプレースホルダのユーザに対する表示方法を制御します。
- [Title]。GUI 上でユーザによりわかりやすいパラメータの名前を指定するために使用されます。プレースホルダにタイトルが指定されていない場合は、プレースホルダ自体が表示されます。
- [Edit] アイコン。一部のタイプには、プレゼンテーションを制御するためのより多くの設定があります。たとえば、文字列のプレースホルダを IP アドレスや URL としてさらに絞り込むことができます。その場合に、入力したテキストの形式が正しくないと、入力フォームにエラーが表示されます。さらに、一部のタイプでは、ユーザ入力ではなく、システム情報に基づいて設定することもできます。詳細については、以下の「システムと動的変数」を参照してください。
- [Move up/down] コントロール。これらの矢印を使用すると、ユーザにプレースホルダを表示する順序を変更できます。プレースホルダは、設定に表示される順序ではなく、ユーザが最も理解しやすいという条件に基づいてグループ化することができます。

また、テンプレートエディタにはプレビュー機能があり、デバイスレコードを作成および編集するときに、プレースホルダの形式がユーザにどのように表示されるかを示す例として使用できます。

プレースホルダのタイプ

次のプレースホルダのタイプを使用できます。

- [String]：このタイプのプレースホルダは、単純なテキスト入力ボックスとして GUI に表示されます。
- [Integer]：整数はテキスト入力ボックスとして表示され、表示される数値を増減するためのコントロールが備わっています。このフィールドに入力できるのは数字のみです。

- [boolean]：ブールプレースホルダが GUI にチェックボックスとして表示されます。このチェックボックスをオンにすると、プレースホルダでは文字列値が「true」に設定されます。このチェックボックスをオフした場合は、値は「false」になります。また、セクションをブールとして指定することもできます。この場合、そのセクション内に含まれている設定はそのセクションのチェックボックスがオンになっている場合にのみ含めることができます。
- [Container]：コンテナタイプは、フォーム内で他のプレースホルダをグループ化するために使用できます。
- [List]：リストは、生成された構成ファイルで複数回繰り返される可能性のある設定のコンテナまたはセクションです。リスト内のプレースホルダにフォーム要素が生成されると、リスト内の要素を追加または削除するためのコントロールが追加されます。

上記の単純なタイプに加えて、[Edit] アイコンをクリックすると文字列変数をさらに絞り込むことができます。利用可能なオプションは下記の通りです。

- プレースホルダにデフォルト値を指定する。
- 文字列プレースホルダの最小長または最大長を設定する。
- 選択可能な事前に定義された選択肢のリストを指定する（[Enum] オプションを使用）。
- 文字列の形式をホスト名、URI、IPv4 アドレス、または IPv6 アドレスのいずれかに制限する。大量のコンテンツを入力する可能性が高い場合は、文字列をテキストエリアとして指定することもできます。

システム変数と動的変数

プレースホルダはユーザー入力から値を取得するだけでなく、システム内で定義されたパラメータから値を取得することもできます。システム変数は、マネージャの IP アドレスなど、マネージャ自体に定義されているパラメータです。

システム変数から値を取得するようにプレースホルダを設定することで、マネージャはユーザの介入なしにその値を設定に挿入します。一部の複雑な展開では、システム変数が正しく機能するようにするためユーザ入力が必要になる場合があります。詳細については、プラットフォーム設定の管理 （126 ページ）を参照してください。

動的変数はシステム変数に似ていますが、ログインしているユーザーやデバイスが属するデバイスグループなどの情報に基づいて動的に生成される値です。システム変数と動的変数は、デバイスとシステム間でのテンプレートの移植性を高めるために使用されます。

設定テンプレートの作成

設定テンプレートを作成する場合は、まず適切なタイプのネットワークデバイスを目的の設定値で設定した後、そのデバイス設定のバックアップを作成してマネージャにアップロードし、それを開始点として使用することをお勧めします。

付録 A：設定テンプレートの管理

または、[Save As]機能を使用して既存のテンプレートのコピーを作成することもできます。いずれの方法でも、既存の設定から開始することで、テンプレートの作成にかかる時間を短縮し、目的の結果を得るために必要なリビジョン数を減らすことができます。

新しいテンプレートを作成する場合は、そのテンプレートが所属する組織と、テンプレートが使用される可能性がある製品 ID（PID）を指定する必要があります。製品 ID には ***'s** と **?'s** をワイルドカード文字として使用できます。

開始時の設定を作成した後は、次のプロセスを使用してその設定を更新できます。

1. **[Network Plug and Play]** > **[Configurations]** に移動します。
2. 構成を選択し、[edit]アイコンをクリックして、テンプレートエディタで開始構成を開きます。

   テンプレートエディタが表示され、テキストエディタウィンドウの左側に最初の構成ファイルが示されます。テキストエディタでは、検索、置換、いくつかのカーソル操作のキーシーケンスなど、多くの一般的な編集機能がサポートされています。コマンドのリストについては、以下の表を参照してください。
3. 「設定構文 （181 ページ）」の説明に従って、プレースホルダを挿入して設定を変更します。新しいプレースホルダが挿入されるたびに、対応するエントリが右側のフォームに追加されます。
4. 右側のフォームを使用して各プレースホルダに関連付けられているメタデータを変更し、プレースホルダが最適な方法でユーザに表示されるようにします。メタデータの指定に関する詳細については、上記の「設定テンプレートの管理 （181 ページ）」を参照してください。[Preview] 機能を使用すると、デバイスレコードが作成されるときに、ユーザーにフォームがどのように表示されるかを確認できます。
5. デバイス間で異なるすべての設定パラメータに対してプレースホルダを作成するまで、ステップ 3 と 4 を繰り返します。
6. 作成したテンプレートに問題がなければ、[Save] をクリックします。

（注） テンプレートを保存するたびに、新しいバージョンのテンプレートが作成されます。古いバージョンのテンプレートは、明示的に削除しない限り、マネージャに保持されます。テンプレートがデバイスに割り当てられると、そのテンプレートの特定のバージョンがデフォルトで最新バージョンに割り当てられます。新しいバージョンが作成されても、既存のデバイスは作成時に割り当てられたバージョンを引き続き使用します。デバイスに現在割り当てられているテンプレートバージョンは削除できません。

付録 A：設定テンプレートの管理

表 *23 :* 一般的なエディタコマンド

機能	説明	キーのバインド	
		PC	Mac
Select All	エディタの内容全体を選択します。	Ctrl+A	Cmd+A
Kill Line	行のカーソルの後の部分を削除します。空白のみで構成されている場合は、行の末尾の改行も削除されます。		Ctrl+K
Delete Line	最後の改行を含め、カーソルの下の行全体を削除します。	Ctrl+D	Cmd+D
Undo	最後の変更を元に戻します。	Ctrl-Z	Cmd+Z
Redo	最後に元に戻した変更をやり直します。	Ctrl+Y	Shift+Cmd+Z Cmd+Y
Go Doc Start	カーソルをドキュメントの先頭に移動します。	Ctrl+Home	Cmd+↑ Cmd+Home
Go Doc End	カーソルをドキュメントの末尾に移動します。	Ctrl+End	Cmd+End Cmd+↓
Go Line Start	カーソルを行の先頭に移動します。	Alt+←	Ctrl+A
Go Line End	カーソルを行の末尾に移動します。	Alt+→	Ctrl+E
Indent More	現在の行または選択項目をインデントします。	Ctrl-]	Cmd+]
Indent Less	現在の行または選択項目のインデントを解除します。	Ctrl+[	Cmd+[
Find		Ctrl+F	Cmd+F
Find Next		Ctrl+G	Cmd+G
Find Prev		Shift+Ctrl+G	Shift+Cmd+G
Replace		Shift+Ctrl+F	Cmd+Alt+F
Replace All		Shift+Ctrl+R	Shift+Cmd+Alt+F

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。