



Cisco Business Dashboard & Probe バージョン 2.4.1 アドミニストレーションガイド

初版：2020年7月14日

最終更新：2022年4月19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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

【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。



The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries.

© 2021 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	Cisco Business ダッシュボードの概要 1
	Cisco Business ダッシュボードについて 1
	対象読者 2
	関連資料 2
	用語 3
	Cisco Business Dashboardのシステム要件 4
	Cisco Business Dashboard Probe のシステム要件 6

第 2 章	Cisco Business Dashboard & Probe の使用 9
	Cisco Business Dashboard GUI の使用 9
	Cisco Business Dashboard Probe GUI の使用 12
	Cisco Business Dashboard & Probe のアップグレード 15
	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 16

第 3 章	監視ダッシュボード 19
	監視ダッシュボードについて 19
	ウィジェットの追加 20
	ウィジェットの変更 21
	ウィジェットの削除 22
	ダッシュボードのレイアウトの変更 22

第 4 章	Network 25
	ネットワークについて 25
	ネットワークの詳細について 27

ネットワークビューについて	28
トポロジマップとツールの概要	28
基本的なデバイス情報の表示	32
デバイスアクションの実行	34
デバイス管理インターフェイスへのアクセス	36
詳細なデバイス情報の表示	36
[Floor Plan] の使用方法	39

第 5 章	インベントリ	43
	デバイス インベントリの表示	43

第 6 章	ポート管理	47
	ポート管理について	47

第 7 章	Network Configuration	51
	ネットワーク設定について	51
	ウィザードの使用法	51
	時刻管理の設定	52
	DNS リゾルバの設定	53
	認証の設定	54
	仮想 LAN の設定	55
	ワイヤレス LAN の設定	57

第 8 章	ネットワーク プラグアンドプレイ	59
	ネットワーク プラグアンドプレイについて	59
	ネットワーク要件	59
	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	62
	ネットワーク プラグアンドプレイ サービスの設定	63
	ネットワーク プラグアンドプレイのモニタリング	70

第 9 章	イベント ログ	73
-------	----------------	----

イベント ログについて 73

第 10 章

Reports 75

レポートの概要 75
 ライフサイクルレポートの表示 75
 サポート終了レポートの表示 77
 メンテナンス レポートの表示 78
 ワイヤレス ネットワーク レポートの表示 79
 ワイヤレス クライアント レポートの表示 82

第 11 章

Administration 87

管理について 87
 組織の管理 88
 デバイス グループ (Device Groups) 90
 デバイスのクレデンシヤル 92
 ユーザの管理 93
 モニタリングのデフォルト値の変更 96
 モニタリングプロファイルの管理 97
 ログイン試行の表示 99
 レポート設定の管理 100

第 12 章

System 101

システムについて 101
 ライセンスの管理 102
 証明書の管理 104
 電子メール設定の管理 107
 API 使用状況の表示 108
 Dashboard 設定のバックアップと復元 109
 プラットフォーム設定の管理 110
 プライバシーの管理 112
 ログ設定の管理 115

ローカル Probe の管理	117
統合設定の管理	117
Connectwise Manage	117
サポートされる機能	118
前提条件	118
Connectwise Manage 統合の設定	119
Connectwise Manage 統合の使用	123
Webex	128
サポートされる機能	128
前提条件	128
Webex の統合の設定	129
Webex 統合の使用	130

第 13 章**通知 133**

通知について	133
サポートされる通知	133
現在のデバイスの通知の表示とフィルタリング	135
デバイスの履歴通知の表示とフィルタリング	137

第 14 章**ジョブ管理 139**

ジョブおよびジョブセンターについて	139
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	139
スケジュールプロファイルの管理	141
変更期間の管理	142

第 15 章**トラブルシューティング 145**

ネットワーク診断情報の取得	145
Probe のログ設定の管理	146

第 16 章**よく寄せられる質問 149**

よくある質問 (FAQ)	149
--------------	-----

検出の FAQ	150
設定の FAQ	151
セキュリティ上の留意事項の FAQ	151
リモートアクセスの FAQ	157
ソフトウェア アップデートの FAQ	158

第 17 章**付録 A : 設定テンプレートの管理 161**

概要	161
設定構文	161
設定テンプレートの作成	164



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。

- [Cisco Business ダッシュボードについて](#) (1 ページ)
- [対象読者](#) (2 ページ)
- [関連資料](#) (2 ページ)
- [用語](#) (3 ページ)
- [Cisco Business Dashboardのシステム要件](#) (4 ページ)
- [Cisco Business Dashboard Probe のシステム要件](#) (6 ページ)

Cisco Business ダッシュボードについて

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、ファームウェアアップデートのリリースや、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。Probe 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管理されている場合、デバイスに対して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。

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るすべてのデバイスのリストについては、『[Cisco Business Dashboard - Device Support List](#)』 [英語] 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。

• 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。詳細については、場所列に記載されているパス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
Oracle VirtualBox	Cisco Business Dashboard Installation Guide for Oracle VirtualBox
Microsoft Hyper-V	Cisco Business Dashboard Installation Guide for Microsoft Hyper-V

サポートされるプラットフォーム	参照先
VMware vSphere、ワークステーション、およびフュージョン	Cisco Business Dashboard Installation Guide for VMware
Ubuntu Linux (Dashboard & Probe) および Raspbian Linux (Probe のみ)	Cisco Business Dashboard 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。
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。 <ul style="list-style-type: none"> 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/ 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。

用語	説明
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。
<ul style="list-style-type: none"> • 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	任意の Windows PC から vCenter Server または ESXi に、ユーザーがリモート接続できるようにするユーザー 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、およびモニター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。
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。

Cisco Business Dashboardのシステム要件

Cisco Business ダッシュボードは、Ubuntu Linux ディストリビューションで使用するためのインストーラとして、仮想マシンイメージとして配布され、AWS マーケットプレイス (<https://aws.amazon.com/marketplace>) を通じて Amazon Web Services 用に利用できます。

仮想マシンで Cisco Business ダッシュボード を実行する場合、ハイパーバイザは次のいずれかである必要があります。

- Microsoft Hyper-V バージョン 10.0 以降
- Oracle VirtualBox バージョン 6.1 以降
- VMWare

- ESXi バージョン 6.0 以降
- Fusion バージョン 11.5 以降
- Workstation バージョン 15.1 以降

Ubuntu Linux で Cisco Business ダッシュボード を実行するには、ご使用の環境が、64 ビット Intel アーキテクチャ プラットフォーム上で Ubuntu バージョン 16.04.x (Xenial Xerus) または 20.04.x (Focal Fossa) を実行している必要があります。シスコでは、Ubuntu サーバーディストリビューションを使用すること、および Cisco Business ダッシュボード で必要となるパッケージのみをインストールすることをお勧めします。

表 1 に、管理下のデバイスの数に基づいて Cisco Business ダッシュボード に必要となるコンピューティングリソースを示します。

表 1: Cisco Business ダッシュボード コンピューティングリソースの要件

サポート対象デバイス数	vCPU 数	RAM	ディスク容量
最大 300	2	4GB	60 GB
最大 2500 台	12	24 GB	60 GB

AWS で Cisco Business ダッシュボード を実行するには、AWS アカウントが必要です。次の AWS インスタンスタイプがサポートされています。

- c5.large : 最大 300 台の管理対象デバイス
- c5.4xlarge : 最大 2,500 台の管理対象デバイス

Cisco Business ダッシュボード は Web ユーザーインターフェイスを通じて管理されます。このインターフェイスを使用するには、以下のいずれかのブラウザが必要です。

- Apple Safari (MacOS のみ) : 2 つの最新メジャーバージョン
- Google Chrome : 最新バージョン
- Microsoft Edge : 2 つの最新メジャーバージョン
- Mozilla Firefox : 最新バージョン



(注) Safari を使用している場合は、Cisco Business ダッシュボードプローブ からの証明書が [Always Trust] に設定されていることを確認します。そうでないと、セキュア Web ソケットの使用に依存する特定の機能が失敗することが予期されます。これは、Safari Web ブラウザの制限です。

ネットワークで、Cisco Business ダッシュボードプローブ のすべてのインスタンスが Cisco Business ダッシュボード との TCP 接続を確立できる必要があります。使用されるポートとプロトコルの詳細については、「よく寄せられる質問」を参照してください。

Cisco Business Dashboard Probe のシステム要件

Cisco Business ダッシュボードプローブは仮想マシンイメージとして配布され、また、次のオペレーティングシステムで使用するインストーラとして配布されます。

- 64 ビット インテルアーキテクチャプラットフォームで実行する Ubuntu Linux ディストリビューション
- Raspberry Pi で実行する Raspbian Linux ディストリビューション

Cisco Business ダッシュボードプローブは、高実績の Cisco 100 ～ 500 シリーズ製品の組み込み機能としても使用できます。

Cisco Business ダッシュボードプローブを仮想マシンとして実行するには、お使いの環境が次の要件を満たしている必要があります。

- ハイパーバイザ：
 - Microsoft Hyper-V バージョン 10.0 以降
 - Oracle VirtualBox バージョン 6.1 以降
 - VMWare
 - ESXi バージョン 6.0 以降
 - Fusion バージョン 11.5 以降
 - Workstation バージョン 15.1 以降
- 仮想マシン リソースの要件は次のとおりです。
 - CPU：64 ビット インテルアーキテクチャ X1
 - メモリ：512 MB
 - ディスク領域：5 GB

Ubuntu Linux オペレーティングシステムで Cisco Business ダッシュボードを実行するには、ご使用の環境が次の要件を満たしている必要があります。

- Ubuntu 16.04 Xenial Xerus (Cisco Business ダッシュボードプローブ バージョン 2.2.x および 2.3.x)
- Ubuntu 20.04 Focal Fossa (Cisco Business ダッシュボードプローブ バージョン 2.3.x 以降)
- CPU：64 ビット インテルアーキテクチャ X1
- メモリ：512 MB
- ディスク領域：5 GB

Raspberry Pi オペレーティングシステムで Cisco Business ダッシュボードプローブ を実行するには、お使いの環境が次の要件を満たしている必要があります。

- ハードウェア：Raspberry Pi 3 モデル B/B+ または Raspberry Pi 4 モデル B
- ディスク領域：5 GB
- OS：Raspberry Pi OS Buster

Cisco Business 製品で組み込みアプリケーションとして Cisco Business ダッシュボードプローブ を実行するには、Cisco Business ダッシュボードプローブ の機能をサポートしているファームウェアバージョンを実行するサポート対象の製品が必要です。ハードウェアとバージョンの要件の詳細については、「[Cisco Business Dashboard - Device Support List](#)」[英語]を参照してください。また、プラットフォーム固有のその他の要件を決定するには、製品の管理ガイドも参照してください。

Cisco Business ダッシュボードプローブ は Web ユーザインターフェイスを通じて管理されます。このインターフェイスを使用するには、以下のいずれかのブラウザが必要です。

- Apple Safari (MacOS のみ)：2 つの最新メジャーバージョン
- Google Chrome：最新バージョン
- Microsoft Edge：2 つの最新メジャーバージョン
- Mozilla Firefox：最新バージョン

Cisco Business ダッシュボードプローブ は、次の要件を満たしているネットワークデバイスを監視し、それらにアクセスします。

- Cisco Business ダッシュボードプローブ が実行している PC と同じサブネットに存在するか、または管理対象デバイスに直接接続され、TCP/IP を通じて到達できる必要があります。
- サポート対象の Cisco Business または Cisco Small Business 100 ～ 500 シリーズデバイスである必要があります。



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 (9 ページ)
- Cisco Business Dashboard Probe GUI の使用 (12 ページ)
- Cisco Business Dashboard & Probe のアップグレード (15 ページ)
- 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 (16 ページ)

Cisco Business Dashboard GUI の使用

ナビゲーション ペインリンクの説明と Cisco Business ダッシュボード GUI の概要。

[Home] ウィンドウ

図 1: Cisco Business Dashboard ホームページ

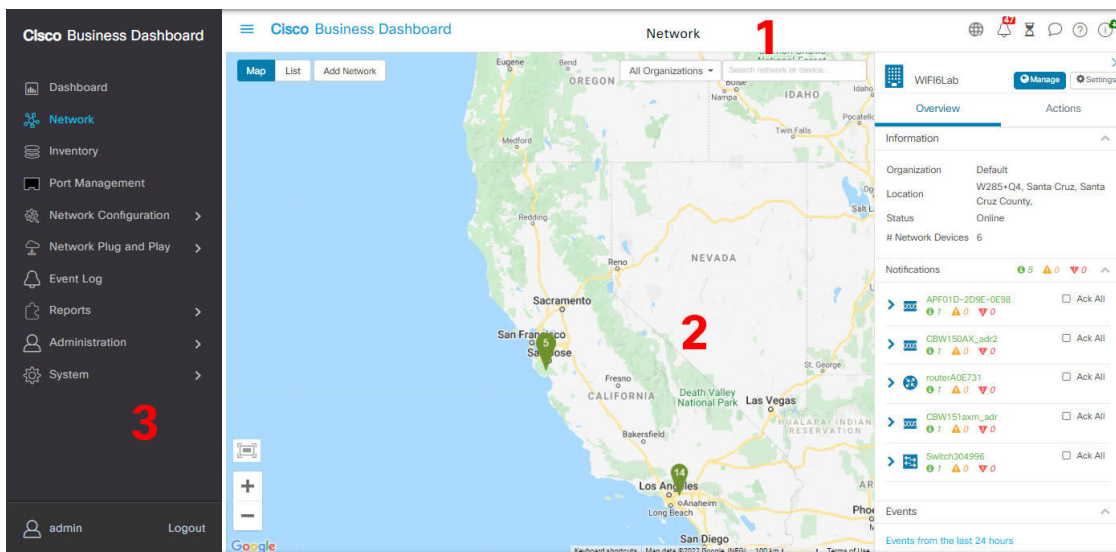





表 2: Cisco Business Dashboard ホームページ









名前	Description
ナビゲーション ペイン	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。
作業ペイン	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。
ヘッダー ツール バー	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。 <ul style="list-style-type: none"> • 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

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。

表 3: ナビゲーションペインのオプション


アイコン	名前	Description
	Dashboard	[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	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が含まれています。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	[Inventory]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。

アイコン	名前	Description
	Port Management	[Port Management]では、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、設定変更を行うことができます。
	Network Configuration	[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。
	Network Plug and Play	[Network Plug and Play]により、ネットワークデバイスのゼロタッチ展開が有効になり、インストール時に自動的にファームウェアと設定ファイルを Cisco Business ダッシュボードからダウンロードすることができます。
	Event Log	[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	[Reports] 見出しの下に、サポート終了案内、保証情報、サービス契約の詳細など、お使いの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いくつかのレポートがあります。
	Administration	[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	[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。
	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 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。

表 4: ヘッダー ツールバーのオプション

アイコン	オプション	Description
	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、ナビゲーションウィンドウが表示されます。

アイコン	オプション	Description
	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ースの言語を選択できます。
	通知センター	このアイコンには、Cisco Business ダッシュボードで未確認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、[Notification] パネルが表示されます。このパネルでは、表示される通知イベントをフィルタリングできます。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 (135 ページ) を参照してください。
	ジョブセンター	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を表示します。ジョブには、ユーザ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。
	フィードバック	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送る場合にクリックします。
	ヘルプ	Cisco Business ダッシュボードのオンラインヘルプドキュメント。
	Cisco Business Dashboard 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。

Cisco Business Dashboard Probe GUI の使用

Cisco Business ダッシュボードプローブにログインすると、[Home] ページが表示されます。

図 2: Cisco Business Dashboard ホームページ

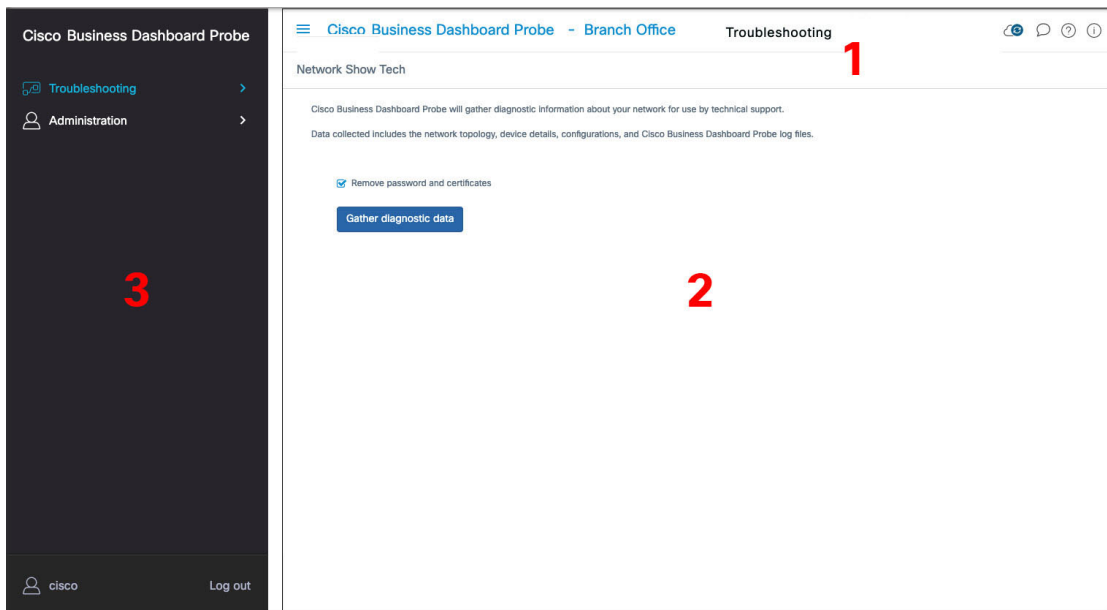





表 5: Cisco Business Dashboard ホームページ

名前	Description
ナビゲーションペイン	<p>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] ボタ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。</p> <p>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。</p>
作業ペイン	<p>機能インターフェイスが表示される領域です。</p> <p>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。</p>
ヘッダーバー	<p>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。</p> <ul style="list-style-type: none"> • 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 • Probe のサイト名を含むヘッダーテキスト • 言語選択ドロップダウン • 通知、フィードバック、状況依存ヘルプなどの機能のための一連のアイコン

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。






表 6: ナビゲーション ペインのオプション


アイコン	名前	Description
	Troubleshooting	ネットワークでの問題を特定するのに役立つ診断ツールが、[Troubleshooting] セクションにあります。
	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。

表 7: ヘッダーバーのオプション

アイコン	オプション	Description
	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、ナビゲーションウィンドウが表示されます。
	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。
	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。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	Cisco Business ダッシュボードプローブ のオンラインヘルプドキュメント。

アイコン	オプション	Description
	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。

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

シスコは随時、Cisco Business Dashboard & Probe 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 [About Cisco Business Dashboard] に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。

Dashboard に更新をダウンロードし適用させるには、次の手順を実行します。

1. [About Cisco Business Dashboard] をクリックして、[About Cisco Business Dashboard] 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、その更新に対応す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 <インストーラのファイル名>` 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 を並行してアップデートすることも、Probe を個別にアップデート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] をクリックして、[About Cisco Business Dashboard] 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、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、エラーメッセージを受け取ります。
3. 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。
4. 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、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。[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。
3. ネットワークの [Basic Info] パネルで [Action] タブを選択します。
4. [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。

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 Dashboard & Probe 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 Dashboard & Probe バージョン 2.3.0 では、Ubuntu バージョン 20.04 (Focal Fossa) のサポートが追加されました。Cisco Business ダッシュボードの将来のバージョンは、Ubuntu 20.04 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 の間的大幅な変更により、Cisco Business Dashboard & Probe 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。さらに、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. まず、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。ダッシュボード GUI にログオンし、[System] > [Backup] に移動します。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ことをお勧めします。

既存のダッシュボードがサーバで実行されている Ubuntu Linux インストール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ことをお勧めします。

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] の順に移動し、指定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、[Upload & Restore] ボタンをクリックして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できます。

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 \(109 ページ\)](#) 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。

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、プローブをホストす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中の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、<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。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、<https://cisco.com/go/cbd-docs> [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

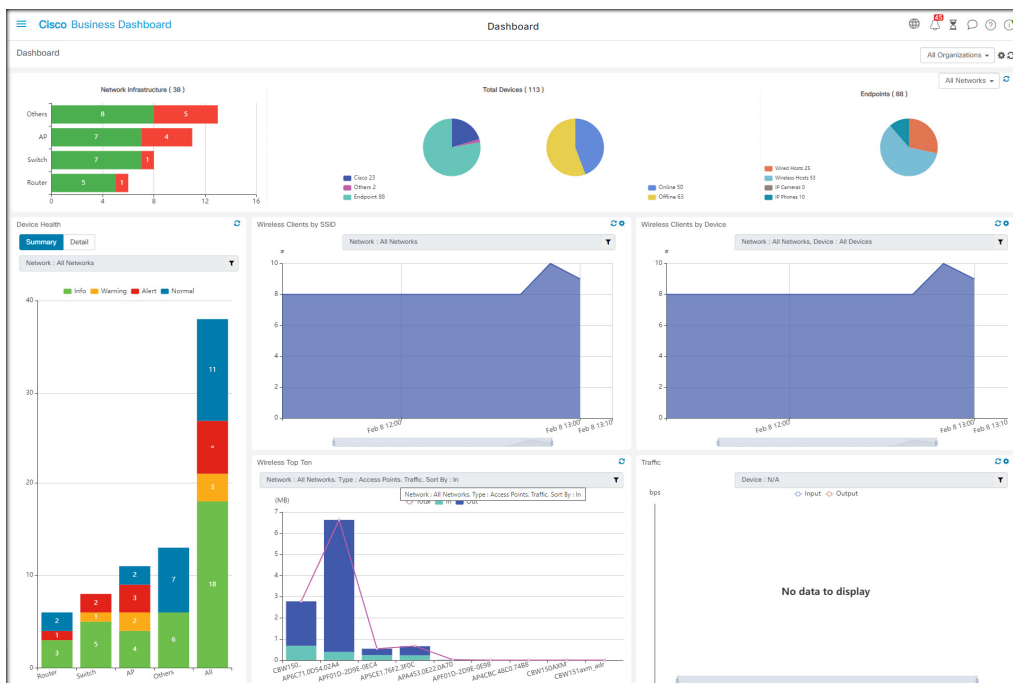
監視ダッシュボード

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 \(19 ページ\)](#)
- [ウィジェットの追加 \(20 ページ\)](#)
- [ウィジェットの変更 \(21 ページ\)](#)
- [ウィジェットの削除 \(22 ページ\)](#)
- [ダッシュボードのレイアウトの変更 \(22 ページ\)](#)

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。
Device Health	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。
デバイスのクライアン ト数	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。
Traffic	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。

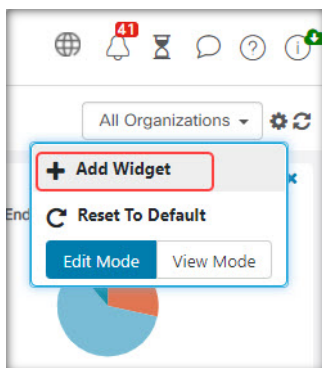
各ウィジェットのコントロールを使用すると、表示されるデータをカスタマイズできます。Dashboard の右上にある組織のドロップダウンを使用すると、特定の組織に表示される情報を制限できます。

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、[ウィジェットの追加] を選択します。

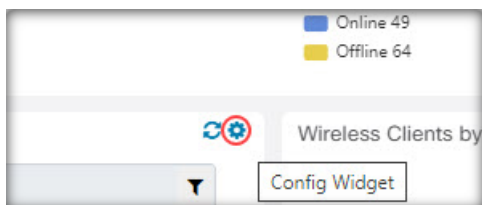


- ステップ2** ポップアップリストから、追加するウィジェットの種類を選択します。新しいウィジェットがダッシュボードに表示されます。
- ステップ3** 新しいウィジェットをダッシュボード内の目的の場所にドラッグし、必要に応じてサイズを変更します。
- ステップ4** 歯車アイコンをもう一度クリックし、[表示モード] を選択して変更内容を保持します。

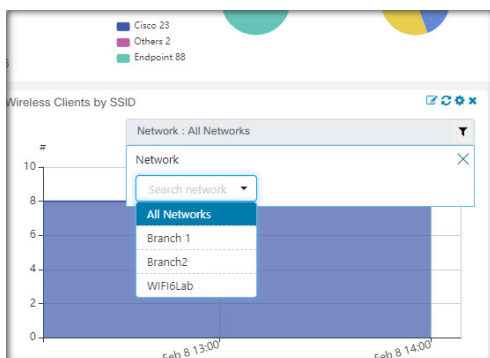
ウィジェットの変更

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 [ウィジェットの構成 (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、[編集モード (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、Dashboard で [編集モード (Edit Mode)] になっている必要があります。

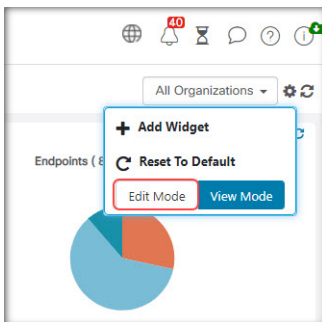
ウィジェットの削除

- 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、[編集モード] 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、[表示モード] を選択して変更内容を保持します。

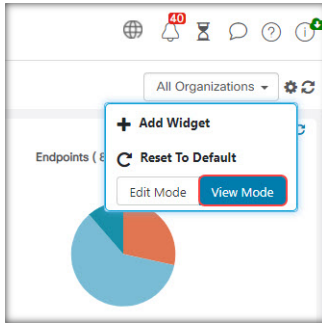
ダッシュボードのレイアウトの変更

[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、[編集モード] を選択します。



- ステップ2** ウィジェットをダッシュボード内で移動するには、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につれて、ダッシュボードのサイズが使用可能な幅に合わせて自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、[表示モード] を選択して変更内容を保持します。





第 4 章

Network

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 (25 ページ)
- ネットワークの詳細について (27 ページ)
- ネットワークビューについて (28 ページ)
- トポロジマップとツールの概要 (28 ページ)
- 基本的なデバイス情報の表示 (32 ページ)
- デバイスアクションの実行 (34 ページ)
- デバイス管理インターフェイスへのアクセス (36 ページ)
- 詳細なデバイス情報の表示 (36 ページ)
- [Floor Plan] の使用方法 (39 ページ)

ネットワークについて

[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。[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。

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、単一のクラスターアイコンに置き換えられます。クラスターアイコンをクリックすると、そのクラスター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。

- [Map/List] の選択：このコントロールを使用して、マップ上またはテーブル内にネットワークを表示するように選択します。
- [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：ドロップダウンから個々の組織を選択して表示す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します。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：マップを拡大および縮小するには、これらのコントロールを使用します。(+) 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：このボタンを使用すると、すべてのネットワークマーカーを表示できるように自動的にマップが縮小されます。

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、**作業**ペイン内でマップを移動することもできます。

[List View] では、次のコントロールを使用できます。

- [Map/List] の選択：このコントロールを使用して、マップ上またはテーブル内にネットワークを表示するように選択します。
- [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。
- [Organization] ドロップダウン：ドロップダウンから個々の組織を選択して表示す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。

- ネットワーク名
- 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、[ネットワークの詳細について \(27 ページ\)](#) 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 Dashboard 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。

ネットワークの詳細について

[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 ログの設定方法の詳細については、[Probe のログ設定の管理 \(146 ページ\)](#) を参照してください。

ネットワークビューについて

ネットワークの [Basic Info] パネルの [Manage] をクリックすると、そのネットワークの [Network View] が表示されます。[Network View] には、ネットワークに関する複数のビューが用意されています。

- [Topology] ビュー：ネットワーク内の検出されたすべてのデバイスの論理的なトポロジが表示されます。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] ビュー：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できます

次に、[Network View] ページで実行するすべてのタスクに共通して提供される追加コントロールを示します。

- [Organization and Network] の選択：これらのドロップダウンを使用すると、メインのネットワークページに戻ることなく、ネットワークと組織を切り替えることができます。別のネットワークのトポロジまたはフロアプランを表示するには、ドロップダウンを使用してそのネットワークを選択します。
- [Network Actions] ドロップダウン：このドロップダウンを使用すると、選択したアクションをサポートしているネットワーク内のすべてのデバイス上で実行できます。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 (<https://www.ciscoactiveadvisor.com>) [英語] へのインベントリのアップロードも実行できます。Cisco Active Advisor の詳細については、<https://help.ciscoactiveadvisor.com> [英語] を参照してください。

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 ダッシュボードクエリは、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。収集されるデータには、Cisco Business スイッチ、ルータ、ワイヤレスアクセスポイントからの CDP & LLDP ネイバー情報、MAC アドレステーブル、関連するデバイステーブルなどがあります。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] パネルを表示できます。[Basic Info] 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、まずナビゲーションから [Network] を選択し、目的のネットワークのアイコンまたはテーブル行をクリックし、[View] をクリックします。そのネットワークの [Topology Map] 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] の左上にあります。








表 8: トポロジコントロール

アイコン	アイコンの名前	Description
	ズームイン	[Topology] ウィンドウの表示を調整します。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。
	ズームアウト	[Topology] ウィンドウの表示を調整します。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。
	トポロジの再レイアウト	手動変更によりトポロジが無効になった後、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。
	選択してズーム	拡大する領域を選択するには、クリックしてドラッグします。
	ステージを合わせる	ネットワーク全体が表示領域を占めるようになるまで拡大します。
	フルスクリーンモードにする	画面いっぱいに 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。
	トポロジのエクスポート	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ンロード場所に保存されます。
	トポロジの設定	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。

表 9: トポロジのアイコン

アイコン	ネットワーク要素	Description
	アクセス ポイント	ワイヤレス アクセス ポイントの表現。
	クラウド	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。
	リンク	リンクは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	ルータを表します。
	スイッチ	スイッチを表します。
	ホスト	有線接続でネットワークに接続したホストを表します。
	ワイヤレス ホスト	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。[Overlays] は [Topology] の右上の検索ボックスの横にあります。

表 10: [Overlays & Filters] パネル

項目	Description
Select Overlay	<p>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。</p> <ul style="list-style-type: none"> • [Link Utilization View] : 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識別します。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。 <p>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。</p> <ul style="list-style-type: none"> • [VLAN View] : 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。 <p>[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。</p> <ul style="list-style-type: none"> • [POE View] : 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] : 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。デバイスは、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選択できます。またはトポロジマップの 2 つのデバイスをシフトクリックしても選択できます。
Select Tag	<p>[Select Tag] ラベルの下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。</p>
Show only: <ul style="list-style-type: none"> • Routers • Switches • Wireless • Hosts • Others 	<p>[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中でオンにします。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。</p>

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、[詳細なデバイス情報の表示 \(36 ページ\)](#) 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 \(36 ページ\)](#) 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、以下の手順を実行します。

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、詳細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 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。

表 11: 基本的なデバイス情報

項目名	Description
[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	<i>Media Access Control (MAC)</i> 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が必要です。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。

項目名	Description
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	
<p>[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。</p> <p>[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 (135 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。</p>	
[Events] パネル	
<p>[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。</p>	
[POE] パネル	
<p>[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。</p>	
[Stack Information] パネル	
<p>[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。</p>	
Service	
<p>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。</p>	
Connected Device	
<p>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。</p>	

[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 \(34 ページ\)](#) 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 [トポロジマップ (Topology Map)] ページまたは [インベントリ (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 [基本情報] パネルで、[アクション] 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。

ファームウェアの最新へのアップグレード	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。
ローカルからのアップグレード	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	<p>現在のデバイス設定のコピーを Dashboard に保存できます。</p> <ol style="list-style-type: none"> [バックアップ設定] をクリックします。 [バックアップ設定] 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。 [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 [キャンセル] をクリックします。 <p>バックアップ設定ジョブが作成されます。このジョブは [タスクセンター] に表示される場合があります。</p>

構成の復元	<p>以前バックアップした設定をデバイスに復元できます。</p> <p>[構成のリストア] をクリックします。</p> <p>次のバックアップ設定オプションが用意されています。</p> <ul style="list-style-type: none"> • [バックアップデバイス名]: 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 • [他のバックアップ]: 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 • [他の互換性のあるデバイスのバックアップ]: 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 <p>バックアップ設定を行うには、以下の手順を実行します。</p> <ol style="list-style-type: none"> 1. [復元設定] 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。 <p>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、[構成のリストア] ボタンが有効になります。</p> <p>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。</p> <ol style="list-style-type: none"> 2. [構成のリストア] をクリックしてこのアクションを完了します。 <p>復元設定ジョブが作成されます。このジョブは [タスクセンター] に表示される場合があります。</p>
再起動	<p>デバイスを再起動します。</p> <p>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。</p>
実行設定を保存	<p>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、デバイスを次回リブートしたときに、設定変更が保持されます。</p>
削除	<p>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。</p>

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、[ジョブ管理 \(139 ページ\)](#) 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] : デバイスで設定されているワイヤレス LAN を表示できます

(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。

表 12: 詳細なデバイス情報

項目名	Description
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	<i>Media Access Control (MAC)</i> 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が必要です。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。

項目名	Description
Description	デバイスまたは製品の説明。
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とワイヤレス 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](#)」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 13: 設定のバックアップ

項目	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。 <ul style="list-style-type: none"> • [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

この章は、次の項で構成されています。

- [デバイス インベントリの表示 \(43 ページ\)](#)

デバイス インベントリの表示

[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 14: 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。
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が必要です。これらのアドレスはデバイスごとに固有成りであり、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。

項目	説明
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。
 - **Download Latest Firmware**
 - **Apply Firmware Upgrade From Local**
 - **Backup Configuration**
 - **Restore Configuration**
 - **Reboot Device**
 - **Save Running Configuration**
 - **Delete**

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

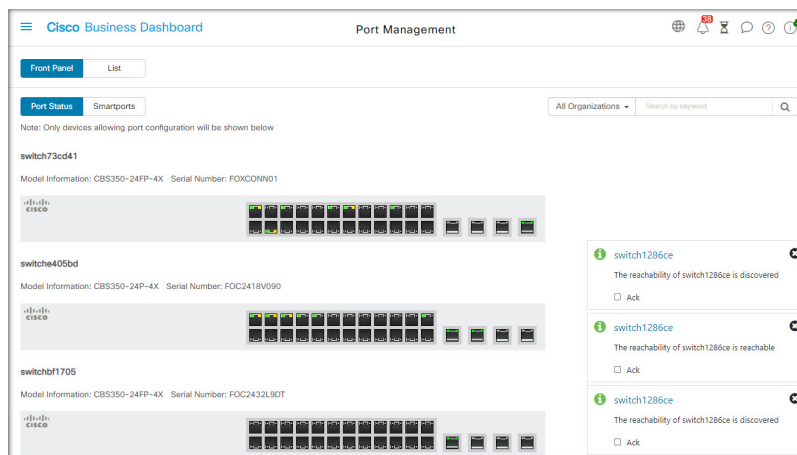
- [ポート管理について \(47 ページ\)](#)

ポート管理について

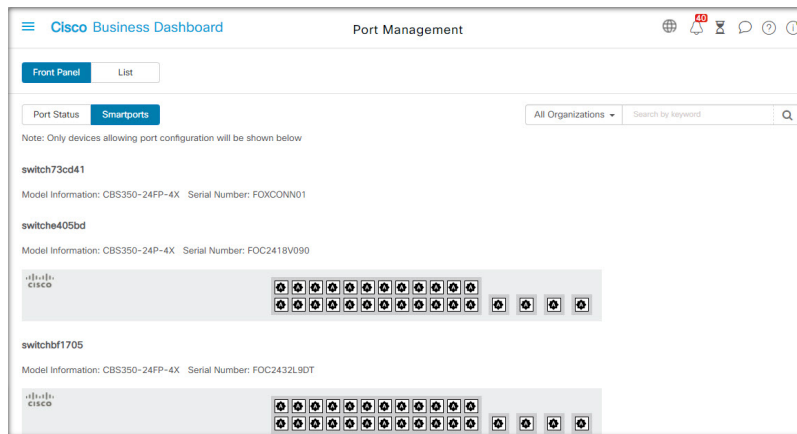
[ポート管理 (Port Management)] は、Cisco Business ダッシュボードによって設定可能なスイッチポートを含む各デバイスの前面パネルビューとして利用できます。このページでは、トラフィックカウンタなどのポートのステータスを参照したり、ポートの設定を変更することができます。また、このページでは、Smartport をサポートするデバイス上のポートについて、Smartport ロールを表示および設定することもできます。検索ボックスを使用して表示するデバイスを制限できます。デバイス名、製品 ID、シリアル番号の全部または一部を入力して、目的のデバイスを探します。

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。

[物理 (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 と共に表示されます。

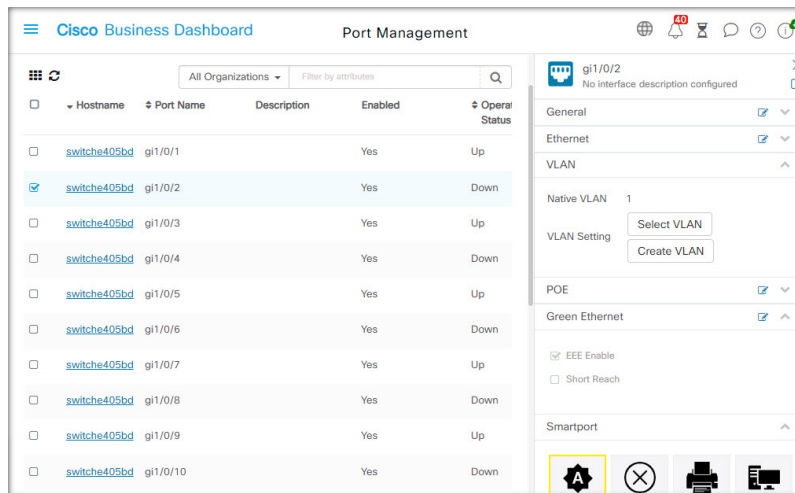


[スマートポート (Smartport)] ビューでは、各ポートの現在の Smartport ロールを表示したり、ロールを変更したりできます。各ポートには、現在のロールを示すアイコンがオーバーレイ表示されます。



(注) [スマートポート (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[基本情報]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。



全般	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ており、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。
イーサネット	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
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。[VLAN の選択] または [VLAN の作成] 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。[電源入れ直し (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。
グリーンイーサネット	このパネルでは、ポートの Energy Efficient Ethernet (EEE) 設定を管理できます。
Smartport	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 [編集] アイコンをクリックします。変更を加えたら、[保存] アイコンをクリックします。



第 7 章

Network Configuration

この章は、次の項で構成されています。

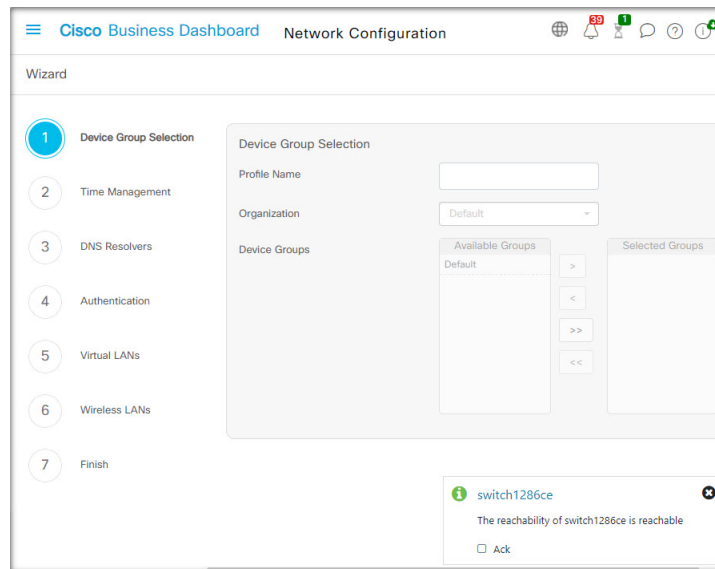
- ネットワーク設定について (51 ページ)
- ウィザードの使用方法 (51 ページ)
- 時刻管理の設定 (52 ページ)
- DNS リゾルバの設定 (53 ページ)
- 認証の設定 (54 ページ)
- 仮想 LAN の設定 (55 ページ)
- ワイヤレス LAN の設定 (57 ページ)

ネットワーク設定について

[ネットワーク設定] 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

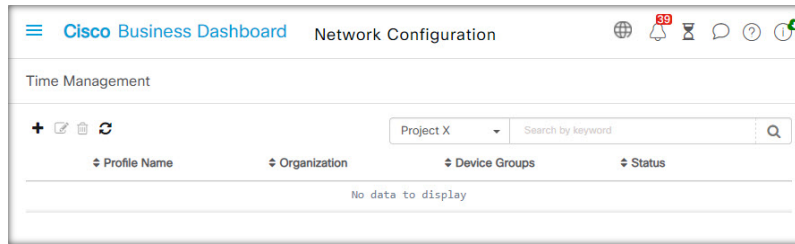
ウィザードを使用すると、ネットワーク設定の要素ごとに設定プロファイルを作成し、それらのプロファイルをもとに1つ以上のデバイス グループに1つのワークフローで割り当てることができます。



1. [ネットワーク設定 (Network Configuration)] > [ウィザード (Wizard)] の順に移動します。
2. [デバイスグループの選択] 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. [次へ (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、[次へ] 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、[スキップ] をクリックします。
5. 前の画面に戻る場合は、[戻る] 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。[終了] 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

[時刻管理] ページでは、ネットワークのタイムゾーン、夏時間、NTP サーバーを設定できます。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. [ネットワーク設定 (Network Configuration)] > [時刻管理 (Time Management)] の順に移動します。
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. [デバイスグループの選択] 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. [時刻設定] 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 [夏時間] 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 [NTP の使用] 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 サーバーアドレスを指定します。
7. [保存 (Save)] をクリックします。

時刻管理設定プロファイルを変更

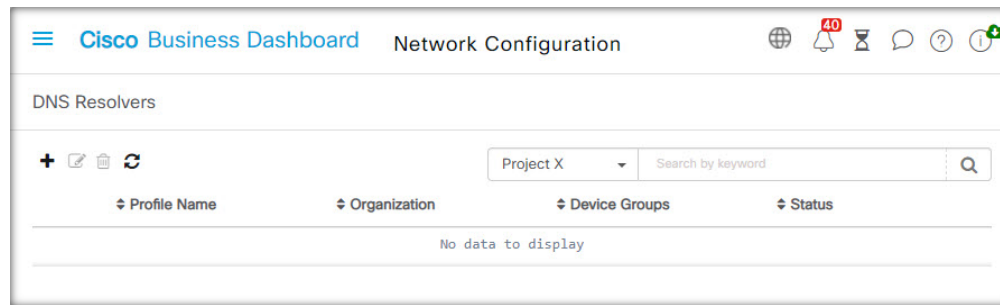
1. 変更するプロファイルの横にあるオプションボタンを選択し、[編集] アイコンをクリックします。
2. プロファイル設定に必要な変更を加え、[更新] をクリックします。

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. [削除] アイコンをクリックします。

DNS リゾルバの設定

[DNS リゾルバ] 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ーを設定できます。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. [ネットワーク設定 (Network Configuration)] > [DNS リゾルバ (DNS Resolvers)] の順に移動します。
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. [デバイスグループの選択] 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 サーバー アドレスを指定します。
6. [保存 (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

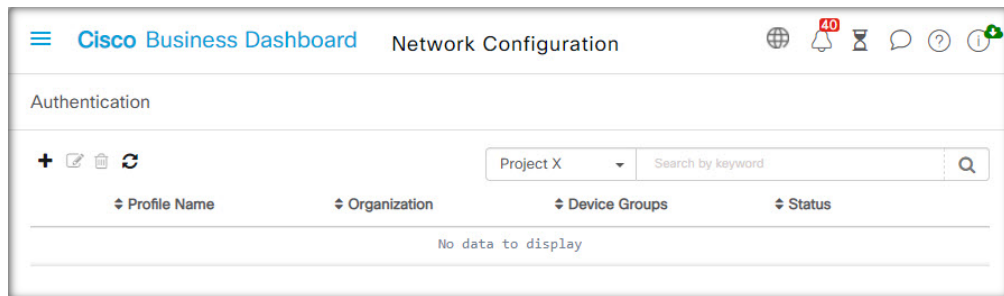
1. 変更するプロファイルの横にあるオプションボタンを選択し、[編集] アイコンをクリックします。
2. プロファイル設定に必要な変更を加え、[更新] をクリックします。

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. [削除] アイコンをクリックします。

認証の設定

[認証] 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. [ネットワーク設定 (Network Configuration)]> [認証 (Network Configuration)] の順に移動します。
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. [デバイスグループの選択] 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. 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ーを追加できます。
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. [保存 (Save)] をクリックします。

認証設定プロファイルを変更

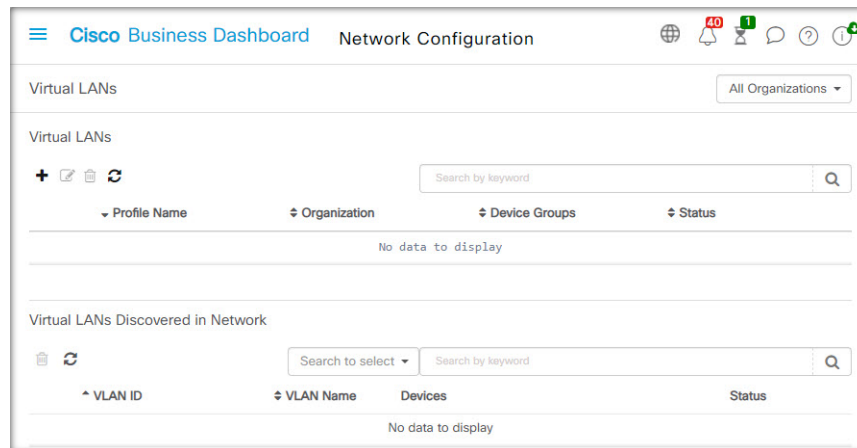
1. 変更するプロファイルの横にあるオプションボタンを選択し、[編集] アイコンをクリックします。
2. プロファイル設定に必要な変更を加え、[更新] をクリックします。

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. [削除] アイコンをクリックします。

仮想 LAN の設定

[仮想 LAN (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. [ネットワーク設定 (Network Configuration)] > [仮想 LAN (Virtual LANs)] の順に移動します。
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. [デバイスグループの選択] 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、[別の VLAN を追加] をクリックし、手順 4 に戻ります。
6. [保存 (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、[編集] 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、[更新] 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、[削除] 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

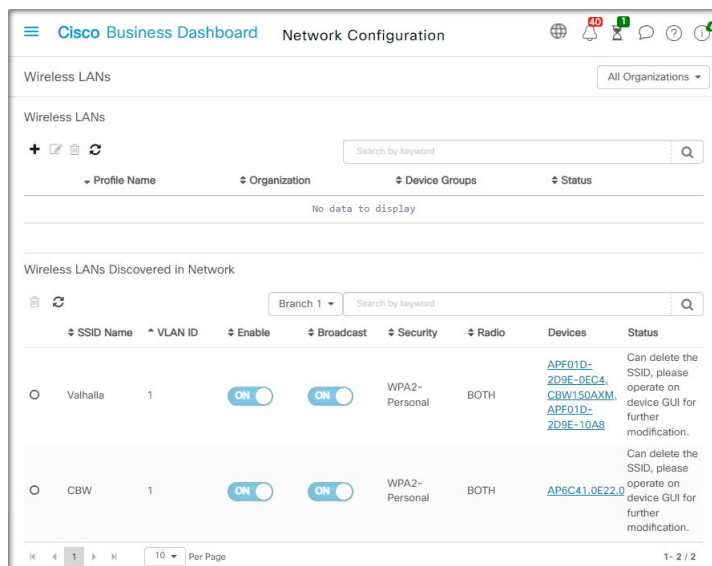
検出された VLAN の表で、削除する 1 つ以上の VLAN の横の [削除] アイコンをクリックします。



(注) VLAN 1 は削除できません。

ワイヤレス LAN の設定

[ワイヤレス LAN] 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。



無線 LAN を作成

1. [ネットワーク設定 (Network Configuration)] > [ワイヤレス LAN (Wireless LANs)] の順に移動します。
2. + (プラス) アイコンをクリックして新しいワイヤレス LAN を追加します。
3. [デバイスグループの選択] 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. 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。

5. 要件に合わせて、[有効化]、[ブロードキャスト]、[セキュリティ]、および[無線]設定を変更することもできます。
6. 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、[別の LAN を追加] をクリックし、手順 3 に戻ります。
7. 選択したセキュリティ モード ([Enterprise] または [Personal]) に応じて、認証に使用する RADIUS サーバーか、あらかじめ共有されたキーを指定します。
8. [保存 (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、[編集] 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、[更新] 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、[削除] 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 [仮想 LAN] 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無線 LAN 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、[削除] 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必要があります。



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 \(59 ページ\)](#)
- [ネットワーク要件 \(59 ページ\)](#)
- [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 \(62 ページ\)](#)
- [ネットワーク プラグアンドプレイ サービスの設定 \(63 ページ\)](#)
- [ネットワーク プラグアンドプレイのモニタリング \(70 ページ\)](#)

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。

- **手動設定**：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のアドレスを手動で設定できます。

- **DHCP** : ベンダー固有の情報オプションで、サーバのアドレスがデバイスに提供される場合があります。
- **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。
- **プラグ アンド プレイ 接続サービス** : 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 接続サービスに接続しようとします。このサービスにより、デバイスはサーバ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。

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
- **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。
- **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
- **TtrustpoolBundleURL** : 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。

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。

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 \(104 ページ\)](#) 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。次に、[Next] をクリックします。
4. 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。
5. 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。
6. 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。3 つのグラフが表示され、デバイスグループ別、PnP 対応デバイス別、および 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（要求元不明デバイス）別に分類されたデバイスのステータスが示されます。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 15: 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	
事前に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
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	ユーザによって明示的に無視された要求元不明デバイス

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。同様に、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。

新しい対応デバイスを作成するには、次の手順を実行します。

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。

既存のデバイスを編集するには、次の手順を実行します。

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します。
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。

対応デバイスを削除するには、次の手順を実行します。

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するには、および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、以下を行います。

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。

デバイスをプロビジョニングせずに [Unclaimed] リストから削除するには、以下を行います。

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。無視したデバイスを再要求するには、以下を行います。

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、サーバで未要求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、以下を行います。

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導入できます。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、以下を行います。

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 イメージとして指定するには、以下を行います。

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、以下を行います。

1. [Network Plug and Play] > [Images] に移動します。

- 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。設定テンプレートの詳細については、「付録A」の「[設定テンプレートの管理](#)」を参照してください。

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変更またはコピーして使用することも可能です。

新しい設定を手動で作成するには、次の手順を実行します。

- [**Network Plug and Play**] > [**Configurations**] に移動します。
- + (プラス) アイコンをクリックします。
- 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 のカンマ区切り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。

- 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。テンプレートの構文とメタデータの詳細については、「[設定テンプレートの管理](#)」を参照してください。

[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。

- 設定に問題なければ、[Save] をクリックします。

設定ファイルをアップロードするには、以下を行います。

- [**Network Plug and Play**] > [**Configurations**] に移動します。
- [Upload] アイコンをクリックします。
- 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。

設定を削除するには、以下を行います。

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、以下を行います。

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（104 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 サービスに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 16: 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。
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 \(73 ページ\)](#)

イベント ログについて

イベントログではネットワークで生成されたイベントを検索およびソートするためのインターフェイスが提供されます。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]** : 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]** : 表示するイベントの重大度を選択します。[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]** : 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]** : イベントを表示するネットワークを1つ以上選択します。入力すると、一致したサイトが表示されます。
- **[Device]** : イベントを表示するデバイスを1つ以上選択します。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 アドレスごとにデバイスを指定することができます。

フィルタ条件に一致するイベントが次の表に表示されます。この表は列のヘッダーをクリックするとソートされます。



第 10 章

Reports

この章は、次の項で構成されています。

- レポートの概要 (75 ページ)
- ライフサイクルレポートの表示 (75 ページ)
- サポート終了レポートの表示 (77 ページ)
- メンテナンス レポートの表示 (78 ページ)
- ワイヤレス ネットワーク レポートの表示 (79 ページ)
- ワイヤレス クライアント レポートの表示 (82 ページ)

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 Report] : 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 Report] : 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表示します。
- [Maintenance Report] : 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。次の表に提供される情報を示します。

表 17: ライフサイクルレポート

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。
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せん。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。

表 18: サポート終了レポート

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。
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せん。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。次の表に提供される情報を示します。

表 19: メンテナンス レポート

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せん。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。

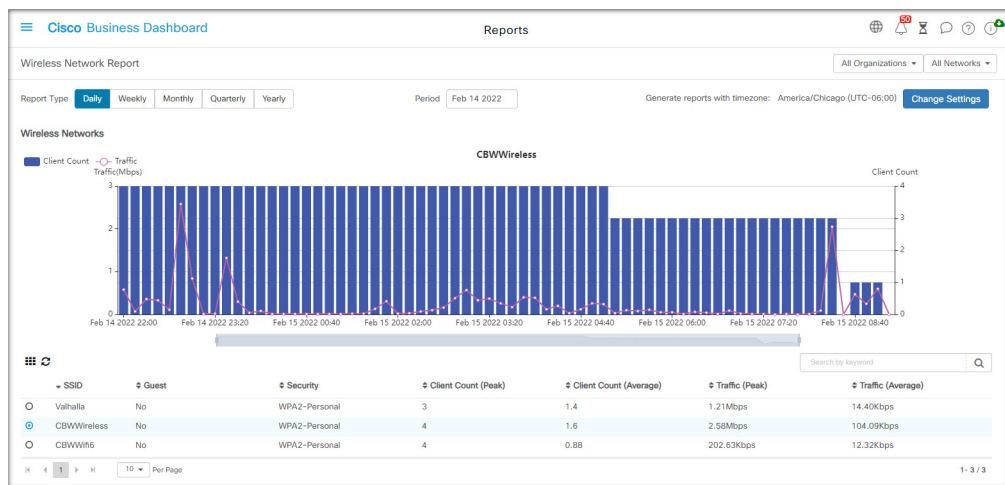
レポートの左上にある [column selection] アイコンを使用すると、表示される情報をカスタマイズできます。アイコンをクリックして、表示されるチェックボックスを使用すると、レポートに含める列を選択できます。

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。

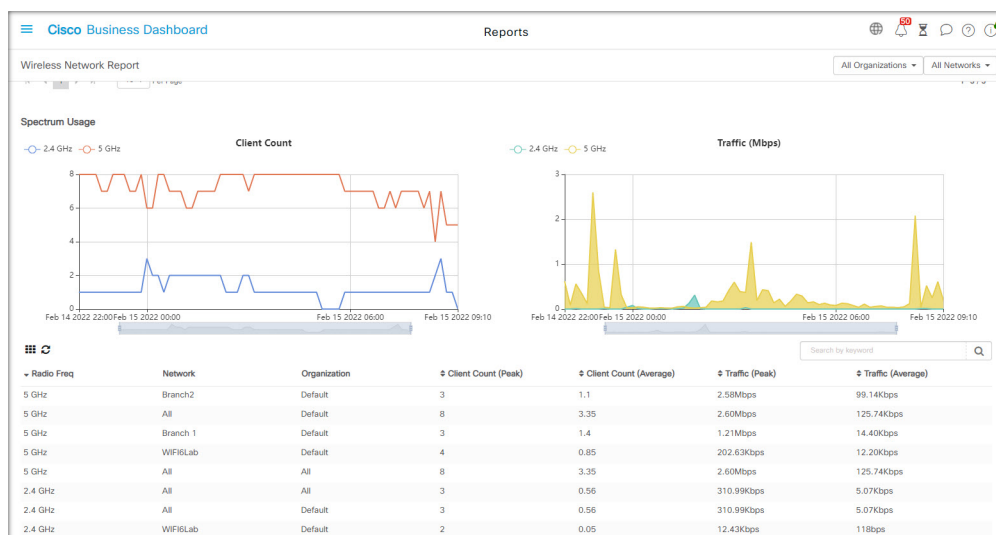
いくつかのデータセットには、選択した行の時間の経過に伴う内訳を示すグラフが含まれています。グラフ上の凡例のラベルをクリックするとデータの各セットの表示を切り替えられます。

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。

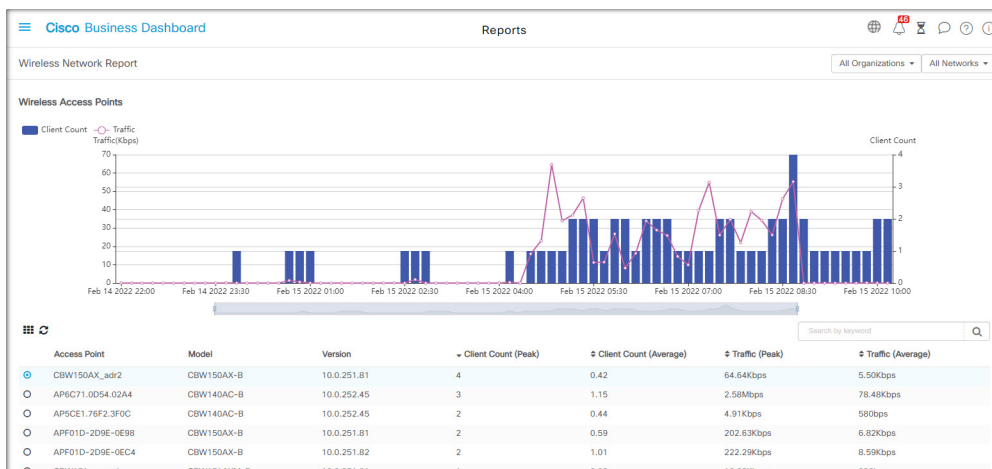


ワイヤレス ネットワーク テーブル	
SSID	ワイヤレス ネットワーク名。
ネットワーク (デフォルトでは非表示)	SSID があるネットワーク。
組織 (デフォルトでは非表示)	SSID が属する組織。
ゲスト	SSID がゲスト アクセス用に設定されているかどうか。
セキュリティ	SSID 用に設定されたセキュリティ方式。
クライアント カウント (ピーク)	レポートの対象期間に SSID に関連付けられたクライアントの最大数。
クライアント カウント (平均)	レポートの対象期間に SSID に関連付けられたクライアントの平均数。

ワイヤレス ネットワーク テーブル	
トラフィック (ピーク)	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。
トラフィック (平均)	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。



スペクトル使用テーブル	
無線周波数	使用中の無線周波数帯 (2.4 GHz または 5 GHz)。
ネットワーク	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。
組織	スペクトル使用状況データが適用される組織。
クライアント カウント (ピーク)	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。
クライアント カウント (平均)	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。
トラフィック (ピーク)	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。
トラフィック (平均)	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

アクセス ポイント	アクセス ポイントの名前。
ネットワーク (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。
組織 (デフォルトでは非表示)	アクセス ポイントが属する組織。
モデル	アクセス ポイントのモデル。
バージョン	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。
クライアント カウント (ピーク)	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。
クライアント カウント (平均)	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。
トラフィック (ピーク)	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。
トラフィック (平均)	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。

SSID	MAC	First Seen	Last Seen	Total Time Visible	Channel	Average Signal Strength	Seen By
olsonhome	5C:E2:8C:DE:08:21	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-51dBm	AP4CBC.48C0.74B8
Hiltron502AD-EasyConnect	84:0B:7C:D5:52:A8	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-80dBm	AP4CBC.48C0.74B8
lanlam	60:B7:6E:F9:5F:56	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-64dBm	AP4CBC.48C0.74B8
null	0E:62:A6:80:42:C9	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-60dBm	AP4CBC.48C0.74B8
Dirty	60:6C:63:BA:42:C8	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-79dBm	AP4CBC.48C0.74B8
CBWWiFi6	F0:1D:2D:9E:61:AF	Feb 15 2022 09:05	Feb 15 2022 09:05		64(5GHz)	-63dBm	AP4CBC.48C0.74B8
Dixie	90:AA:C3:30:24:C8	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-78dBm	AP4CBC.48C0.74B8
Popeyes Guest	92:6C:AC:91:78:94	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-83dBm	AP4CBC.48C0.74B8
DG860AD2	BC:CA:85:FB:62:E0	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-66dBm	AP4CBC.48C0.74B8
EON-Private	90:6C:AC:91:78:94	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-83dBm	AP4CBC.48C0.74B8

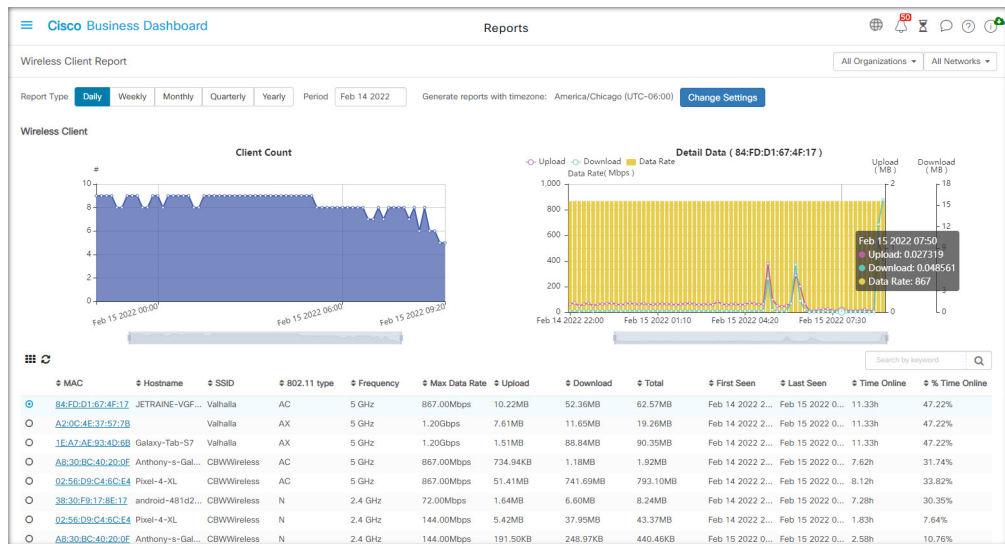
不正なアクセス ポイント テーブル	
SSID	検出された SSID。
ネットワーク (デフォルトでは非表示)	検出アクセス ポイントがあるネットワーク。
組織 (デフォルトでは非表示)	検出アクセス ポイントが属する組織。
MAC	不正なアクセス ポイントの MAC アドレスの検索。
最初の確認日時	不正なアクセス ポイントが最初に検出された時刻。
最新の確認日時	不正なアクセス ポイントが最後に表示された時刻。
可視合計時間	不正なアクセス ポイントがオフラインだった合計時間。
チャンネル	不正なアクセス ポイントが使用したワイヤレス チャンネル。
平均信号強度	アクセスポイントの検出により検出された不正なアクセス ポイントの平均信号強度。
検出元	不正なアクセス 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
ホスト名	クライアントのホスト名（使用可能な場合）。
組織	クライアントで最後に表示された組織。
ネットワーク	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 タイプ	クライアントで使用される 802.11 バリエーション。
頻度	クライアントで使用される周波数帯域。
最大データ レート	クライアントで使用された最大データ レート。
アップロード	クライアントでアップロードされたデータの量。
ダウンロード	クライアントでダウンロードされたデータの量。
合計	クライアントで送受信されたデータの総量。
最初の確認日時	クライアントで最初に検出された時刻。
最新の確認日時	クライアントで最後に表示された時刻。
時間オンライン	クライアントがオンラインだった合計時間。
% オンライン時間	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 20: 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。
ホスト名	クライアントのホスト名（使用可能な場合）。
ユーザー名	ゲスト ポータルにクライアントが入力したユーザー名。
組織	クライアントで最後に表示された組織。
ネットワーク	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 タイプ	クライアントで使用される 802.11 バリエーション。
頻度	クライアントで使用される周波数帯域。
最大データ レート	クライアントで使用された最大データ レート。
アップロード	クライアントでアップロードされたデータの量。
ダウンロード	クライアントでダウンロードされたデータの量。
合計	クライアントで送受信されたデータの総量。
最初の確認日時	クライアントで最初に検出された時刻。
最新の確認日時	クライアントで最後に表示された時刻。
時間オンライン	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	
% オンライン時間	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) [最初に表示 (First Seen)]タイムスタンプと [最後に表示 (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

Administration

この章は、次の項で構成されています。

- [管理について](#) (87 ページ)
- [組織の管理](#) (88 ページ)
- [デバイス グループ \(Device Groups\)](#) (90 ページ)
- [デバイスのクレデンシャル](#) (92 ページ)
- [ユーザの管理](#) (93 ページ)
- [モニタリングのデフォルト値の変更](#) (96 ページ)
- [モニタリングプロファイルの管理](#) (97 ページ)
- [ログイン試行の表示](#) (99 ページ)
- [レポート設定の管理](#) (100 ページ)

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。

組織の管理

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。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、デフォルトで組織が1つ作成されます。

新規組織の作成

新しい組織を作成するには、次の手順を実行します。

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。変更期間の詳細については、[ジョブ管理 \(139 ページ\)](#) を参照してください。
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。

既存の組織の変更

既存の組織を変更するには、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

組織を削除するには、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の管理

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の管理 \(97 ページ\)](#) 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の管理](#)」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の変更 \(96 ページ\)](#) を参照してください。

組織に関連付けられているユーザの管理

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。

ユーザを組織に関連付けるには、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、**[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を選択します。



⚠ 管理者レベルのユーザは、すべての組織に暗黙的に関連付けられており、ドロップダウンリストには表示されません。

組織からユーザを削除するには、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、**[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の管理

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、次の手順を実行します。

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 (Device Groups)

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。

デバイスグループを作成

Group Name	Default Group	Description	Organization	# Network Devices
Default	Yes	Default group for default organization	Default	24
ProjectX	Yes	Default group for organization Proje...	Project X	0

1. [管理]>[デバイス グループ]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。[保存 (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。

デバイスグループを変更

1. [管理]>[デバイス グループ]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、[編集]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。[保存 (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 [デフォルト] グループに移動されます。



⚠ [デフォルト] グループからデバイスを削除することはできません。[デフォルト] 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. [管理]>[デバイス グループ]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、[削除]アイコンをクリックします。



注 [デフォルト] 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ためには、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、プローブがデフォルトのユーザー名 (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、ユーザー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. **[管理] > [デバイス クレデンシャル]** 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. [ユーザー名]/[パスワード] フィールド、[SNMP コミュニティ] 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. **[適用 (Apply)]** をクリックします。プローブ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、ステップ 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 **[編集]** 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. ユーザー名とパスワードか、SNMP クレデンシャルをフィールドに入力します。
3. **[適用 (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 [パスワードの表示] 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、[パスワードを非表示] ボタンをクリックします。また、テ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。保存されているログイン情報を削除するには、以下の手順に従います。

1. [管理] > [デバイス クレデンシャル] 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 [削除] ボタンをクリックします。

ユーザの管理

[User Management] ページでは、ユーザが Cisco Business ダッシュボードにアクセスする方法を制御したり、それらのユーザと Dashboard が通信する方法に影響する設定を変更したりすることもできます。

Cisco Business ダッシュボードは、次の 4 つのタイプのユーザをサポートしています。

- **管理者**：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。
- **組織管理者**：組織管理者は 1 つ以上の組織の管理に限定されており、システムに変更を加えることはできません。
- **オペレータ**：オペレータは組織管理者と同様の権限を持ちますが、ユーザを管理することはできません。
- **読み取り専用**：読み取り専用ユーザは、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。

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。

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。

ローカルユーザデータベースへの新しいユーザの追加

新しいユーザを追加するには、以下の手順を実行します。

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、ユーザタイプを指定します。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。

ユーザの変更

既存のユーザを変更するには、以下のようになります。

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。

ユーザの削除

既存のユーザを削除するには、以下のようになります。

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の変更

パスワードの複雑さ要件を有効にするか変更するには、以下のようになります。

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 認証の有効化

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。

認証ソースとして Azure Active Directory を有効にするには、次の手順を実行します。

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。
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。

ローカル認証の管理

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、次の手順を実行します。

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、次の手順を実行します。

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の復元

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、次の手順を実行して回復します。

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の変更

ユーザ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、次の操作を実行します。

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の変更

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**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] > [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の管理**」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、**組織の管理 (88 ページ)** を参照してください。

モニタリングプロファイルの管理

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。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、次のチャン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 (107 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 (117 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 (117 ページ)** を参照してください。

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、システムレベルまたは組織単位で、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、**組織の管理 (88 ページ)** と **モニタリングのデフォルト値の変更 (96 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の追加

新しいモニタリングプロファイルを追加するには、次の手順を実行します。

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、プロファイルに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、個々のモニタを有効または無効にすることができます。
7. 通知モニタには、**[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のコピー

既存のモニタリングプロファイルをコピーするには、次の手順を実行します。

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の変更

既存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]** > **[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の削除

既存のモニタリングプロファイルを削除するには、次の手順を実行します。

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。

表 21: ログイン試行テーブル

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。有効な値には、ログインとログアウトが含まれます。
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] ページでは、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刻と終了時刻は、選択したタイムゾーンのローカル時刻になります。



第 12 章

System

この章は、次の項で構成されています。

- システムについて (101 ページ)
- ライセンスの管理 (102 ページ)
- 証明書の管理 (104 ページ)
- 電子メール設定の管理 (107 ページ)
- API 使用状況の表示 (108 ページ)
- Dashboard 設定のバックアップと復元 (109 ページ)
- プラットフォーム設定の管理 (110 ページ)
- プライバシーの管理 (112 ページ)
- ログ設定の管理 (115 ページ)
- ローカル Probe の管理 (117 ページ)
- 統合設定の管理 (117 ページ)

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。

このオプションは、次のページに分かれています。

- [License] : Dashboard のソフトウェアライセンスを管理します。
- [Certificate] : Dashboard のセキュリティ証明書を管理します。
- [Email Settings] : 電子メールをセットアップします。
- [API Usage] : Cisco Business ダッシュボード API の使用状況を監視します。
- [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] : Dashboard 用の設定とその他データを復元します。
- [Platform Settings] : Dashboard のネットワーク設定を管理します。
- [Privacy Settings] : シスコと共有できるデータを制御します。

- [Log Settings] : Dashboard のログ設定を変更します。
- [Local Probe] : Dashboard にホストされた Probe を管理します。
- [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。

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。このページには、次の 2 つの情報パネルがあります。

- [Smart Software Licensing Status] : 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、および使用中のスマート アカウントに関する情報が表示されます。
- [Smart License Usage] : 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量とタイプ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を示されます。

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、次の手順を実行します。

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。[General] タブをクリックします。

3. [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。[Create Token] をクリックします。
4. 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。
5. Cisco Business ダッシュボード ユーザーインターフェイスに移動し、[System] > [License] を選択します。
6. [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。[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、ユーザー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の Dashboard の削除

スマートアカウントから Dashboard を削除するには、割り当てられたライセンスをプールに戻し、次の手順を実行します。

1. Cisco Business ダッシュボード ユーザー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を確認し、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 のライセンス割り当てをただちに更新するには、次の手順を実行します。

1. Cisco Business ダッシュボード ユーザー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、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、以下を行います。

1. Cisco Business ダッシュボード ユーザー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、以下を行います。

1. Cisco Business ダッシュボード ユーザー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、次の手順を実行します。

1. Cisco Business ダッシュボード ユーザー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

CSR を生成するには、以下を行います。

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。

新しい証明書のアップロード

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、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. [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、承認された担当者だけ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。

自己署名証明書の再生成

自己署名証明書を再生成するには、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. **[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。

現在の証明書の表示

現在の証明書を表示するには、以下を行います。

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、以下を行います。

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> [英語]) 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ました。これを行うには、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 サーバにインターネットからアクセスする必要があります。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 \(110 ページ\)](#) を参照してください。

電子メール設定の管理

[電子メール設定] 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サーバー	使用する SMTP サーバーのドメイン名または IP アドレス。
SMTPポート	メールを送信するために使用される TCP ポート。
E メール暗号化	使用する暗号化方式には、次のものが含まれます。 <ul style="list-style-type: none"> なし TLS SSL
認証	電子メール認証を有効または無効にします。
ユーザー名	認証が有効な場合に提示するユーザー名。
パスワード	認証が有効な場合に提示するパスワード。
送信元の電子メールアドレス	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、[接続のテスト] 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せん。

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。

表 22: API クライアント情報テーブル

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。

フィールド	説明
# 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。

表 23: [Subscribed Networks] テーブル

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、次の手順に従います。

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することもできます。

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。

Dashboard に設定バックアップを復元するには、次の手順を実行します。

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。

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、**[Network Settings]**、**[Web Server]**、**[System Variables]** の3つのグループに分類されており、このページにはグループごとに個別のタブが用意されています。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)



(注) この手順は Cisco Business ダッシュボード for AWS には適用されません。

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す。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、次の手順を実行します。

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) この手順は Cisco Business ダッシュボード for AWS には適用されません。ネットワーク設定を変更するには、AWS の EC2 コンソールを使用します。

Dashboard のネットワーク設定を変更するには、次の手順を実行します。

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、以下を行います。

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。

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 サーバポートを変更するには、以下を行います。

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. [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。

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、次の手順を実行します。

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、次の手順を実行します。

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

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、次の手順を実行します。

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。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。
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、次の手順を実行します。

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、次の手順を実行します。

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確認するには、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、次の手順を実行します。

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。

ホストの syslog サービスへのファイル送信を有効にするには、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、`/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、ローガー設定の **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 ~ 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 の Cisco Business ダッシュボードには表示されません。

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 ダッシュボード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、アカウントिंग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
- デバイスを再起動します
- 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。

- 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 24: 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 25 : [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 <code>https://na.connectwise.net</code> 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. 組織と会社名の間に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

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 \(124ページ\)](#) の表 30-32 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进行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 26: *Connectwise Manage Configuration* フィールドの使用方法

フィールド	Description
設定名	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。 <ul style="list-style-type: none"> • 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	
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 27: 自動化チケットのタイプ \(126 ページ\)](#) 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 28: 自動化チケットのサブタイプ \(126 ページ\)](#) 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 29: 自動化チケットのステータス \(127 ページ\)](#) 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 27: 自動化チケットのタイプ

タイプ	Description
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 28: 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。

サブタイプ	説明
Run Now	アクションはすぐに実行する必要があります。

表 29: 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ตอบสนอง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の管理 \(97 ページ\)](#) を参照してください。

[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 28: 自動化チケットのサブタイプ \(126 ページ\)](#) 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。



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。

- [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。



- 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。

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。

- [System] > [Integration Settings] の順に選択します。
- 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。
- [Settings] アイコンをクリックして、[Webex Settings] ページを表示します。
- 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。
- 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の管理 \(97 ページ\)](#) 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回答して 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の管理 \(97 ページ\)](#) を参照してください。

[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 30: 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。

コマンド	説明
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。
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 \(133 ページ\)](#)
- [サポートされる通知 \(133 ページ\)](#)
- [現在のデバイスの通知の表示とフィルタリング \(135 ページ\)](#)
- [デバイスの履歴通知の表示とフィルタリング \(137 ページ\)](#)

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、これらの通知は通知センターに表示されません。

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。

The screenshot shows the Cisco Business Dashboard Notification Center interface. At the top, there are navigation icons and a search bar. Below the search bar, there are filters for 'All Organizations', 'Notification Type: All Types', 'Severity: Info', 'Higher', and 'Include Acknowledged Notifications:'. A summary bar shows 40 info notifications, 2 warning notifications, and 3 error notifications. The main table lists notifications with columns for Organization, Network, Hostname, MAC Address, Notification, Timestamp, and Ack. The notifications include warnings about CPU health level, device online/offline status, and device reachability for various networks like Branch 1, WiFiLab, and Branch 2.

Organization	Network	Hostname	MAC Address	Notification	Timestamp	Ack
Default	Branch 1	APF01D-2D9E-0EC4	F0:1D:2D:9E:0E:C4	Warning CPU health level	Feb 17 2022 07:12:48	<input type="checkbox"/>
Default	WiFi6Lab	CBW151axm_adr	F0:1D:2D:9E:0B:6C	Device online	Feb 17 2022 07:09:15	<input type="checkbox"/>
Default	Branch 1	ATA191	00:BF:77:18:EF:F6	Device reachable	Feb 16 2022 07:36:03	<input type="checkbox"/>
Default	Branch2	AP4CBC.48C0.74B8	4C:8C:48:C0:74:B8	Rogue Access Points detected	Feb 15 2022 09:05:15	<input type="checkbox"/>
Default	Branch2	APA453.0E22.0A70	A4:53:0E:22:0A:70	Device reachable	Feb 15 2022 09:01:23	<input type="checkbox"/>
Default	Branch2	APA453.0E22.0A70	A4:53:0E:22:0A:70	Device online	Feb 15 2022 09:01:23	<input type="checkbox"/>
Default	Branch2	ciscoAp	0E:C9:C8:29:A0:01	Device reachable	Feb 15 2022 08:58:43	<input type="checkbox"/>
Default	Branch2	AP6C71.0D54.02A4	6C:71:0D:54:02:A4	Device reachable	Feb 15 2022 08:58:22	<input type="checkbox"/>
Default	Branch2	AP5CE1.76F2.3F0C	5C:E1:76:F2:3F:0C	Device reachable	Feb 15 2022 08:58:22	<input type="checkbox"/>

表 31: 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	情報	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	警告	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	アラート	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	警告	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 (プローブが認証されたとき)
クレデンシャルが必要です/ユーザー ID	警告	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 (プローブが認証されたとき)
デバイスサービス/SNMP	警告	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	警告	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)

イベント	レベル	説明	自動的にクリアされるか
状況	警告/アラート	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			
ファームウェア	情報	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	警告/アラート	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。	非対応
メンテナンス有効期限	警告/アラート	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	警告/アラート	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	警告/アラート	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）
接続済みクライアント	警告/アラート	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

1 つのデバイスまたはすべてのデバイスに対して現在有効な通知を表示するには、以下の手順を実行します。

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。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。

表 32:

アイコン	Description
	情報（緑色の円形のアイコン）
	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）

- [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。
 - 表示されている通知のフィルタリング：この操作の手順を以下に示します。
- 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。使用可能なフィルタは次のとおりです。

表 33: 使用可能なフィルタ

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	表示する通知の重大度。次のいずれかを指定できます。 <ul style="list-style-type: none"> • Info • Warning • Alert <p>[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。</p>
ACK を含める	確認応答済みの通知を含めます。

フィルタ	説明
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。
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。 フィルタ内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、「[組織の管理](#)」または「[モニタリングのデフォルト値の変更](#)」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、[イベントログ (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。

[基本情報 (Basic Info)] パネルまたは[デバイスの詳細] パネルには、個々のデバイスが表示されます。

[基本情報 (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。

[デバイスの詳細 (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) [デバイスの詳細 (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冠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 \(139 ページ\)](#)
- [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 \(139 ページ\)](#)
- [スケジュールプロファイルの管理 \(141 ページ\)](#)
- [変更期間の管理 \(142 ページ\)](#)

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、定期的に行う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、次の手順を実行します。

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 34: 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を表示を制限します。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。
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わけではありません。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、次の手順を実行します。

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。ジョブが変更ウィンドウで行われるようにスケジュールされている場合、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 \(142 ページ\)](#) 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、次の手順を実行します。

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. 提供されたフォームを使用して、必要に応じ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、次の手順を実行します。

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. テーブルの右端にある [Actions] 列を確認します。プロファイルを削除するには [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、次の手順を実行します。

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. テーブルの右端にある [Actions] 列を確認します。[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。組織の変更期間を変更するには、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。

組織の変更期間とは異なる特定のネットワークの変更期間を設定するには、次の手順を実行します。

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。

組織の変更期間を使用するようにネットワークを設定するには、次の手順を実行します。

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 \(145 ページ\)](#)
- [Probe のログ設定の管理 \(146 ページ\)](#)

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、次の手順を実行します。

1. [Network] に移動し、診断情報を収集するネットワークを選択します。[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。

2. 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。

3. [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、以下の手順を実行します。

1. 診断情報ファイルを、PC 上の便利な場所に解凍します。
2. Web ブラウザを使用して、作成した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サポートエンジニアの主要な関心事です。

特定のネットワークのログ設定を変更するには、[Network] に移動し、設定を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、[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 35: ログ設定

フィールド	説明
Log Level	<p>ログに記録する詳細レベル。次のオプションを使用できます。</p> <ul style="list-style-type: none"> • [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

フィールド	説明
Log Module	<p>メッセージを保存するモジュール。次のオプションを使用できます。</p> <ul style="list-style-type: none"> • [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 <p>必要に応じて複数のモジュールを選択できます。</p>

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 \(145 ページ\)](#) 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。

- [よくある質問 \(FAQ\) \(149 ページ\)](#)
- [検出の FAQ \(150 ページ\)](#)
- [設定の FAQ \(151 ページ\)](#)
- [セキュリティ上の留意事項の FAQ \(151 ページ\)](#)
- [リモートアクセスの FAQ \(157 ページ\)](#)
- [ソフトウェアアップデートの FAQ \(158 ページ\)](#)

よくある質問 (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 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* と呼ぶ。RFC 6762 と 6763 を参照)
- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (『IEEE specification 802.1AB』を参照)
- Simple Network Management Protocol (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構築します。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 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 サーバーと SNMP サーバー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. デバイスのあるデバイス 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 36: 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	利用方法
TCP 22	インバウンド	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	インバウンド	HTTP	Dashboard への Web アクセス。セキュア Web サーバー（ポート 443）へのリダイレクト。
TCP 443	インバウンド	HTTPS [多重化 TCP (Multiplexed 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	利用方法
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)	インバウンド	HTTPS	デバイスへのリモートアクセス。 この範囲は、[システム (System)] > [プラットフォーム設定 (Platform Settings)] ページを使用して制御できます。
UDP 53	アウトバウンド	DNS	ドメイン名解決。
UDP 123	アウトバウンド	NTP	時刻同期。
TCP 443	アウトバウンド	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にアクセスします。
UDP 5353	アウトバウンド	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 37: 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	利用方法
TCP 22	インバウンド	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	インバウンド	HTTP	Probe への Web アクセス。セキュア Web サーバー (ポート 443) へのリダイレクト。
TCP 443	インバウンド	HTTPS	Probe へのセキュア Web アクセス。

ポート	方向	プロトコル	利用方法
UDP 5353	インバウンド	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	アウトバウンド	DNS	ドメイン名解決。
UDP 123	アウトバウンド	NTP	時刻同期
TCP 80	アウトバウンド	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	アウトバウンド	SNMP	ネットワーク デバイスの管理。
TCP 443	アウトバウンド	HTTPS [多重化 TCP (Multiplexed 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 サービスにアクセスします。 Probe と Dashboard 間の通信。
UDP 5353	アウトバウンド	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 38 : 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。このサーバーは、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。
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。このサーバーは、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。 これらのサーバーは、[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。このサーバーは、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ーで使用するプロセスとシステムサービスを示します。

表 39: 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	Web サーバー
/usr/lib/ciscobusiness/dashboard/bin/mongosvc /usr/lib/ciscobusiness/dashboard/bin/mongod	データベース 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ー
/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 40: 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/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 サーバー Dashboard サーバーに配置されている場合、 プローブは Dashboard Web サーバーを共有 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、ユーザーは 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、そのデバイス用の工場デフォルトのログイン情報（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セキュリティ保護されていますか。
- 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ログイン情報は、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、**finditprb recoverpassword** ツールを実行するか、Manager のコンソールにログインし、**finditmgr 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、パスワードには AWS インスタンス ID が設定されます。

- Q. 仮想マシンのブートローダ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。

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ていますか。
- 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パススルーします。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 (HTTP Header)] 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` ユーザーでログオンし、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 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` ユーザーでログオンし、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 を使用している際に 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` ユーザーでログオンし、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

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を超える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。



第 17 章

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。

- [概要（161 ページ）](#)
- [設定構文（161 ページ）](#)
- [設定テンプレートの作成（164 ページ）](#)

概要

設定テンプレートは、設定要件が非常に類似している複数のデバイスがある場合に使用できませんが、いくつかのパラメータはデバイスごとに異なっている必要があります。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。実際には、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。



- (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を変更された場合、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。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、このコンテンツ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 URI としてさらに絞り込むことができます。その場合、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、生成されたコンフィギュレーション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 \(110 ページ\)](#) 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。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]** に移動してテンプレートエディタで設定を選択し、**[Edit]** アイコンをクリックして設定を開始します。
2. 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。リストについては、次の表 41: 一般的なエディタコマンドを参照してください。
「設定構文」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。
3. 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「**テンプレートメタデータ**」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、ユーザにフォームがどのように表示されるかを確認できます。
4. 手順 2 と手順 3 を繰り返して、デバイスごとに異なるすべての設定パラメータのプレースホルダを作成します。
5. 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。

表 41: 一般的なエディタコマンド

機能	Description	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

機能	Description	キーのバインド	
		PC	Mac
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