



## **Cisco Business Dashboard & Probe アドミニストレーションガイド、バージョン 2.2.x**

初版：2020年7月14日

最終更新：2020年9月2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/](http://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](http://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)

© 2020 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/](http://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.

© 2020 Cisco Systems, Inc. All rights reserved.





## 目次

---

第 1 章	<b>Cisco Business ダッシュボードの概要</b> 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 5

---

第 2 章	<b>Cisco Business Dashboard &amp; Probe の使用</b> 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

---

第 3 章	<b>モニタリング ダッシュボード</b> 17
	監視ダッシュボードについて 17
	ウィジェットの追加 18
	ウィジェットの変更 18
	ウィジェットの削除 18
	ダッシュボードのレイアウトの変更 19

---

第 4 章	<b>ネットワーク</b> 21
	ネットワークについて 21
	ネットワークの詳細について 23
	ネットワーク ビューについて 24

トポロジマップとツールの概要	24
基本的なデバイス情報の表示	28
デバイスアクションの実行	30
デバイス管理インターフェイスへのアクセス	32
詳細なデバイス情報の表示	32
フロアプランの使用方法	35

---

**第 5 章****インベントリ 39**

デバイスインベントリの表示	39
---------------	----

---

**第 6 章****ポート管理 43**

ポート管理について	43
-----------	----

---

**第 7 章****ネットワーク設定 45**

ネットワーク設定について	45
ウィザードの使用方法	45
時刻管理の設定	46
DNS リゾルバの設定	47
認証の設定	47
仮想 LAN の設定	48
ワイヤレス LAN の設定	49

---

**第 8 章****ネットワーク プラグアンドプレイ 51**

ネットワーク プラグアンドプレイについて	51
ネットワーク要件	51
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	54
ネットワーク プラグアンドプレイ サービスの設定	55
ネットワーク プラグアンドプレイのモニタリング	63

---

**第 9 章****イベントログ 65**

イベントログについて	65
------------	----

---

**第 10 章****レポート 67**

- レポートについて 67
- ライフサイクル レポートの表示 68
- サポート終了レポートの表示 69
- メンテナンス レポートの表示 70
- ワイヤレス ネットワーク レポートの表示 71
- ワイヤレス クライアント レポートの表示 73

---

**第 11 章****管理 77**

- 管理について 77
- 組織の管理 78
- デバイス グループの管理 80
- デバイス クレデンシャルの管理 81
- ユーザの管理 83
- モニタリングのデフォルト値の変更 86
- モニタリング プロファイルの管理 87
- ログイン 試行の表示 89
- レポート設定の管理 90

---

**第 12 章****システム 91**

- システムについて 91
- ライセンスの管理 92
- 証明書の管理 94
- 電子メール設定の管理 97
- API 使用状況の表示 98
- Dashboard 設定のバックアップと復元 99
- プラットフォーム設定の管理 100
- プライバシーの管理 102
- ログ設定の管理 105
- ローカル Probe の管理 107

---

第 13 章	<b>通知</b>	<b>109</b>
	通知について	109
	サポートされる通知	109
	現在のデバイスの通知の表示とフィルタリング	111
	デバイスの履歴通知の表示とフィルタリング	112

---

第 14 章	<b>トラブルシューティング</b>	<b>113</b>
	ネットワーク診断情報の取得	113
	プローブのログ設定の管理	114

---

第 15 章	<b>よくある質問</b>	<b>117</b>
	よくある質問 (FAQ)	117
	検出の FAQ	118
	設定の FAQ	119
	セキュリティ上の留意事項の FAQ	119
	リモートアクセスの FAQ	122
	ソフトウェアアップデートの FAQ	123

---

第 16 章	<b>付録 A : 設定テンプレートの管理</b>	<b>125</b>
	概要	125
	設定構文	125
	設定テンプレートの作成	128





# 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](#) (5 ページ)

## Cisco Business ダッシュボードについて

Cisco Business ダッシュボードには Cisco Business ネットワークを監視および管理するのに役立つツールが用意されています。Cisco Business ダッシュボードはネットワークを自動的に検出し、シスコのスイッチ、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 Cisco Business デバイスを設定および監視できます。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、2つの独立した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型アプリケーションです。*Dashboard*とも呼ばれる主要な Cisco Business Dashboard アプリケーションと、*Probe*とも呼ばれる Cisco Business ダッシュボード Probe の1つまたは複数のインスタンスで構成されます。

Cisco Business ダッシュボードのシングルインスタンスがネットワーク内の使いやすい場所にインストールされます。*Dashboard*のユーザ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。

Cisco Business ダッシュボードプローブのインスタンスがネットワーク内の各サイトに1つずつインストールされ、*Dashboard*と関連付けられます。*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。

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おり、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。それは次のようなものです。

- **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ダッシュボードに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ダッシュボードに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：デバイスサポートリスト](#)』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 クイックスタートガイド](#)』を参照してください。
- **設置ガイド**

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。

対応プラットフォーム	所在地
Amazon Web Services	<a href="#">Cisco Business Dashboard インストールガイド（Amazon Web Services 用）</a>
Oracle VirtualBox	<a href="#">Cisco Business Dashboard インストールガイド（Oracle VirtualBox 用）</a>
Microsoft Hyper-V	<a href="#">Cisco Business Dashboard インストールガイド（Microsoft Hyper-V 用）</a>

対応プラットフォーム	所在地
VMWare vSphere、ワークステーション、およびフュージョン	<a href="#">Cisco Business Dashboard インストールガイド (VMWare 用)</a>
Ubuntu Linux (Dashboard & Probe) および Raspbian Linux (Probe のみ)	<a href="#">Cisco Business Dashboard インストールガイド (Linux 用)</a>

## 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"> <li>記述子ファイル (.OVF)</li> <li>Manifest (.MF) および証明書ファイル (任意)</li> </ul>
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、 <a href="https://www.raspberrypi.org/">https://www.raspberrypi.org/</a> を参照してください。
Raspbian	Raspberry Pi 向けに最適化された Debian ベースの Linux ディストリビューション。詳細については、 <a href="https://www.raspbian.org/">https://www.raspbian.org/</a> 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"> <li>• VMWare ESXi</li> <li>• VMWare V5</li> <li>• vSphere Server</li> <li>• VMWare Workstation</li> </ul>	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、ユーザがリモート接続できるようにするユーザインターフェイス。vSphere Client のプライマリインターフェイスを使用して、VM、そのリソース、およびホストの作成、管理、およびモニタを行うことができます。VM へのコンソールアクセスも提供します。

## 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、ハイパーバイザー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) を実行している必要があります。シスコでは、Ubuntu サーバ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	#vCPU	RAM	ディスク領域
最大 300	2	4GB	60GB
最大 2,500	12	24 GB	60GB

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.xlarge : 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 [常に信頼] 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、「よくある質問」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。

- PC 上で実行する 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 x 1
  - 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 バージョン 16.04.x (Xenial Xerus)
- CPU：64 ビット インテル アーキテクチャ x 1
- 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：Raspbian 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：デバイスサポートリスト](#)」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 GUI の使用

Cisco Business ダッシュボードの GUI の概要とナビゲーションペインのリンクの説明

[ホーム] ウィンドウ

図 1: Cisco Business Dashboard ホームページ

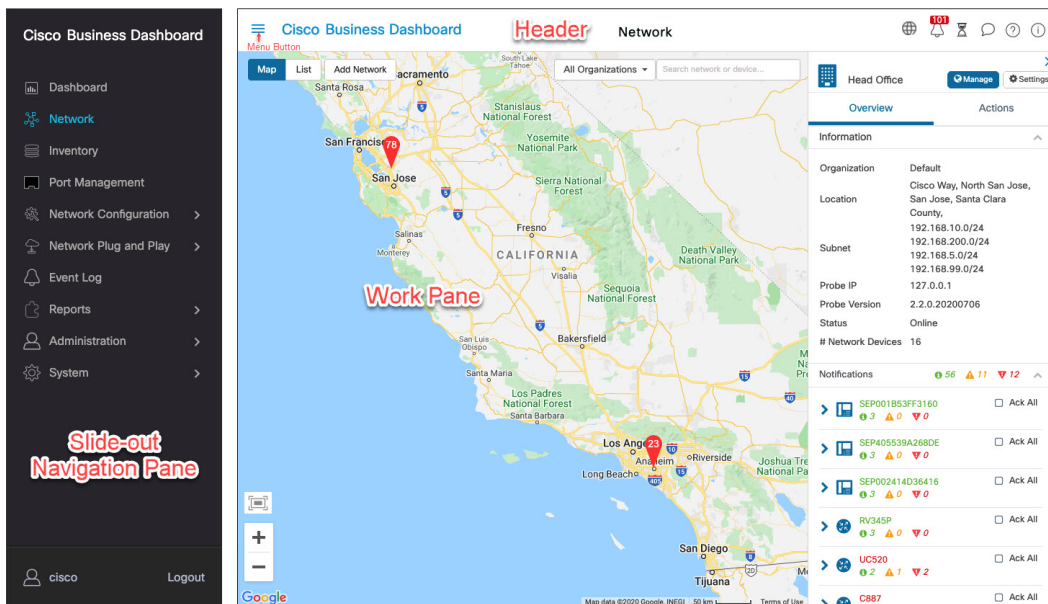





表 2: Cisco Business Dashboard ホームページ

名前	説明
[ナビゲーション] ペイン	<p>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、[メニュー (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。</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] ツールバー	<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"> <li>• ナビゲーションウィンドウを表示するためのメニューボタン</li> <li>• ヘッダー</li> <li>• 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</li> </ul>

### [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	説明
	ダッシュボード	ダッシュボードを使用すると、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。
	ネットワーク	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	[インベントリ]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、リポ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	説明
	ポート管理	ポート管理では、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。
	ネットワーク設定	[ネットワークの設定] 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。
	ネットワークプラグアンドプレイ	[ネットワーク プラグアンドプレイ] 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	[イベント] 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。
	レポート	[レポート] 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。
	管理 (Administration)	[管理] 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	[システム] 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。
	ユーザ オプション	現在ログインしているユーザは、[ログアウト (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	説明
	[メニュー (Menu) ] 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 (Language Selection) ]	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、[通知] 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 <a href="#">現在のデバイスの通知の表示とフィルタリング (111 ページ)</a> 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、および完了済みの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、[ホーム] ページが表示されます。

図 2: Cisco Business Dashboard ホームページ

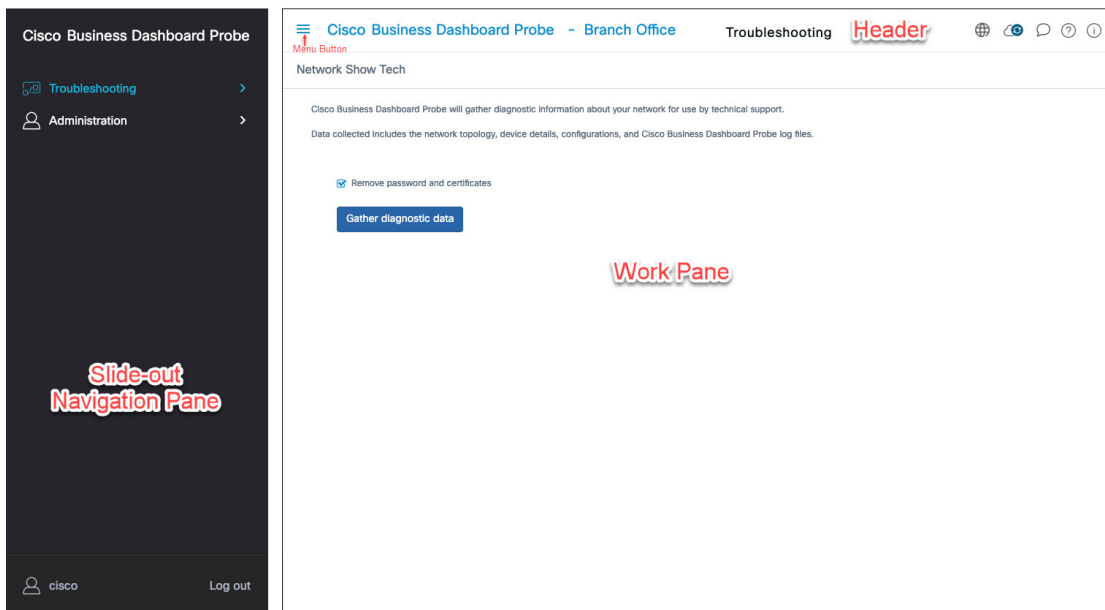





表 5: Cisco Business Dashboard ホームページ

名前	説明
[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、[メニュー (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"> <li>• ナビゲーションウィンドウを表示するためのメニューボタン</li> <li>• Probe のサイト名を含むヘッダー テキスト</li> <li>• 言語選択ドロップダウン</li> <li>• 通知、フィードバック、コンテキスト対応ヘルプなどの機能のための一連のアイコン</li> </ul>

### [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	説明
	トラブルシューティング	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、[トラブルシューティング] セクションにあります。
	管理 (Administration)	[管理 (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。
	ユーザオプション	現在ログインしているユーザは、[ログアウト (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	説明
	[メニュー (Menu)] 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 (Language Selection)]	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 ダッシュボードとプローブ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	説明
	<b>Cisco Business Dashboard Probe</b> 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](https://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 [Cisco Business Dashboard について (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. [Cisco Business Dashboard について (About Cisco Business Dashboard)] をクリックして、[Cisco Business Dashboard について (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、[アップグレード (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。[Cisco Business Dashboard について (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/jp/go/cbd-sw> に移動し、右下の製品選択パネルから [ソフトウェアのダウンロード (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. [Cisco Business Dashboardについて (About Cisco Business Dashboard)] をクリックして、[Cisco Business Dashboardについて (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、[アップグレード] 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 [ネットワーク] を選択します。[マップビュー (Map View)] または [リスト (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 [基本情報 (Basic Info)] パネルで [アクション (Action)] タブを選択します。
4. [アップグレード (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プローブ アプリケーションを更新することができません。
-





## 第 3 章

# モニタリング 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 \(17 ページ\)](#)
- [ウィジェットの追加 \(18 ページ\)](#)
- [ウィジェットの変更 \(18 ページ\)](#)
- [ウィジェットの削除 \(18 ページ\)](#)
- [ダッシュボードのレイアウトの変更 \(19 ページ\)](#)

## 監視ダッシュボードについて

Cisco Business ダッシュボードの [ダッシュボード] ページでは、ネットワークとそのデバイスのリアルタイムパフォーマンスを表示でき、データがグラフィカルな形式で提供されます。この監視ダッシュボードは、ユーザ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。

- [インベントリの概要] ウィジェット：ネットワークで検出されたデバイスの内訳を表示します。
- [デバイスヘルス] ウィジェット：ネットワーク内のデバイスの全体的な稼働状態を表示します
- [WLAN クライアント カウント] ウィジェット：選択したワイヤレス ネットワークに関連付けられているデバイスの数を表示します
- [デバイス クライアント カウント] ウィジェット：選択したワイヤレス アクセス ポイントに関連付けられているデバイスの数を表示します
- [ワイヤレス トップ 10] ウィジェット：トラフィックまたはクライアント数に基づいた上位 10 のワイヤレス ネットワーク、アクセス ポイント、またはクライアントを表示します。
- [トラフィック] ウィジェット：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。**ダッシュボード**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。これを使用すると、表示されるデータをさらに絞り込むことができます。

## 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。新たに選択した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

- 
- ステップ1** 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2** ウィジェットの右上にある歯車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。また、ダッシュボードが**編集モード**のときにウィジェットに表示される編集アイコンをクリックして、ウィジェットのタイトルを変更することもできます。
- 

## 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

ダッシュボードのレイアウトは、次の手順を使用して簡単に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

# ネットワーク

この章は、次の項で構成されています。

- [ネットワークについて \(21 ページ\)](#)
- [ネットワークの詳細について \(23 ページ\)](#)
- [ネットワーク ビューについて \(24 ページ\)](#)
- [トポロジマップとツールの概要 \(24 ページ\)](#)
- [基本的なデバイス情報の表示 \(28 ページ\)](#)
- [デバイスアクションの実行 \(30 ページ\)](#)
- [デバイス管理インターフェイスへのアクセス \(32 ページ\)](#)
- [詳細なデバイス情報の表示 \(32 ページ\)](#)
- [フロアプランの使用方法 \(35 ページ\)](#)

## ネットワークについて

[ネットワーク] 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。[マップ] 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。[リスト] 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。

[ネットワーク マップ] には以下のコントロールがあります。

- [マップ/リスト] 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。
- [ネットワークの追加] 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。

- [組織]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。
- [検索]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。
- [ズーム]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。
- [画面のサイズに合わせる]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。

[リスト ビュー]では、次のコントロールを使用できます。

- [マップ/リスト]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。
- [列の選択]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。
- [ネットワークの追加]：そのネットワークのプローブを展開する前に、プラス (+) 記号をクリックして新しいネットワークを追加します。
- [更新]：[更新] 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。
- [組織]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。
- [検索]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 [基本情報] パネルが表示されます。[基本情報] 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
- ネットワークのプローブ 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、[基本情報] 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。

- [管理] 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。
- [設定] をクリックすると、[ネットワークの詳細] パネルが表示されます。[ネットワークの詳細] パネルの詳細については、[ネットワークの詳細について \(23 ページ\)](#) を参照してください。
- [アクション] 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。
  - [削除 (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。
  - [アップグレード] をクリックすると、このネットワークのプロブ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

[ネットワークの詳細] 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。この情報には、次のものが含まれます。

- 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クレデンシャル
- このネットワーク内のプロブのロギング設定。プロブログの設定方法の詳細については、[プロブのログ設定の管理 \(114 ページ\)](#) 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 [基本情報] パネルの [管理] をクリックすると、そのネットワークの [ネットワーク ビュー] が表示されます。[ネットワーク ビュー] 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。

- [トポロジ] 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
- [フロアプラン] 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、[ネットワーク ビュー] 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。

- [組織とネットワーク] 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。
- [ネットワークアクション] 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、[ネットワークアクション] 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>) 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> 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 [基本情報] パネルを表示できます。[基本情報] 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。



[トポロジ]マップで[オーバーレイ]をクリックすると[オーバーレイとフィルタ]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

[トポロジマップ]にアクセスするには、まず[ナビゲーション]から[ネットワーク]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、[表示]をクリックします。そのネットワークの[トポロジマップ]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、[トポロジ]マップの左上にあります。








表 8: トポロジコントロール

アイコン	アイコンの名前	説明
	拡大	[トポロジ]ウィンドウのビューを調整します。表示エリアでネットワークのサイズを拡大するには、メニューバーの <b>+</b> (プラス) アイコンをクリックします。
	縮小	[トポロジ]ウィンドウのビューを調整します。表示エリアでネットワークのサイズを縮小するには、 <b>-</b> (マイナス) アイコンをクリックします。
	リレイアウト トポロジ	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。
	選択に合わせてズーム	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。

## トポロジアイコン

次のアイコンが [トポロジ] ウィンドウに表示されます。

表 9: トポロジアイコン

アイコン	ネットワーク要素	説明
	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。
	Host	有線接続でネットワークに接続したホストを表します。
	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、[オーバーレイ] をクリックすると [トポロジ] マップの右側に表示されます。[オーバーレイ] は [トポロジ] の右上の検索ボックスの横にあります。

表 10: [Overlays &amp; Filters] パネル

項目	説明
オーバーレイの選択	<p>この機能は、ビューの選択に基づく追加情報で [トポロジ] 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"> <li>• [リンク使用率ビュー]: 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、[トポロジ] 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。</li> </ul> <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"> <li>• [VLAN ビュー]: 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。</li> </ul> <p>[Overlay] ドロップダウンで [VLAN ビュー] 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"> <li>• [POE ビュー]: 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。</li> <li>• [L2 パストレース]: 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。</li> </ul>
タグを選択する	<p>[タグの選択] ラベルの下のテキストボックスで <b>デバイス タグ</b> 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、[詳細情報] パネルに割り当てられます。</p>
表示のみ: <ul style="list-style-type: none"> <li>• ルータ</li> <li>• スイッチ</li> <li>• ワイヤレス</li> <li>• ホスト</li> <li>• その他</li> </ul>	<p>[トポロジ] 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。[基本情報]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 \(32 ページ\)](#) 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 \(32 ページ\)](#) 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** [ネットワーク] ページでネットワークを選択し、[管理] 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** [基本情報] パネルの [概要] 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	説明
情報パネル	
モデル	デバイスのモデル名。
説明	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 アドレス	<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。
ステータス (Status)	デバイスのオンライン/オフライン ステータス。
[ドメイン (Domain)]	デバイスのドメイン名。

項目名	説明
Vendor	デバイスのメーカー。
ネットワーク	デバイスがあるネットワークの名前。
組織	デバイスが属する組織。
<b>[通知] パネル</b>	
<p>[通知パネルヘッダー] : [通知]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>[通知パネル本文] : 通知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、<a href="#">現在のデバイスの通知の表示とフィルタリング (111 ページ)</a> 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>	
<b>[イベント] パネル</b>	
<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、[イベントログ (Event Log) ] にアクセスします。</p>	
<b>[POE] パネル</b>	
<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>	
<b>[スタック情報] パネル</b>	
<p>[スタック情報] 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>	
<b>サービス</b>	
<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>	
<b>接続装置</b>	
<p>ホスト デバイスには、[接続されたデバイス] 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>	

[概要] タブに加え、[基本情報] パネルにも [アクション] 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 \(30 ページ\)](#) を参照してください。

## デバイスアクションの実行

ファームウェアの更新、設定のバックアップと復元、リブートなどのアクションを、ネットワーク内のデバイスに対して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] ページまたは [インベントリ] ページで、アクションを実行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** [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。
バックアップ コンフィギュレーション	<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"> <li>[バックアップ設定] をクリックします。</li> <li>[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。</li> <li>[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。</li> </ol> <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"> <li>• [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</li> <li>• [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</li> <li>• [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</li> </ul> <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"> <li>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。</li> </ol> <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"> <li>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。</li> </ol> <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>(注) 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としたときに、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>

## 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** [トポロジ] ページまたは [インベントリ] 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** [基本情報] パネルで、右上隅にある [表示] 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) [表示 (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** [トポロジ] ページまたは [インベントリ] 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** [基本情報] パネルで、右上隅にある [その他の情報] をクリックします。

**ステップ3** [詳細情報] 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。

- [ダッシュボード] : 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
- [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。
- [ワイヤレス LAN] : 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。
- [イベント ログ] : 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
- [設定のバックアップ] : 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。

- [保留中の設定] : 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	説明
ホスト名	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 [編集] をクリックします。 <b>Save</b> をクリックして変更を保存します。
モデル	デバイスのモデル名。
MAC アドレス	<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。
ステータス (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。
アクション	[アクション] ドロップダウンと [デバイス GUI を開く] アイコンを使用すると、[詳細情報] 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。
[ドメイン (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。
説明	デバイスまたは製品の説明。
デバイス グループ (Device Group)	このデバイスが属するデバイス グループ。
ネットワーク	このデバイスが属するネットワーク。

項目名	説明
組織	このデバイスが属する組織。
PnP パラメータ	ネットワーク プラグ アンド プレイを使用してデバイスに配信されるイメージと設定ファイル。[編集] アイコンをクリックして変更を加え、[保存] アイコンをクリックして変更を適用するか、または[キャンセル] をクリックして保存せずに終了します。
TAG	[TAG] フィールドに任意の英数字を入力し、 <b>Enter</b> 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 <b>✕</b> をクリックします。 <b>Save</b> 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。
Firmware Version	現在デバイスで動作しているファームウェアのバージョン。新しいバージョンを利用できる場合、そのバージョンが現在のバージョンの横の括弧内に表示されます。アップデートのリリース ノートを表示したり、それをデバイスに適用するためのアイコンも表示されます。
検出方法	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。
保留中の設定	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** [ダッシュボード] 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** 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 \(43 ページ\)](#) を参照してください。
- ステップ 7** 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 8** [イベント ログ] 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 9** 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、[設定バックアップ] 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
タイムスタンプ	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。
備考	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。
バックアップの実行者	コンフィギュレーションをバックアップしたユーザ。
アクション	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"> <li>• [デバイスへの設定の復元] : 選択したバックアップをデバイスに復元します。</li> <li>• [PC への設定の保存] : 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</li> <li>• [設定の削除 (Delete configuration) ] : バックアップを削除します。</li> <li>• [設定の表示] : 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。</li> </ul>

また、[バックアップ設定] 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 10** [保留中の設定] 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。

## フロアプランの使用方法

[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. [ネットワーク ビュー] に移動し、[フロアプラン] 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 [ホーム] 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[新しいフロア]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。
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. [ネットワーク ビュー]に移動し、[フロアプラン]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. [デバイスの追加]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、正しい場所にあるフロアプラン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. [ネットワーク ビュー]に移動し、[フロアプラン]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. [ネットワーク ビュー]に移動し、[フロアプラン]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[ホーム]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[編集]アイコンをクリックします。変更が完了したら、[保存]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[編集]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、[保存]アイコンをクリックします。

### フロアプランの削除

1. [ネットワーク ビュー]に移動し、[フロアプラン]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[ホーム]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[削除]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[削除]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 \(39 ページ\)](#)

## デバイス インベントリの表示

[インベントリ]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

品目	説明
ホスト名	デバイス名を表示します。
Typeタイプ (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)。
タグ	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かつ一意であり、ネットワーク内の他のデバイスでは使用されません。
Serial Number	デバイスのシリアル番号。
Version	デバイスの現在のファームウェア バージョン。

品目	説明
[ベンダー (Vendor)] (デフォルトでは非表示)	デバイスを製造したベンダー。
モデル	デバイスのモデル名。
組織	デバイスが属する組織。
ネットワーク	デバイスが属するネットワーク。
通知	デバイスの未処理通知の数
<b>PnP</b> ステータス (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。

[インベントリ] ページでは、次の追加のコントロールを使用できます。

- [列の選択] 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。
- [フィルタ] ボックス：[フィルタ] ボックス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。
- [追加] 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。
- [更新] 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。
- [アクション] 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。
  - 最新ファームウェアのダウンロード
  - ローカルからのファームウェア アップグレードの適用
  - バックアップ コンフィギュレーション
  - 構成の復元
  - デバイスの再起動
  - 実行設定を保存
  - 削除



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) これらの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

この章は、次の項で構成されています。

- [ポート管理について \(43 ページ\)](#)

## ポート管理について

[ポート管理] 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 ビューを提供します。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] : このビューでは、物理レイヤでポートのステータスを確認したり、設定を変更できます。速度、二重化、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。
- [Smartport] : このビューでは、各ポートの現在の Smartport ロールを表示したり、ロールを変更できます。各ポートには、現在のロールを示すアイコンがオーバーレイ表示されます。



(注) Smartport は、組み込み (またはユーザ定義) 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 (General)] : [全般 (General)] 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] : 速度とデュプレックスの設定を制御できます。
- [VLAN] : [VLAN] 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] : [POE] 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。[電源切り替え] ボタンをクリックして、接続している POE デバイスの電源を切り替えることもできます。
- [グリーンイーサネット] : [グリーンイーサネット] パネルでは、ポートの Energy Efficient Ethernet (EEE) 設定を管理することができます。
- [Smartports] : [Smartports] パネルには、ポートで利用可能な Smartports のルールが表示されます。ル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ル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

# ネットワーク設定

この章は、次の項で構成されています。

- ネットワーク設定について (45 ページ)
- ウィザードの使用方法 (45 ページ)
- 時刻管理の設定 (46 ページ)
- DNS リゾルバの設定 (47 ページ)
- 認証の設定 (47 ページ)
- 仮想 LAN の設定 (48 ページ)
- ワイヤレス LAN の設定 (49 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。

### ウィザードの使用方法

1. [ネットワーク設定] > [ウィザード] 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。[次へ (Next)] をクリックします。

3. 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。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。
5. 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の作成

1. [ネットワーク設定] > [時刻管理] 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の変更

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の削除

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の作成

1. [ネットワーク設定] > [DNS リゾルバ] 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の変更

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の削除

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 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の作成

1. [ネットワーク設定] > [認証] 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. ローカルユーザ認証用に1つ以上のユーザ名とパスワードの組み合わせを指定します。+ (プラス) アイコンをクリックすることでユーザを追加できます。
5. 複雑なパスワードの使用を義務付けることも選択できます。
6. [保存 (Save) ]をクリックします。

#### 認証設定プロファイルの変更

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の削除

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]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 の作成

1. [ネットワーク設定] > [仮想 LAN] 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 の変更

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 の削除

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。

### 作成されていない VLAN の削除 Cisco Business ダッシュボード

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。

### ワイヤレス LAN の作成

1. [ネットワーク設定] > [ワイヤレス LAN] 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 の変更

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 の削除

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。
- 

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

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 \(51 ページ\)](#)
- [ネットワーク要件 \(51 ページ\)](#)
- [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 \(54 ページ\)](#)
- [ネットワーク プラグアンドプレイ サービスの設定 \(55 ページ\)](#)
- [ネットワーク プラグアンドプレイのモニタリング \(63 ページ\)](#)

## ネットワーク プラグアンドプレイについて

[ネットワーク プラグアンドプレイ]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。

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あります。

- **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。文字列のこの部分を変更する必要はありません。
- **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 のデフォルトポートは 80、HTTPS のデフォルトポートは 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。このパラメータは、trustpool セキュリティを使用してすべてのデバイスが確実に同期されるようにする場合に必須です。

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、ローカル ネーム サーバを使用してこの FQDN の IP アドレスを解決します。

### 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。証明書を受け入れ、接続を続行するには、証明書が次の条件を満たしている必要があります。

- 証明書は信頼できる証明機関 (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、[共通名] フィールドまたは [サブジェクト代替名] 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、[共通名] フィールドまたは [サブジェクト代替名] 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、[共通名] フィールドまたは [サブジェクト代替名] 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。[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ラ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 \(94 ページ\)](#) 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。[次へ (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

[ネットワーク プラグアンドプレイ] ダッシュボードにより、ネットワーク プラグアンドプレイ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、さまざまなステータスの意味を示します。

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 (Status)	説明 (Description)
<b>グループ (Groups)</b>	
事前プロビジョニング済み	保留状態の PnP 対応デバイスのみが含まれるデバイスグループ。
進行中 (In Progress)	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
Provisioned	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
<b>有効なデバイス</b>	
Pending	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
Provisioned	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。
<b>要求元不明デバイス</b>	
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、[すべての組織]のデータを表示する[管理者]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. [ネットワーク プラグ アンド プレイ]>[対応デバイス]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[新しいデバイスの追加 (Add New Device)]に入力し、[次へ (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[デフォルト (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の含まれているテンプレートである場合は、このデバイスで使用する必要があ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. [次へ (Next)]をクリックして、[サマリー (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[プレビュー (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、[終了 (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. [ネットワーク プラグ アンド プレイ (Network Plug and Play)]>[対応デバイス (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、[編集 (Edit)]をクリックします。または、デバイスの名前をクリックすることもできます。
3. [次へ (Next)]をクリックして[デバイスのプロビジョニング (Provision Device)]画面を表示します。必要に応じて、イメージやコンフィギュレーションファイルを変更し、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. [次へ (Next)] をクリックして、[サマリー (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[プレビュー (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、[終了 (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設定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. [ネットワーク プラグアンドプレイ]>[対応デバイス] 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、[削除 (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設定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 [対応デバイス (Enabled Devices)] テーブルに追加されます。

### 要求元不明デバイス



- (注) [要求元不明デバイス] ページは、管理者のみが使用できます。

要求元不明デバイスとは、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. [ネットワーク プラグアンドプレイ]>[要求されていないデバイス] に移動し、[未要求] 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 [要求元不明デバイス (Unclaimed Device)] フォームに入力し、[次へ (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[デフォルト (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の含まれているテンプレートである場合は、このデバイスで使用する必要があ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. [次へ (Next)] をクリックして、[サマリー (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[プレビュー (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、[終了 (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 [未要求] リストから削除するには、以下を行います。

1. [ネットワーク プラグアンドプレイ]>[要求されていないデバイス]に移動し、[未要求] 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 [無視] をクリックします。

デバイスが [無視] 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. [ネットワーク プラグアンドプレイ]>[要求されていないデバイス]に移動し、[無視] タブを選択します。
2. 再要求するデバイスの[無視の解除] ボタンをクリックします。

デバイスが [未要求] 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。

### デバイスの自動要求



(注) [自動要求] 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. [ネットワーク プラグアンドプレイ]>[自動要求デバイス]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 [自動要求デバイス (Auto Claim Device) ] フォームに入力し、[次へ (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 [デフォルト (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の含まれているテンプレートである場合は、このデバイスで使用する必要があ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. [次へ (Next) ] をクリックして、[サマリー (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 [プレビュー (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、[終了 (Finish) ] をクリックします。

インベントリに存在していない新しいデバイスは、自動要求ルール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設定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 [要求元不明] 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

[イメージ] 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. [ネットワーク プラグアンドプレイ] > [イメージ] 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、[ファイルのアップロード] 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. [アップロード (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. [ネットワーク プラグアンドプレイ]>[イメージ]に移動します。
2. [イメージ]テーブルでイメージのオプションボタンを選択し、[編集]をクリックします。
3. [製品 ID のデフォルトイメージ]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. [保存 (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. [ネットワーク プラグアンドプレイ]>[イメージ]に移動します。
2. 削除するイメージのオプションボタンを選択し、[削除]をクリックします。

### デバイスの設定ファイル

[設定 (Configurations) ]ページでは、設定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、設定ファイルをデバイスに導入できます。設定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。

コンフィギュレーションファイルは、単純なテキストファイルである場合もあれば、複数のデバイスで同じコンフィギュレーション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。

さまざまなデバイスタイプの設定テンプレートから選択する機能が Dashboard アプリケーションに含まれています。これらのテンプレートはそのまま使用することもできますし、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。

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

左上のフィールドに設定の名前を入力します。組織を選択し、この設定をサポートする製品 ID のカンマ区切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。

4. 左側のテキスト領域にテキストを入力するか、または貼り付けて、設定を作成します。必要に応じて、右側のコントロールを使用してメタデータに適切な変更を加えます。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。

[プレビュー (Preview) ] ボタンを使用すると、デバイスに割り当てられたときに設定テンプレートがどのように表示されるかを確認できます。

5. 設定に問題なければ、[保存 (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。

1. [ネットワーク プラグアンドプレイ] > [設定] に移動します。
2. [アップロード (Upload) ] アイコンをクリックします。
3. ドロップダウンから設定に組織を選択します。設定の名前を指定し、必要に応じて説明を追加します。
4. ご使用のPCから設定ファイルをドラッグし、[ファイルのアップロード] 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. [アップロード (Upload) ] をクリックします。

コンフィギュレーション ファイルの内容を確認する必要がある場合、アップロードしたコンフィギュレーション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. [ネットワーク プラグアンドプレイ] > [設定] 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、[削除 (Delete) ] アイコンをクリックします。

### 設定の管理

[ネットワーク プラグアンドプレイの設定] 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。[チェックイン時間間隔] 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. [ネットワーク プラグアンドプレイ] > [設定] 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. [保存 (Save) ] をクリックします。

[チェックイン時間間隔] 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 [サブジェクト代替名 (Subject Alternative Name) ] フィールドに指定された値の他に、[共通名 (Common Name) ] フィールドの内容を [サブジェクト代替名 (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 \(94 ページ\)](#) 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、[対応デバイス] ページまたは [要求されていないデバイス] 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 ステータス] 列の表示を可能にすることで、[インベントリ] 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
保留中	デバイスが定義されている一方で、サービスには未接続。
プロビジョニング	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。
エラー	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。
プロビジョニング済み	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 \(65 ページ\)](#)

## 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。

- [時刻]：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。
- [重大度]：表示するイベントの重大度を選択します。[高く]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。
- [タイプ]：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。
- [ネットワーク]：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。
- [デバイス]：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

# レポート

---

この章は、次の項で構成されています。

- [レポートについて](#) (67 ページ)
- [ライフサイクルレポートの表示](#) (68 ページ)
- [サポート終了レポートの表示](#) (69 ページ)
- [メンテナンス レポートの表示](#) (70 ページ)
- [ワイヤレス ネットワーク レポートの表示](#) (71 ページ)
- [ワイヤレス クライアント レポートの表示](#) (73 ページ)

## レポートについて

Cisco Business ダッシュボードの[レポート]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。

- [ライフサイクルレポート]: 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。
- [サポート終了レポート]: 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。
- [メンテナンス レポート]: 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。
- [ワイヤレス ネットワーク]: 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。
- [ワイヤレスクライアント]: 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
ネットワーク名 (Network Name)	デバイスがあるネットワークの名前。
組織	デバイスが属する組織。
ホスト名	デバイスのホスト名。
デバイスタイプ	デバイスのタイプ。
モデル	デバイスのモデル番号。
製造週	デバイスの製造日を、週番号と年で表示します。
ファームウェアアップデート使用可能	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。
サポート終了ステータス	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。
メンテナンスステータス	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 [検索] ボックスを使用すると、結果をフィルタ処理できます。[検索] 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、[組織] 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[列選択]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
ネットワーク名 (Network Name)	デバイスがあるネットワークの名前。
組織	デバイスが属する組織。
製品ID	デバイスの製品 ID またはパーツ番号。
ホスト名	デバイスのホスト名。
デバイスタイプ	デバイスのタイプ。
現在の状況	製品のサポート終了プロセスの段階。
通知日	サポート終了案内が発行された日付。
販売最終日	製品がシスコによって販売されなくなる日付。
ソフトウェア リリースの最終日	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。
新しいサービス契約の最終日	デバイスに対して新たなサポート契約を結ぶ最終日付。
サービス更新の最終日	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。
[サポート終了日 (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。
推奨後継製品	推奨される後継製品。
製品速報	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 [検索] ボックスを使用すると、結果をフィルタ処理できます。[検索] 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、[組織] 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 [列選択] 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
ネットワーク名 (Network Name)	デバイスがあるネットワークの名前。
組織	デバイスが属する組織。
ホスト名	デバイスのホスト名。
デバイスタイプ	デバイスのタイプ。
モデル	デバイスのモデル番号。
Serial Number	デバイスのシリアル番号。
ステータス (Status)	デバイスの現在のサポート ステータス。
[カバレッジ終了日 (Coverage End Date) ]	現在のサポート契約が切れる日付。
保証終了日	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 [検索] ボックスを使用すると、結果をフィルタ処理できます。[検索] 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、[組織] 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[列選択]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。

表 20: ワイヤレス ネットワーク レポート

フィールド	説明
<b>ワイヤレス ネットワーク テーブル</b>	
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。
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。
<b>スペクトル使用テーブル</b>	
無線周波数	使用中の無線周波数帯 (2.4 GHz または 5 GHz) 。

フィールド	説明
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。
<b>ワイヤレス アクセス ポイント テーブル</b>	
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。
<b>不正なアクセス ポイント テーブル</b>	
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。



フィールド	説明
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。

次の表に提供される情報を示します。

表 21: ワイヤレスクライアントテーブル

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。

ワイヤレスクライアントテーブル	
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 22: 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）。
ユーザ名	ゲスト ポータルにクライアントが入力したユーザ名。
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。

ワイヤレス ゲスト テーブル	
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。



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





# 第 11 章

## 管理

---

この章は、次の項で構成されています。

- [管理について](#) (77 ページ)
- [組織の管理](#) (78 ページ)
- [デバイス グループの管理](#) (80 ページ)
- [デバイス クレデンシャルの管理](#) (81 ページ)
- [ユーザの管理](#) (83 ページ)
- [モニタリングのデフォルト値の変更](#) (86 ページ)
- [モニタリングプロファイルの管理](#) (87 ページ)
- [ログイン試行の表示](#) (89 ページ)
- [レポート設定の管理](#) (90 ページ)

## 管理について

Cisco Business ダッシュボードの [管理] 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。

- **[組織]** : Cisco Business ダッシュボード に組織を作成し、管理します。
- **[デバイスグループ]** : 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。
- **[デバイス クレデンシャル]** : ネットワーク デバイスにアクセスするときに使用するクレデンシャルを入力します。
- **[ユーザ]** : Cisco Business ダッシュボード へのユーザ アクセスを定義します。
- **[通知のデフォルト]** : 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。
- **[ログイン試行]** : 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。
- **[レポートの設定]** : 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。[通知のデフォルト値]と[レポート設定]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、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組織に属し、各ユーザは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. [管理] > [組織] 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. [保存 (Save) ] をクリックします。
6. 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. [管理] > [組織] 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、[編集] アイコンをクリックします。
3. 必要に応じて変更を加え、[保存] をクリックします。

### オーガナイゼーションの削除

組織を削除するには、次の手順を実行します。

1. [管理] > [組織] 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、[削除] 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. [管理]>[組織]に移動します。
2. 変更する組織の名前をクリックし、[モニタリングプロファイル (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 \(87 ページ\)](#) 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 [モニタリングのデフォルト値から継承 (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. [保存 (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 \(86 ページ\)](#) 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. [管理]>[組織]に移動します。
2. 変更する組織の名前をクリックし、[ユーザ] 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。



- (注) 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. [管理] > [組織] に移動します。
2. 変更する組織の名前をクリックし、[ユーザ] タブを選択します。
3. テーブル内のユーザの横にある [削除] 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。[組織の詳細] ページの [ネットワーク] 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. [ネットワーク] に移動し、変更するネットワークを選択します。[その他] をクリックして [ネットワークの詳細] パネルを表示します。
2. ネットワーク名の横にある [編集] 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 グループの管理

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。1回の操作で設定できるように、複数のネットワークデバイスが一緒にグループ化されます。

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 ポイントに適用され、スイッチには適用されず、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。

### 新しいデバイス グループの作成

新しいデバイス グループを作成するには、以下の手順を実行します。

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 グループの変更

既存のデバイス グループを変更するには、以下の手順を実行します。

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。



(注) [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

デバイス グループを削除するには、以下の手順を実行します。

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 クレデンシャルの管理

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名 (cisco) 、パスワード (cisco) 、SNMP コミュニティ (public) を使用して、デバイスを認証しようとします。この試みに失敗すると通知が生成され、ユーザが有効なクレデンシャルを指定する必要があります。有効なクレデンシャルを指定するには、以下の手順を実行します。

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。パスワードは必ずプレーンテキストを使用して入力してください。



(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、以下の手順を実行します。

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。保存されているクレデンシャルを削除するには、以下の手順を実行します。

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

[ユーザ管理 (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 ユーザがローカルデータベースに対して認証されるようにします。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を受けることが可能になりました。

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. [管理者] > [ユーザ] に移動し、[ユーザ] 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. [保存 (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、[組織] 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. [管理者] > [ユーザ] に移動し、[ユーザ] 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、[編集] 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. [保存 (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、[組織] 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 [削除] 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. [管理者] > [ユーザ] に移動し、[ユーザ] 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 [削除] 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. [管理者] > [ユーザ] に移動し、[ユーザ設定] タブを選択します。
2. [認証ソース (Authentication Source) ] の [ローカル (Local) ] タブを選択し、必要に応じて [ユーザパスワードの複雑性 (User Password Complexity) ] の設定を変更して、[保存 (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 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、**[管理 (Administration)] > [ユーザ (Users)]** に移動します。[ユーザ設定 (User Settings)] タブを選択し、[認証ソース (Authentication Source)] の **[Azure AD]** タブを選択します。
3. [有効化 (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。[保存 (Save)] をクリックします。
6. [ユーザグループマッピング (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. [有効化 (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、**[システム (System)] > [プラットフォーム設定 (Platform Settings)]** ページの **[システム変数 (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インします。

2. [管理者]>[ユーザ]に移動し、[ユーザ設定]タブを選択します。[認証ソース (Authentication Source) ]で、[ローカル (Local) ]タブを選択します。
3. [有効化 (Enable) ]チェックボックスをオフにして、[保存 (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. [管理者]>[ユーザ]に移動し、[ユーザ設定]タブを選択します。[認証ソース (Authentication Source) ]で、[ローカル (Local) ]タブを選択します。
2. [有効化 (Enable) ]チェックボックスをオンにして、[保存 (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. [管理者]>[ユーザ]に移動し、[ユーザ設定]タブを選択します。
2. 必要に応じて、[ユーザセッション]パラメータを変更し、[保存]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、[モニタリングのデフォルト値 (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. [管理 (Administration) ]>[モニタリングのデフォルト値 (MonitoringDefaults) ]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. [保存 (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 \(78 ページ\)](#) 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、複数の重大度レベル（情報、警告、アラート）があり、ユーザインターフェイスのポップアップメッセージと電子メール通知を生成できます。アクティブな通知は[通知センター (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[イベントログ (Event Log)]に記録されます。



- (注) 電子メール通知を使用する場合は、電子メールの設定が適切に行われていることを確認する必要があります。詳細については、「[電子メール設定の管理](#)」を参照してください。

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

複数のモニタリングプロファイルを作成し、システムレベルで、または組織ごとに、異なるデバイスタイプに異なるプロファイルを割り当てることができます。プロファイルへのテンプレートの割り当てに関する詳細については、[組織の管理 \(78 ページ\)](#) と [モニタリングのデフォルト値の変更 \(86 ページ\)](#) 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. [管理 (Administration)] > [モニタリングプロファイル (Monitoring Profiles)] に移動します。
2. [+] (プラス) アイコンをクリックして新しいプロファイルを作成します。

3. プロファイルの名前と、プロファイルを関連付ける組織を指定します。ここで [すべての組織 (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なり、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. [保存 (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、[編集 (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. [管理 (Administration)] > [モニタリングプロファイル (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、[名前を付けて保存 (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、[保存 (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。[デフォルトにリセットする (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. [管理 (Administration)] > [モニタリングプロファイル (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、[編集 (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、[保存 (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。[デフォルトにリセットする (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. [管理 (Administration) ] > [モニタリングプロファイル (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、[削除 (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 [管理 (Administration) ] > [モニタリングのデフォルト値 (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ログアウトのすべての試行の成功と失敗の両方のログを保持します。ログを表示するには、[管理] > [ログイン試行] 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 23: ログイン試行テーブル

フィールド	説明
ユーザ名	イベントに関連付けられているユーザ名。
[表示名 (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 タイプ (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。
ステータス (Status)	試行が成功したか失敗したかを示します。
タイムスタンプ	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

[レポート設定] 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

# システム

---

この章は、次の項で構成されています。

- [システムについて](#) (91 ページ)
- [ライセンスの管理](#) (92 ページ)
- [証明書の管理](#) (94 ページ)
- [電子メール設定の管理](#) (97 ページ)
- [API 使用状況の表示](#) (98 ページ)
- [Dashboard 設定のバックアップと復元](#) (99 ページ)
- [プラットフォーム設定の管理](#) (100 ページ)
- [プライバシーの管理](#) (102 ページ)
- [ログ設定の管理](#) (105 ページ)
- [ローカル Probe の管理](#) (107 ページ)

## システムについて

Cisco Business ダッシュボードの [システム] 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。

- [ライセンス (License) ] : Dashboard のソフトウェアライセンスを管理します。
- [証明書 (Certificate) ] : Dashboard のセキュリティ証明書を管理します。
- [電子メールの設定] : 電子メールをセットアップします。
- [API の使用状況] : Cisco Business ダッシュボード API の使用状況を監視します。
- [バックアップ (Backup) ] : Dashboard 用の設定とその他のデータをバックアップします。
- [復元 (Restore) ] : Dashboard 用の設定とその他データを復元します。
- [プラットフォーム設定 (Platform Settings) ] : Dashboard のネットワーク設定を管理します。
- [プライバシー設定] : シスコと共有できるデータを制御します。

- [ログ設定 (Log Settings)] : Dashboard のログ設定を変更します。
- [ローカルProbe (Local Probe)] : Dashboard にホストされた Probe 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。

[ライセンス (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。

- [スマート ソフトウェア ライセンシングの状況] : 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。
- [スマートライセンスの使用状況] : このパネルには、ネットワークの現在の状態に基づいて、必要なライセンスの数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。[ステータス] 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 インターフェイスに移動し、[システム] > [ライセンス] を選択します。
6. [レジスタ] 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 インターフェイスに移動し、[システム] > [ライセンス] を選択します。
2. 右上にあるドロップダウンリストから [登録解除...] を選択します。ポップアップで [登録解除] をクリックして確定します。

#### ライセンスをただちに確認

Cisco Business ダッシュボード 毎日チェックを実行して、ネットワークに対して使用できる十分なライセンスがその時点で存在するかどうか確認し、必要なライセンスの数が減少している場合にはただちに更新を行います。ただし、必要なライセンスの数が増加している場合、またはプールに対してライセンスが追加または削除された場合、Dashboard が更新されるまでに最大で 1 日かかる場合があります。Dashboard 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 インターフェイスに移動し、[システム] > [ライセンス] を選択します。
2. 右上のドロップダウンリストから [ライセンスを再確認しています... (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

[登録をただちに更新 (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ダッシュボードインターフェイスに移動し、[システム]>[ライセンス] を選択します。
2. 右上にあるドロップダウン リストから [許可をただちに更新] を選択します。

### 登録を今すぐ更新

[登録をただちに更新] 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ダッシュボードインターフェイスに移動し、[システム]>[ライセンス] を選択します。
2. 右上にあるドロップダウン リストから [登録をただちに更新...] 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ダッシュボードインターフェイスに移動し、[システム]>[ライセンス] を選択します。
2. 右上にあるドロップダウン リストから [再登録] 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、[この製品インスタンスが登録済みの場合は、再登録します (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プライベート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. [システム] > [証明書] 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. [作成] 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 [ダウンロード] 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. [システム] > [証明書] に移動し、[証明書の更新] タブを選択します。
2. [証明書のアップロード] 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 [PKCS12 のアップロード] 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. [アップロード] 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一方で、他のブラウザでは警告なしに証明書が受け入れられることがあります。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. [システム]>[証明書]に移動し、[証明書の更新]タブを選択します。
2. [自己署名証明書の更新]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、証明書の構築に使用されます。
3. [保存 (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. [システム]>[証明書]に移動し、[現在の証明書]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. [システム]>[証明書]に移動し、[現在の証明書]タブを選択します。
2. ページ下部にある[ダウンロード (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。コマンドにリスト



されているすべての名前は、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 \(100ページ\)](#) 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。このページでは、以下のパラメータを設定できます。

表 24: 電子メール設定

フィールド	説明
SMTPサーバ	使用する SMTP サーバ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。 オプションには、次のものが含まれます。 <ul style="list-style-type: none"> <li>• なし</li> <li>• TLS</li> <li>• SSL</li> </ul>
認証	電子メール認証を有効または無効にします。
ユーザ名	認証が有効な場合に提示するユーザ名。
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す。

## API 使用状況の表示

[APIの使用状況] 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分間の要求モニタ]：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。
- [要求履歴] 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クライアント情報] 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クライアント情報] テーブルに表示される情報について説明します。

表 25: APIクライアント情報テーブル

フィールド	説明
APIバージョン	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。
クライアント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。
クライアントモジュール	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。
クライアントバージョン	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。
ユーザ名	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、キーに関連付けられているユーザ名が表示されます。
最後にアクセスしてからの時間	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。

フィールド	説明
登録されたネットワークの数	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。
登録されたライセンス済みデバイスの数	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クライアント情報] テーブルにあるクライアントの [#登録済みネットワーク] 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 [登録済みネットワーク] テーブルが表示されます。次のテーブルに、[登録済みネットワーク] テーブルに表示される情報について説明します。

表 26: [登録済みネットワーク] テーブル

フィールド	説明
ネットワーク	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。
登録されたライセンス済みデバイスの数	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。

バックアップを実行するには、次の手順に従います。

1. [システム] > [バックアップ] 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、[パスワード] および [パスワードの確認] フィールドに入力します。
3. [バックアップとダウンロード] 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 [ステータスの表示] 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. [システム]>[復元]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、[パスワード]フィールドに入力します。
3. [アップロードと復元]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上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。[復元]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

[プラットフォーム設定 (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、[ネットワーク設定 (Network Settings)]、[Webサーバ (Web Server)]、[システム変数 (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 ([ネットワーク設定 (Network Settings)] タブ)



(注) これは、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前で、Bonjourアドバタイズメントを生成する際、Cisco BusinessダッシュボードがDashboardを特定するために使用されます。Dashboardのホスト名を変更するには、次の手順を実行します。

1. [システム (System)]>[プラットフォーム設定 (System Platform Settings)]に移動し、[ネットワーク設定 (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. [保存 (Save)] をクリックします。

### ネットワーク設定の変更 ([ネットワーク設定 (Network Settings)] タブ)



(注) これは、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. [システム (System)] > [プラットフォーム設定 (System Platform Settings)] に移動し、[ネットワーク設定 (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 [静的 IP] です。[静的 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. [保存 (Save)] をクリックします。

#### 時刻設定の変更 ([ネットワーク設定 (Network Settings)] タブ)

[時刻設定 (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. [システム (System)] > [プラットフォーム設定 (System Platform Settings)] に移動し、[ネットワーク設定 (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。

[ローカルクロック] 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、[クロック] をクリックして、PC の時刻と同期させます。

4. [保存 (Save)] をクリックします。

#### ポート設定の変更 ([Webサーバ (Web Server)] タブ)

[ポート設定 (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. [システム (System)] > [プラットフォーム設定 (System Platform Settings)] に移動し、[Webサーバ (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. [保存 (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、[プラットフォーム設定] 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サーバ (Web Server)] タブ)

[アクセス制御 (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. [システム (System)] > [プラットフォーム設定 (System Platform Settings)] に移動し、[Webサーバ (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. [保存 (Save)] をクリックします。

### システム変数の管理 ([システム変数 (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. [システム (System)] > [プラットフォーム設定 (System Platform Settings)] に移動し、[システム変数 (System Variables)] タブを選択します。
2. 必要に応じて、[外部システム設定 (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. [保存 (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。提供されるサービスには次のものがあります。

- **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せん。この機能は、デフォルトで無効にされています。

- **ライフサイクル レポート**：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。
- **ソフトウェアの更新**：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。
- **製品の改善**：この機能により、Cisco Businessダッシュボードは、シスコの製品ポートフォリオをさらに発展させる目的で、ネットワーク内のハードウェアとソフトウェアの使用状況に関する情報を送信できます。製品の改善はデフォルトで有効になっています。

これらの機能はすべて**シスコのプライバシー ポリシー**の対象であり、いつでも有効または無効にすることができます。[プライバシー設定 (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. [ネットワーク] ページに移動し、表示するネットワークを選択します。
2. [ネットワーク アクション] ドロップダウンから [CAA にアップロード] を選択します。
3. プロンプトが表示された場合は、[cisco.com](https://www.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. [アップロード (Upload)] をクリックします。また、[送信前にインベントリ データを表示] 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](https://www.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. [ネットワーク] ページに移動してネットワークを選択し、[その他] 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. [新たに検出されたデバイスを自動的にアップロード] 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. [保存 (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. [ネットワーク] ページに移動してネットワークを選択し、[その他] をクリックします。次に、[CAA] タブを選択します。
2. [新たに検出されたデバイスを自動的にアップロード] チェックボックスをオフにします。
3. [保存 (Save) ] をクリックします。

### ライフサイクルレポート

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. [システム] > [プライバシー設定] 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. [保存 (Save) ] をクリックします。

### 製品向上

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. [システム] > [プライバシー設定] に移動します。
2. [シスコに製品改善データを送信する] チェックボックスの横にある [サンプルの表示] リンクをクリックする。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. [システム] > [プライバシー設定] に移動します。
2. [シスコに製品改善データを送信する] チェック ボックスをオフにします。



3. [保存 (Save) ]をクリックします。

#### ソフトウェアアップデート

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. [システム]>[プライバシー設定]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. [保存 (Save) ]をクリックします。

## ログ設定の管理

[ログ設定の管理] 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[情報]ですが、[警告]または[エラー]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[デバッグ]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. [システム]>[ログ設定]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. [保存 (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。[ログ ファイルのダウンロード]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. [システム]>[ローカル プローブ]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. [保存 (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。





## 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 \(109 ページ\)](#)
- [サポートされる通知 \(109 ページ\)](#)
- [現在のデバイスの通知の表示とフィルタリング \(111 ページ\)](#)
- [デバイスの履歴通知の表示とフィルタリング \(112 ページ\)](#)

## 通知について

Cisco Businessダッシュボード 各種のイベントがネットワーク内で発生した場合に通知を生成します。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。また、関心がなくなった通知は確認済みに設定でき、それらの通知はデフォルトで[通知センター]に表示されなくなります。

## サポートされる通知

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

表 27: 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
<b>デバイス通知</b>			
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)

イベント	レベル	説明	自動的にクリアされるか
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 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)
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)
<b>シスコ サポート通知</b>			
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 <a href="http://cisco.com">cisco.com</a> 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)
<b>デバイスの健全性通知</b>			
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)

イベント	レベル	説明	自動的にクリアされるか
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、[通知センター] 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。

- 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）

2. [通知センター] 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、[すべて応答] 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。

3. [フィルタ] ボックスは、テーブルに表示される通知を制限します。デフォルトでは、すべてのタイプとすべての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、[フィルタの追加] 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 28: 使用可能なフィルタ

フィルタ	説明
通知タイプ	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[オフラインのデバイス]を選択します。

フィルタ	説明
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"> <li>• 情報</li> <li>• 警告</li> <li>• アラート</li> </ul> <p>[高く]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。
ネットワーク	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。
[デバイス (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 [基本情報] 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 \(86ページ\)](#)」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、個々のデバイスの [基本情報] パネルまたは [デバイスの詳細] パネルに表示できます。[基本情報 (Basic Info)] パネルには、過去 24 時間のイベントのみが表示され、[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。[デバイスの詳細] パネルのイベントは、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

# 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](#) (113 ページ)
- [プローブのログ設定の管理](#) (114 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. [ネットワーク] 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。[アクション] タブを選択し、[Show Tech] をクリックします。  
  
または、プローブの UI にログオンし、[トラブルシューティング] > [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

プローブから **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。

## プローブのログ設定の管理

Probe の [ログ設定 (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、プローブがそのログ 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、[ネットワーク] に移動し、設定を変更するネットワークを選択します。[その他] をクリックして [ネットワークの詳細] パネルを表示し、[ログ設定] タブを選択します。または、プローブ UI にログオンし、**管理 > ログ設定** 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 29: ログ設定

フィールド	説明
ログレベル	<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"> <li>• [エラー] : エラー レベルのメッセージのみ</li> <li>• [警告] : 警告とエラー</li> <li>• [Info] (デフォルト) : 情報メッセージ以上</li> <li>• [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</li> </ul>

フィールド	説明
ログモジュール	<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"> <li>• [すべて] (デフォルト) :すべてのモジュール</li> <li>• [Call Homeエージェント (Call-home Agent) ] : Probe と Dashboard 間の通信</li> <li>• [ディスカバリ] : デバイス検出イベントとトポロジ検出</li> <li>• [ノースバウンド (Northbound) ] : Dashboard と Probe 間の通信</li> <li>• [サービス] : ノースバウンドとサウスバウンド間のメッセージ変換</li> <li>• [サウスバウンド] : プロブとデバイス間の低レベル通信</li> <li>• [システム] : 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</li> </ul> <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 \(113 ページ\)](#) を参照してください。





## 第 15 章

### よくある質問

---

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 \(FAQ\) \(117 ページ\)](#)
- [検出の FAQ \(118 ページ\)](#)
- [設定の FAQ \(119 ページ\)](#)
- [セキュリティ上の留意事項の FAQ \(119 ページ\)](#)
- [リモートアクセスの FAQ \(122 ページ\)](#)
- [ソフトウェアアップデートの FAQ \(123 ページ\)](#)

### 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 サーバと SNMP サーバの存在の有無もテストします。

## 設定の FAQ

- Q. 新しいデバイスが検出されると何が起こりますか。その設定は変更されますか。
- A. 新しいデバイスはデフォルト デバイス グループに追加されます。デフォルト デバイス グループに設定プロファイルが割り当てられている場合は、その設定が新たに検出されたデバイスに適用されます。
- Q. デバイスのあるデバイス 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 30: 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 (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。
TCP 50000 ~ 51000	インバウンド	HTTPS	デバイスへのリモートアクセス。

ポート	方向	プロトコル	利用方法
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 をアダプタイズする、ローカルネットワークへのマルチキャスト DNS サービスアダプタイズメント。

- 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 31 : 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 (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。
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 サービスアダプ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。



ポート	方向	プロトコル	利用方法
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の証明書で認証された TLS 1.2 セッションを使用して暗号化されています。セッションは Probe から Dashboard に対して開始されます。Dashboard と Probe 間の関連付けを最初に確立する際、ユーザは Probe 経由で Dashboard にログインする必要があります。
- Q.** Cisco Businessダッシュボードはデバイスに「バックドア」アクセスできますか。
- A.** いいえ。Cisco Businessダッシュボードは、サポートされているシスコデバイスを検出すると、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クレデンシャルは、AES-128アルゴリズムを使用して不可逆的に暗号化されます。

- Q. Web UI 用のパスワードをなくした場合、どのようにすれば回復できますか。
- A. Web UI のすべての admin アカウントのパスワードをなくした場合は、Probe のコンソールにログインして **cbdprobe recoverpassword** ツールを実行するか、Dashboard のコンソールにログインして **cisco-business-dashboard recoverpassword** ツールを実行することで、パスワードを回復できます。このツールは、cisco アカウントのパスワードをデフォルトの cisco にリセットします。cisco アカウントが削除されている場合は、デフォルトのアカウントを使用してアカウントを作成します。以下に、このツールを使用してパスワードを回復するために実行するコマンドの例を示します。

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword Cisco Business Dashboard successful!
cisco@cisco-buisness-dashboard:~$
```



(注) Cisco Businessダッシュボード for AWS を使用する場合、パスワードには 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クレデンシャルの場合、ユーザ名は **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（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。



## 第 16 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（125 ページ）](#)
- [設定構文（125 ページ）](#)
- [設定テンプレートの作成（128 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コンフィギュレーションファイルと、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時に設定テンプレートとマージされます。つまり、デバイスがマネージャに接続する前にシステム変数が変更された場合、最終的なデバイス設定はプレビューに表示されるものと異なる場合があります。

設定は、Mustache のテンプレート (<https://mustache.github.io/>) として作成されます。Mustache を使用すると、次のような、Mustache ドキュメントでタグと呼ばれるさまざまなプレースホルダを使用できます。

- 単純な変数。プレースホルダは、デバイスレコードで指定された値に置き換えられます。単純な変数の形式は `{{name}}` です。
- セクション。プレースホルダで設定のブロック（必要な場合は他のプレースホルダも含む）を囲みます。セクションの内容は、最終的な設定から除外するか、1回だけ含めるか、あるいは複数回繰り返すことができます。このタイプのプレースホルダの動作は、テンプレート内のメタデータと、デバイスレコードを作成するときにユーザ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、このコンテナの内容のコピーがデバイス設定で作成されます。
- `{{vlan-id}}` と `{{vlan-name}}` はどちらも単純な変数であり、`{{#vlans}}` リスト内に含まれています。デバイスレコードが作成されると、`{{vlan id}}` と `{{vlan name}}` に複数の値を指定できます。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。

- [必須 (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。
- [タイプ (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。
- [タイトル (Title) ]。これは、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る場合があります。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。
- [編集 (Edit) ] アイコン。特定のタイプでは、プレゼンテーションの制御に使用できる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。その場合に、入力したテキストの形式が正しくないと、入力フォームにエラーが表示されます。さらに、特定のタイプは、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。
- [上/下に移動 (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もあり、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をユーザにどのように表示するか例を示すために使用できます。

## 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。

- [文字列 (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。
- [整数 (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。

- [ブール (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まれます。
- [コンテナ (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。
- [リスト (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追加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、[編集 (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 ([列挙型 (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。入力するコンテンツが多量とな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 \(100 ページ\)](#)」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、[名前を付けて保存 (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するとともに、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. [ネットワーク プラグアンドプレイ (Network Plug and Play)] > [設定 (Configurations)] に移動してテンプレートエディタで設定を選択し、[編集 (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コンフィギュレーションファイルが示されます。テキストエディタでは、検索、置換、およびいくつかのカーソル操作のキーシーケンスを含む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 32: 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。[プレビュー (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. デバイス間で異なるすべての設定パラメータに対してプレースホルダを作成するまで、ステップ 2 と 3 を繰り返します。
5. 作成したテンプレートに問題がなければ、[保存 (Save)] をクリックします。



(注) テンプレートが保存されるたびに、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、それらの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 32: 一般的なエディタコマンド

機能	説明	キーのバインド	
		PC	Mac
すべてを選択	エディタの内容全体を選択します	Ctrl+A	Cmd+A

機能	説明	キーのバインド	
		PC	Mac
キルライン	行のカーソルの後の部分を削除します。これが空白だけ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
品目の削除	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
元に戻す	最後の変更を元に戻します。	Ctrl+Z	Cmd+Z
やり直し	最後に元に戻した変更をやり直します。	Ctrl+Y	Shift+Cmd+Z Cmd+Y
ドキュメントの先頭に移動	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
ドキュメントの末尾に移動	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+↓
行の先頭に移動	カーソルを行の先頭に移動します。	Alt+←	Ctrl+A
行の末尾に移動	カーソルを行の末尾に移動します。	Alt+→	Ctrl+E
さらにインデント	現在の行または選択項目をインデントします。	Ctrl-]	Cmd+]
インデントを少なくする	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+[
検索		Ctrl+F	Cmd+F
Find Next		Ctrl+G	Cmd+G
前を検索		Shift+Ctrl+G	Shift+Cmd+G
置換		Shift+Ctrl+F	Cmd+Alt+F
Replace All		Shift+Ctrl+R	Shift+Cmd+Alt+F