Cisco Business ダッシュボードおよび Probe クイックスタートガイド

初版：2020 年 7 月 13 日

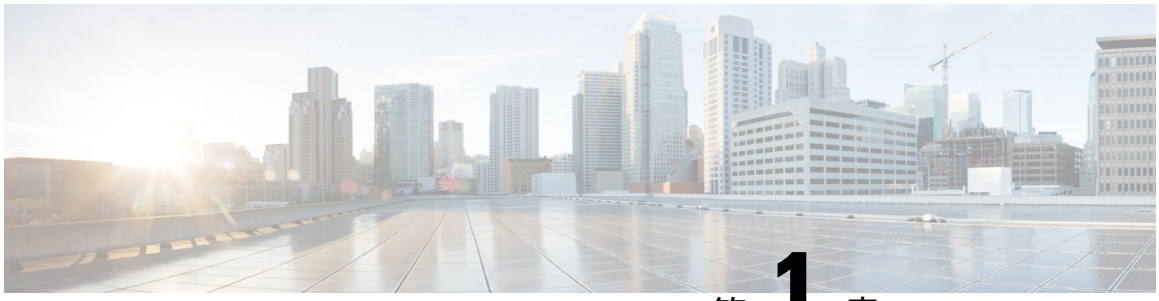
最終更新：2021 年 10 月 6 日

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

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

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

目 次



第 1 章

Cisco Business Dashboard の概要

この章は、次の項で構成されています。

About Cisco Business ダッシュボード

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

Cisco Business ダッシュボードプローブ のインスタンスは、ネットワークの各サイトにインストールされ、Dashboard に関連付けられます。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、Probe を介在させずに管理されます。この方法でネットワークデバイスが直接管理されている場合、デバイスに対するすべての管理機能を使用できますが、ネットワーク検出プロセスは、Probe を介在させる場合と比較して検索範囲が狭くなることがあります。

対象読者

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

関連資料

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

- **クイックスタートガイド（本書）**：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。
- **インストールガイド**

  次の表に、さまざまなプラットフォームに展開できる Dashboard ソフトウェアのすべてのインストールガイドを示します。詳細については、場所列に記載されているパスを参照してください。

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

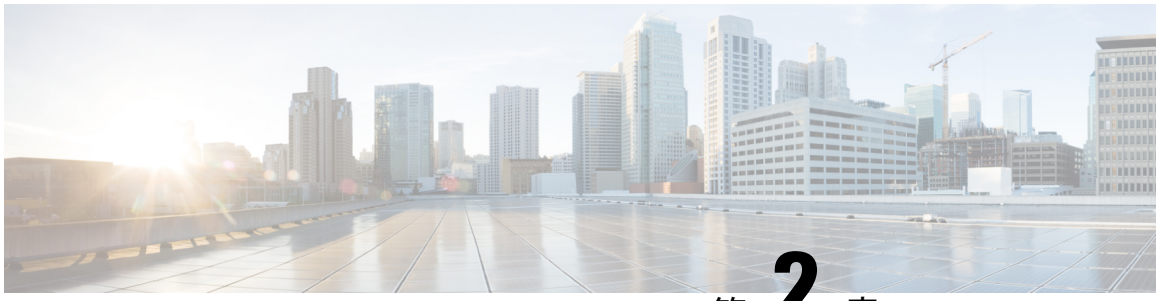
- **アドミニストレーションガイド**：このソフトウェアが提供するすべての機能とオプションに関する詳細およびそれらの設定方法と使用方法を示すリファレンスガイドです。『Cisco Business Dashboard Administration Guide』を参照してください。
- **デバイスサポートリスト**：このリストには、Cisco Business ダッシュボード でサポートされるデバイスの詳細と、各デバイスタイプで利用可能な機能が記載されています。Cisco

Businessダッシュボードでサポートされるすべてのデバイスのリストについては、『Cisco Business Dashboard - Device Support List』を参照してください。

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。 • 記述子ファイル（.OVF） • Manifest（.MF）および証明書ファイル（任意）
Raspberry Pi	Raspberry Pi財団によって開発された、極めて低コストのシングルボードコンピュータ。詳細については、*https://www.raspberrypi.org/* [英語] を参照してください。
Raspberry Pi OS	正式にはRaspbianとして知られるRaspberry Pi OSは、Raspberry Pi用に最適化された、Debianベースの Linuxディストリビューションです。詳細については、*https://www.raspberrypi.org/software/* [英語] を参照してください。
VirtualBox	Oracle Corporationによって提供されている仮想化プラットフォーム。
Virtual Hard Disk（VHD）	ハード ドライブの完全な内容を格納するためのディスクイメージ ファイル形式。
仮想マシン（VM）	ゲスト オペレーティング システムと関連するアプリケーション ソフトウェアが動作可能な、仮想コンピューティング環境。同一のホスト システム上で同時に複数の VMを実行できます。

用語	説明
• VMware ESXi • VMware Fusion • vSphere Server • VMware Workstation	VMware Inc. によって提供されている仮想化プラットフォーム。
vSphere クライアント	vCenter Server または ESXi に任意の Windows PC からリモートで接続できるようにするためのユーザーインターフェイス。vSphere Client のプライマリ インターフェイスを使用して、VM、そのリソース、およびホストの作成、管理、およびモニタ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。



第 2 章

Dashboard の初期セットアップの実行

この章は、次の項で構成されています。

Dashboard の初期セットアップの実行

Dashboard が要件を満たすようにするには、いくつかの設定作業を実行する必要があります。

VM イメージまたは AWS インスタンスでの基本的なシステム設定

Dashboard の IP アドレスや時刻設定など、基本的なシステム設定を行うには、以下の手順に従います。

1. SSH を使用して AWS インスタンスに接続するか、仮想マシンを使用している場合はハイパーバイザに適したツールを使用して、Dashboard のコンソールに接続します。
2. 仮想マシンを使用している場合は、デフォルトのユーザー名とパスワード（cisco）を使用してログインします。AWS インスタンスの場合は、インスタンスを作成したときに指定したキー ペアおよびユーザー名（cisco）を使用します。

   シスコアカウントのパスワードは、ログイン後すぐに変更する必要があります。新しいパスワードは、文字種が混在した、辞書に載っていない単語を使用した複雑なものする必要があります。
3. 初期設定を行うには、コマンド `sudo config_vm` を入力します。プロンプトが表示されたら、cisco アカウント用のパスワードを入力します。`config_vm` ユーティリティは、プラットフォーム設定を変更するための一連の手順を表示します。
4. まず、Dashboard のホスト名を変更するよう求められます。ホスト名は、ネットワークで Dashboard を識別するために使用されます。ここで意味のある名前を選択するか、この手順をスキップしてデフォルトのホスト名のままにすることができます。

（注） この手順は、Cisco Business ダッシュボード for AWS では実行できません。

Dashboard の初期セットアップの実行

5. 次に、Web サーバーポートを変更するように求められます。ポートがデフォルト値から変更された場合は、ネットワークのファイアウォール設定を変更したり、AWS のセキュリティグループ設定を変更したりすることが必要になる場合もあります。
6. 次に、ネットワークインターフェイスを設定するよう求められます。ここでのオプションは static と dhcp（デフォルト）です。static を選択すると、IP アドレス情報、デフォルトゲートウェイ、DNS サーバーアドレスの入力を求められます。ここで変更を行うとネットワーク インターフェイスがリセットされます。

（注） この手順は、Cisco Business ダッシュボード for AWS では実行できません。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。

7. 次に、Dashboard の時刻を設定するよう求められます。時刻同期用の 1 台以上の NTP サーバーを設定することを選択でき（推奨）、タイムゾーンを選択するよう求められます。

（注） 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。

8. 最後に、ブートローダーのパスワードを変更するかどうかを確認するメッセージが表示されます。ブートローダーのユーザー名とパスワードは、システムのブートプロセスを変更するか、失われたオペレーティングシステムのパスワードを回復するために、システムの起動時にコンソールで使用されることもあります。ブートローダーのデフォルトのログイン情報の場合、ユーザー名は **root**、パスワードは **cisco** です。

これらの設定はいつでも変更できます。変更するには、スクリプトを再度実行するか、Web インターフェイスの **[System]** > **[Platform Settings]** を使用します。

Dashboard ユーザーインターフェイスの起動

1. **Google Chrome** や **Microsoft Edge** などの Web ブラウザを起動します。
2. [Address] フィールドに Dashboard の IP アドレスまたはホスト名を入力して **Enter** キーを押します。
3. デフォルトのユーザー名とパスワード（`cisco/cisco`）を入力します。Cisco Business ダッシュボード for AWS を使用している場合、デフォルトのパスワードはインスタンス ID です。インスタンス ID は AWS EC2 コンソールで確認できます。
4. [Login] をクリックします。シスコアカウントのユーザー名とパスワードを変更するよう求められます。新しいパスワードは、長さが 8 文字以上で、3 種類以上の文字クラスを使用している必要があります。
5. [Next] をクリックします。Cisco Business ダッシュボードでどのようにデータが使用されるか、どの情報がシスコと共有されるかに関する情報が表示されます。必要に応じて変更を行い、[Finish] をクリックします。

Cisco Business ダッシュボード ユーザーインターフェイスが表示されます。

組織の作成（オプション）

組織は、ネットワーク、ユーザー、およびデバイスを、通常は個別に管理するグループに分割するために Cisco Business ダッシュボード で使用されます。各ネットワークまたはデバイスは 1 つの組織に属し、各ユーザーは 1 つ以上の組織を管理できます。組織は、顧客、部門、地域などを表す場合がありますが、組織を使用すると、ネットワークのさまざまな部分を管理できるユーザーをより細かく制御できます。Dashboard 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。

新しい組織を作成するには、次の手順を実行します。

1. **[Administration]** > **[Organizations]** に移動します。
2. テーブルの上部にある [+]（プラス）アイコンをクリックします。
3. 組織の名前を指定し、必要な詳細情報を入力します。
4. 新たに検出されたデバイスのデフォルトグループとして使用する必要がある新しいデバイスグループの名前を入力します。新しいデバイスグループが組織とともに作成されます。
5. [Save（保存）] をクリックします。
6. 作成する組織ごとに 1 ～ 5 の手順を繰り返します。

ユーザーの作成とパスワードの変更

初期状態の Dashboard には、単一のデフォルトユーザー名とパスワードが設定されています。

新しいユーザーを追加するには、以下の手順を実行します。

1. **[Administration]** > **[Users]** に移動します。
2. [Users] 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. 表示される [Add user] ウィンドウで、作成するユーザーの詳細情報を入力します。このユーザーが、管理者、組織管理者、オペレータ、読み取り専用ユーザーのいずれであるかを指定します。次に、ユーザーのタイプに応じて付与される権限を示します。
   - 管理者：システム管理を含むすべての機能にアクセスできます。
   - 組織管理者：1 つまたは複数の組織の機能すべてにアクセスできますが、[System] メニューにアクセスすることはできません。
   - オペレータ：割り当てられた組織内のすべての機能にアクセスできますが、ユーザーを管理することはできません。[System] メニューにアクセスすることもできません。
   - 読み取り専用ユーザー：設定は一切変更できず、[Administration] メニューへの制限付きアクセスのみが認められています。[System] メニューにはアクセスできません。
4. [Save] をクリックして新しいユーザーを作成します。

Dashboard の初期セットアップの実行

[Users] ページの [User Settings] タブで、パスワードの複雑度についての制限を設定することもできます。新しいパスワードはこれらの制限を満たす必要があります。

パスワードを変更するには、以下の手順を実行します。

1. ユーザーインターフェイスの右上で自分のユーザー名をクリックして、[My Profile] ドロップダウンメニューを表示します。ページが表示されます。
2. [Reset password] リンクをクリックします。
3. 表示されるボックスに、現在のパスワードと新しいパスワードを入力します。
4. [**Save**] をクリックします。

ライセンスの設定

（注） この手順は Cisco Business ダッシュボード for AWS の従量制課金版には適用されません。

Cisco Business ダッシュボードには Cisco Smart Licensing を使用するためのライセンスが付与されています。初回インストール時、Dashboard は評価モードに設定されます。評価モードでは、最大 10 個のネットワーク デバイスを制限なしで管理でき、10 を超えるデバイスを管理する場合には 90 日以内にライセンスを取得できます。購入したライセンスをシステムに適用するには、ネットワークに関する十分なデバイスライセンスが含まれる Cisco スマートアカウントに Dashboard を関連付ける必要があります。

Dashboard をスマートアカウントに関連付けるには、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…] をクリックして、新しい製品インスタンス登録トークンを作成します。オプションで、説明を追加し、[Expire After] の時間を変更します。[Create Token] をクリックします。
4. トークンの右にある [Actions] ドロップダウンから [Copy] を選択して、新しく作成したトークンをクリップボードにコピーします。
5. Cisco Business ダッシュボード ユーザーインターフェイスに移動し、**[Administration]** > **[License]** を選択します。
6. [レジスタ] をクリックし、表示されるフィールドにトークンを貼り付けます。[OK] をクリックします。

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

Dashboard の初期セットアップの実行

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。ライセンス付与プロセスの詳細については、『Cisco Business Dashboard Administration Guide』の「*Managing Licenses*」を参照してください。

VM イメージでの組み込み Probe の無効化

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

Dashboard の仮想マシンイメージには、Dashboard に対してローカルなネットワーク上のデバイスを管理するための Probe ソフトウェアが含まれます。ローカル ネットワークを管理しない場合、次の手順を使用して組み込み Probe を無効にすることができます。

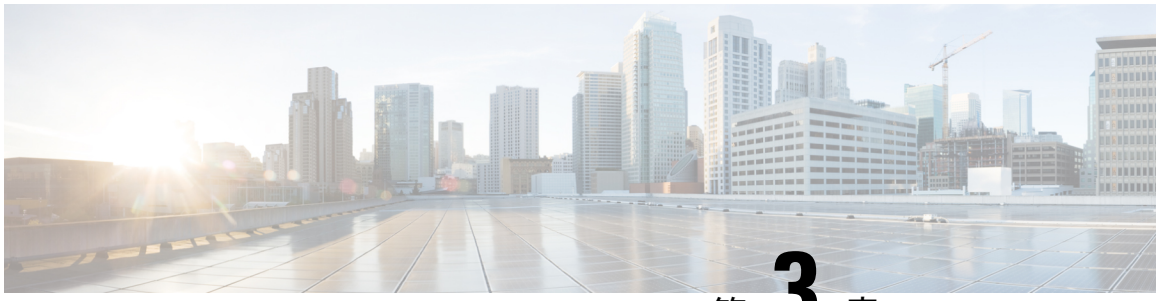
1. **[System]** > **[Local Probe]** に移動します。
2. トグル スイッチをクリックして組み込み Probe を無効にします。
3. [**Save**] をクリックします。

ネットワークの作成（オプション）

後で関連付ける Probe について、Dashboard のネットワークレコードを事前定義することができます。通常、各ネットワークは個別のサイトを表しますが、同じ場所に複数のネットワークを配置することもできます。新しいネットワークを作成するには、次の手順を実行します。

1. [Network] に移動します。
2. [Map View] で [Add Network] をクリックするか、[List View] で [+]（プラス）アイコンをクリックします。
3. ネットワークの名前、組織、デフォルトのデバイスグループを指定します。
4. 該当するフィールドにネットワークのアドレスを入力します。部分的な住所を入力すると、考えられる一致の一覧が表示され、リストから場所を選択できます。また、マップで場所をクリックすることもできます。
5. [**Save**] をクリックします。
6. 作成するネットワークごとに 1 ～ 5 の手順を繰り返します。

Dashboard の初期セットアップの実行



第 3 章

Probe の初期セットアップの実行

この章は、次の項で構成されています。

Probe の初期セットアップの実行

Probe が要件を満たすようにするには、いくつかの設定作業を実行する必要があります。

Probe の IP アドレスの特定

Probe で使用されている IP アドレスを見つけるには、次のいずれかの方法を使用します。

1. Probe のデフォルト IP アドレスの設定は、DHCP を使用して行います。DHCP サーバーが稼働しており、到達可能であることを確認します。使用できる DHCP サーバーがない場合、IP アドレスはデフォルトで 192.168.1.10 になります。
2. コンピュータと同じローカル ネットワーク セグメント内のすべてのサポートされるシスコ デバイスを自動的に検出できる **Cisco FindIT Network Discovery Utility** を使用して Probe を検出およびアクセスできます。各デバイスのスナップショットを表示することや、製品のコンフィギュレーションユーティリティを起動して設定値を表示および指定することができます。詳細については、http://www.cisco.com/go/finditを参照してください。
3. Probe は Bonjour 対応であり、Bonjour プロトコルを使用して自身を自動的にアドバタイズします。Bonjour 対応のブラウザがある場合は、IP アドレスが不明でも、ローカルネットワーク上の Probe を検索できます。
4. 仮想マシン イメージを使用している場合、Probe の IP アドレスは、仮想マシン コンソールから取得できます。ハイパーバイザの管理ツールを使用して仮想マシンのコンソールに接続し、デフォルトのユーザー名/パスワード（cisco/cisco）を使用してログインします。パスワードは、ログインしてすぐに変更する必要があります。新しいパスワードには、複雑で、文字種が混在した、辞書に載っていない単語を使用する必要があります。現在の IP アドレスを示すバナーが表示されます。

   独自の Ubuntu または Raspbian Linux 環境に Probe をインストールしている場合、オペレーティングシステムのツールを使用して IP アドレスを検出することができます。たとえば、

Probe の初期セットアップの実行

シェル プロンプトにコマンド ifconfig を入力し、表示されるインターフェイスとそのアドレスのリストを表示することができます。

（注） ここで設定されたログイン情報は、Probe が Dashboard にアクティブに接続されていない場合に Probe にログオンするために使用されます。Dashboard に接続されている場合は、Dashboard へのログオンに使用したのと同じログイン情報を使用して Probe にアクセスする必要があります。

5. ルータまたは DHCP サーバーにアクセスして、DHCP サーバーによって割り当てられた IP アドレスを検索します。詳細については、DHCP サーバーの取り扱い説明書を参照してください。

ソフトウェア Probe のセットアップ

ソフトウェア Probe は、同じ VM またはホストで実行されている Dashboard がない場合に、仮想マシンまたは Linux ホストで実行される Probe です。

ソフトウェア Probe をセットアップするには、次の手順を実行します。

1. **Google Chrome** や **Microsoft Edge** などの Web ブラウザを起動します。
2. [Address] フィールドに DHCP によって割り当てられた IP アドレスを入力し、[Enter] をクリックします。
3. デフォルトのユーザー名とパスワード（cisco/cisco）を入力します。[Login] をクリックします。
4. シスコアカウントのユーザー名とパスワードを変更するよう求められます。新しいパスワードは、長さが 8 文字以上で、3 種類以上の異なる文字クラスを使用する必要があります。[**Save**] をクリックします。
5. 接続先の Dashboard のアドレスまたはホスト名を指定し、[Next] をクリックします。
6. ブラウザが Dashboard のログイン画面にリダイレクトされます。Dashboard の管理者のログイン情報を使用してログインすると、ブラウザが元の Probe にリダイレクトされます。
7. 新しいネットワークを作成するか、表示されたドロップダウンから既存のネットワークを選択するかを選択します。新しいネットワークを作成することを選択した場合は、表示されたボックスにネットワークの名前と場所を入力します。

   該当するフィールドにネットワークのアドレスを入力します。部分的な住所を入力すると、考えられる一致の一覧が表示され、リストから場所を選択できます。また、マップで場所をクリックすることもできます。
8. [Finish] をクリックします。

Probe の初期セットアップの実行

Cisco 100 ～ 500 シリーズ製品での組み込み Probe の設定

組み込み Probe を Dashboard に関連付けるプロセスでは、接続前に Dashboard と Probe の両方で明示的な設定が必要です。このプロセスによって、組み込み Probe をホストするデバイスをインストールの前に事前定義するか、またはネットワーク プラグアンドプレイなどのゼロタッチ展開メカニズムを使用して自動的に設定できます。

組み込み Probe をセットアップするには、次の手順を実行します。

1. Dashboard の初期セットアップの実行 （5 ページ） で説明されている手順を使用して、組み込み Probe の新しいネットワークレコードを作成します。組織名とネットワーク名をメモします。
2. [Dashboard] UI で、ナビゲーションパネルの下部にあるユーザー名をクリックして [My Profile] ページに移動します。このページで、[Generate Access Key] ボタンを使用して新しい [Access Key] を作成します。必要に応じて、既存のアクセスキーを使用することもできます。

（注） 組み込み Probe を Dashboard に関連付けるために使用されるアクセスキーは、有効期間の長いキーである必要はありません。このキーが有効である必要があるのは、最初の関連付けが行われる時点のみです。Probe と Dashboard が関連付けられると、ネットワークに固有で、定期的に再生成される、アクセスが制限付きの短期間のログイン情報を使用して接続が認証されます。

3. デバイス UI を使用して、Probe の設定ページに移動し、表示されたフィールドに入力します。少なくとも、Dashboard のアドレスとポート、組織名、ネットワーク名、アクセスキー ID と秘密の設定を指定する必要があります。Dashboard の証明書を設定しなければならない場合もあります。詳細については以下を参照してください。必要に応じて、その他の変更を行うことができます。
4. 変更を送信します。Probe は Dashboard に接続し、手順 1 で作成したネットワークに関連付けられます。

Dashboard のアイデンティティの確認

Dashboard との接続を確立する際、Probe は、Dashboard によって提示された証明書が有効であり、信頼できることを確認します。証明書が受け入れられ、接続が続行されるには、証明書が次の条件を満たしている必要があります。

- 証明書は信頼された証明機関（CA）によって署名されている必要があります。または証明書自体を信頼された証明書としてデバイス設定に追加する必要があります。信頼された証明書の追加の詳細については、デバイスのアドミニストレーション ガイドを参照してください。
- Dashboard が IP アドレスとして設定されている場合は、証明書の [Common Name] フィールドまたは [Subject-Alt-Name] フィールドにその IP アドレスが含まれている必要があります。

Probe の初期セットアップの実行

- Dashboard がホスト名として設定されている場合は、証明書の [Common Name] フィールドまたは [Subject-Alt-Name] フィールドにそのホスト名が含まれている必要があります。

Web ユーザーインターフェイスを使用した VM イメージの基本的なシステム設定（オプション）

Probe の IP アドレスや時刻設定など、基本的なシステム設定を Web ユーザーインターフェイスを使用して行うには、以下の手順に従います。

1. **[管理]** > **[プラットフォーム設定]** に移動します。
2. Probe のホスト名を指定します。ホスト名は、ネットワーク上の Probe を識別するために使用されます。
3. 必要に応じて、静的 IP パラメータをフィールドに指定します。デフォルトでは、Probe は DHCP を使用して IP 設定を自動的に決定します。
4. 内部クロックを使用して時刻を維持するように Probe を設定したり、希望する NTP サーバーを指定したりすることもできます。デフォルトでは、Probe は公開 NTP サーバーと時刻を同期します。

（注） 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。

コマンド ラインを使用した VM イメージの基本的なシステムの設定（オプション）

Webインターフェイスを通じて基本的なシステム設定を行う代わりに、以下のようにコマンドラインを使用して設定できます。

1. 仮想マシン コンソールに接続します。
2. デフォルトのユーザー名とパスワード（cisco）を利用してログインします。パスワードは、ログインしてすぐに変更する必要があります。新しいパスワードには、複雑で、文字種が混在した、辞書に載っていない単語を使用する必要があります。
3. 初期設定を行うには、コマンド `sudo config_vm` を入力します。`config_vm` ユーティリティは、プラットフォーム設定を変更するための一連の手順を表示します。
4. まず、Probe のホスト名を変更するよう求められます。ホスト名は、ネットワーク上の Probe を識別するために使用されます。ここで意味のある名前を選択するか、この手順をスキップしてデフォルトのホスト名のままにすることができます。
5. 次に、Web サーバーポートを変更するように求められます。これらのポートがデフォルト値から変更された場合は、ネットワークのファイアウォール設定を変更することが必要になる場合もあります。
6. 次に、ネットワークインターフェイスを設定するよう求められます。ここでのオプションは static と dhcp（デフォルト）です。static を選択すると、IP アドレス情報、デフォルト

Probe の初期セットアップの実行

ゲートウェイ、DNS サーバーアドレスの入力を求められます。ここで変更を行うとネットワーク インターフェイスがリセットされます。

7. 次に、Probe の時刻を設定するよう求められます。時刻同期用の 1 台以上の NTP サーバーを設定することを選択でき（推奨）、タイムゾーンを選択するよう求められます。

（注） 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。

8. 最後に、ブートローダーのパスワードを変更するかどうかを確認するメッセージが表示されます。ブートローダーのユーザー名とパスワードは、システムのブートプロセスを変更するか、失われたオペレーティングシステムのパスワードを回復するために、システムの起動時にコンソールで使用されることもあります。ブートローダーのデフォルトのログイン情報の場合、ユーザー名は **root**、パスワードは **cisco** です。

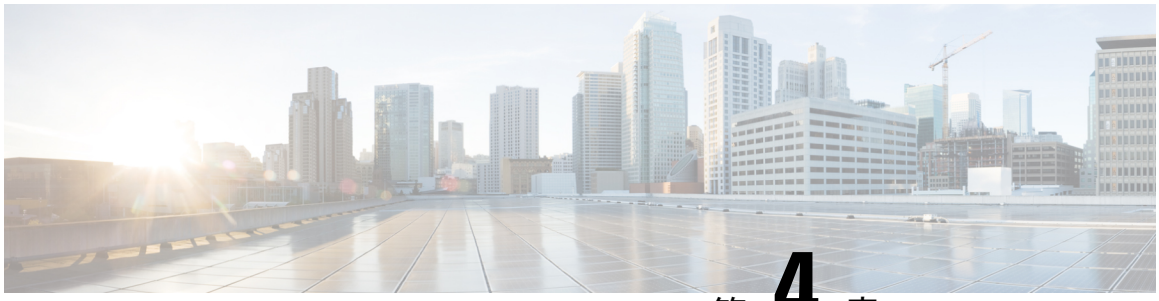
Probe が Cisco Business 製品に組み込まれている場合の基本的なシステム設定

Cisco Business 製品に組み込まれている Probe を使用している場合は、デバイス管理インターフェイスから Probe のユーザーインターフェイスにアクセスします。Probe と Dashboard の関連付けおよびシステム設定の変更の詳細については、デバイスのアドミニストレーション ガイドを参照してください。

Probe と Cisco Business Dashboard が同一ホストに共存している場合の基本的なシステム設定

Cisco Business ダッシュボードと同じホストに共存している Probe には、ユーザーインターフェイスがありません。そのような Probe は、全面的に Dashboard のユーザーインターフェイスを利用して管理されます。

Probe の初期セットアップの実行



第 4 章

直接管理対象デバイスの初期セットアップの実行

この章は、次の項で構成されています。

直接管理対象デバイスの初期セットアップの実行

直接管理対象デバイスは、Dashboard に直接関連付けられ、ネットワークに Probe が存在しない状態で管理されるネットワークデバイスです。特定のデバイスのみが直接管理をサポートします。直接管理をサポートするデバイスとソフトウェアバージョンのリストについては、『Cisco Business Dashboard - Device Support List』[英語] を参照してください。直接管理対象デバイスは、広範囲のネットワークで他のデバイスを検出し、それらのデバイスを Dashboard インベントリに追加します。ただし、この検出プロセスは Probe によって実行されるものほど包括的ではないため、ネットワークトポロジの精度が低下する場合があります。

直接管理対象デバイスを Dashboard に関連付けるプロセスでは、接続前に Dashboard とデバイスの両方で明示的な設定が必要です。このプロセスによって、デバイスを設置前に事前定義するか、ネットワーク プラグ アンド プレイなどのゼロタッチ展開メカニズムを使用して自動的にデバイスを設定できます。

直接管理対象デバイスをセットアップするには、次の手順を実行します。

1. Dashboard の初期セットアップの実行 （5 ページ） で説明されている手順を使用して、デバイスが設置されるネットワークの新しいネットワークレコードを作成します。組織名とネットワーク名をメモします。
2. [Dashboard] UI で、ナビゲーションパネルの下部にあるユーザー名をクリックして [My Profile] ページに移動します。このページで、[Generate Access Key] ボタンを使用して新しい [Access Key] を作成します。必要に応じて、既存のアクセスキーを使用することもできます。

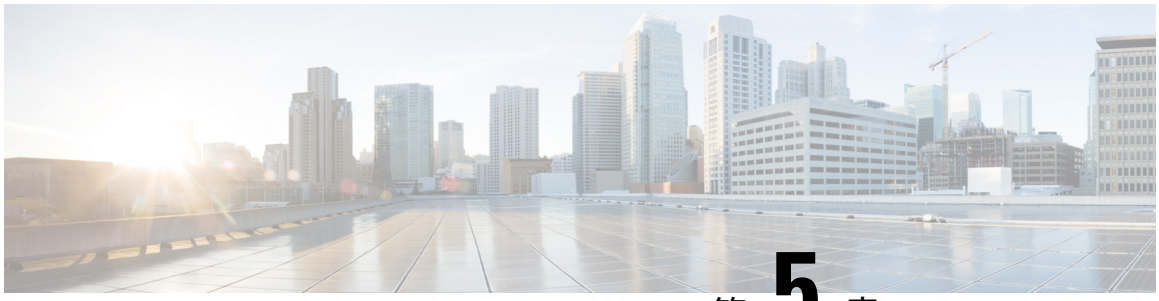
直接管理対象デバイスの初期セットアップの実行

（注） 直接管理対象デバイスを Dashboard に関連付けるために使用されるアクセスキーは、有効期間の長いキーである必要はありません。このキーが有効である必要があるのは、最初の関連付けが行われる時点のみです。デバイスと Dashboard が関連付けられると、デバイスに固有で、定期的に再生成される、アクセスが制限付きの短期間のログイン情報を使用して接続が認証されます。

3. デバイス UI を使用して、Cisco Business ダッシュボードの設定ページに移動し、表示されたフィールドに入力します。少なくとも、Dashboard のアドレスとポート、組織名、ネットワーク名、アクセスキー ID と秘密の設定を指定する必要があります。Dashboard の証明書を設定しなければならない場合もあります。詳細については以下を参照してください。詳細については、デバイスのアドミニストレーション ガイドを参照してください。
4. 変更を送信します。デバイスは Dashboard に接続し、手順 1 で作成したネットワークに関連付けられます。

Dashboard との接続を確立する際、デバイスは、Dashboard によって提示された証明書が有効であり、信頼できることを確認します。証明書が受け入れられ、接続が続行されるには、証明書が次の条件を満たしている必要があります。

- 証明書は信頼された証明機関（CA）によって署名されている必要があります。または証明書自体を信頼された証明書としてデバイス設定に追加する必要があります。信頼された証明書の追加の詳細については、デバイスのアドミニストレーション ガイドを参照してください。
- Dashboard が IP アドレスとして設定されている場合は、証明書の [Common Name] フィールドまたは [Subject-Alt-Name] フィールドにその IP アドレスが含まれている必要があります。
- Dashboard がホスト名として設定されている場合は、証明書の [Common Name] フィールドまたは [Subject-Alt-Name] フィールドにそのホスト名が含まれている必要があります。



第 5 章

「Setting Up the Network」

この章は、次の項で構成されています。

Cisco Business ダッシュボードに関するネットワークの設定

デバイス クレデンシャルの設定

Cisco Business ダッシュボードがネットワークデバイスを管理できるようにするためには、各デバイスにアクセスするための適切なログイン情報を指定する必要があります。

Probe がデバイスを検出すると、まずデフォルトのログイン情報（ユーザー名/パスワード：cisco/cisco）と SNMP コミュニティ（public）を利用してデバイスにアクセスしようとします。しかし、デバイスがデフォルトのクレデンシャルを使用していない場合は、以下で説明する手順に従って、正しいクレデンシャルを指定する必要があります。

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表には、ログイン情報を必要とする、検出されたすべてのデバイスが一覧表示されます。2 番目の表には、有効なログイン情報がすでに認識されているすべての検出済みデバイスが一覧表示されます。
2. ユーザー名とパスワードの組み合わせか、SNMP ログイン情報を、ページの上部にあるそれぞれのフィールドに入力します。さらにログイン情報が必要な場合は、[+]（プラス）アイコンをクリックします。これにより、それぞれの種類のクレデンシャルを 3 セットまで入力できます。
3. [Apply] をクリックします。Probe は、ログイン情報が必要な各デバイスに対して、それぞれのログイン情報をテストします。各デバイスについて正常に機能するクレデンシャルが保存されます。

有効なログイン情報が指定されると、Probe は各ネットワークを検出し、ネットワークのトポロジマップとインベントリを生成します。

ご使用のネットワークの調査

ネットワークのマップまたはリストでネットワークの全体像を示します。すべてのネットワークの概要を表示するには、次の手順を実行します。

1. 前の章で説明されているとおりに Probe を Cisco Business ダッシュボードに関連付けていることを確認します。
2. Dashboard ナビゲーションで [Network] をクリックします。ボタンをクリックして [マップ] ビューまたは [リスト] ビューを表示します。
3. [マップ] ビューでは、マップをクリックし、ドラッグしてマップを移動すること、およびプラスおよびマイナス ボタンを使用して拡大および縮小を行うことができます。Cisco Business ダッシュボードプローブ がインストールされている各ネットワークが、マップ上にアイコンで表示されます。各アイコンには、そのネットワークの未確認の通知の数を示す数字が含まれており、アイコンの色は、未確認の通知のうち重大度が最も高いものを示しています。アイコンをクリックすると、そのサイトの詳細が表示されます。複数のアイコンが重なって識別しづらい場合は、クラスタマーカーに変わり、そのクラスタ内のネットワークアイコンの数が示されます。クラスタマーカーをクリックすると、そのクラスタ内のサイトを拡大できます。

   [リスト] ビューでは、表の左上隅にあるアイコンをクリックすると、表示する列を選択でき、また列見出しをクリックすると、表を並べ替えることができます。
4. 検索ボックスを使用すると、特定のネットワークや、特定のデバイスを含むネットワークを見つけることができます。検索ボックスには、ネットワークの名前、アドレス、または IP アドレスを入力できます。また、デバイスの名前、IP アドレス、MAC アドレス、またはシリアル番号を入力することもできます。
5. ネットワークをクリックすると、そのネットワークの詳細を示す [Basic Info] パネルが表示されます。この情報には、そのネットワークの名前とアドレス、未確認の通知の一覧が含まれています。
6. [Basic Info] パネルの [View] をクリックすると、ネットワークトポロジ図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。[More] をクリックすると、[Network Detail] ビューが開き、このネットワークの設定を変更したり、このネットワークで検出されたすべてのデバイスを表示したりすることができます。

また、[Inventory] を使用して、ネットワーク内のすべてのデバイスに関する詳細情報を表示することもできます。[Inventory] ページには、検出されたすべてのデバイスのリストが表形式で表示されます。リストをフィルタ処理して表示されるデバイスを限定したり、各デバイスをクリックしてそのデバイスの詳細情報を表示したりすることができます。

トポロジ マップのカスタマイズ（オプション）

有効なログイン情報が指定されると、**Probe** は各ネットワークを検出して [Topology] マップを生成します。マップは必要に応じて調整できます。

1. [Network] に移動して、対象のネットワークを選択します。[View] をクリックして、トポロジを表示します。
2. 個々のデバイスアイコンをドラッグしてレイアウトを改善できます。レイアウトに加えた変更はすべてそのまま保持されます。Cisco Business ダッシュボードでは、アイコンの場所がさらに変更されることはありません。アイコンを再度自動配置する場合は、[Relayout Topology] をクリックします。
3. [Overlays] をクリックして、[Overlays and Filters] パネルを開き、チェックボックスを使用して、トポロジ図に表示されるデバイスの種類を制限します。

フロア プランのアップロード（オプション）

デバイスの位置を文書化するために、各ネットワークのフロアプランをアップロードしてネットワークデバイスを配置できます。以降のステップでは、この手順について順を追って説明します。

1. ネットワークのトポロジ図を表示する場合は、[Floor Plan] をクリックします。
2. 建物とフロアの名前を入力した後、画像ファイルをドロップ ゾーンにドラッグするか、ウィジェットの内部をクリックして PC 上の画像ファイルを選択します。サポートされる画像形式には、`.png`、`.gif`、`.jpg` があります
3. **[保存 (Save)]**をクリックして、変更内容を保存します。
4. デバイスをフロアプランに配置するには、[Add Devices] をクリックし、画面下部の検索ボックスにデバイス名または IP アドレスを入力します。一致するデバイスが表示されます。灰色で表示されたデバイスは、フロアプランにすでに配置されています。
5. デバイスをクリックし、フロアプランの正しい場所にドラッグして追加します。

監視ダッシュボードのカスタマイズ

以下の手順で、要件に合わせて監視ダッシュボードをカスタマイズできます。

1. 画面左側のナビゲーションから [ダッシュボード] を選択します。デフォルトのダッシュボードが表示されます。
2. ダッシュボード内の各ウィジェットを移動するには、ダッシュボードの右上にある歯車アイコンをクリックし、[Edit Mode] オプションを選択します。各ウィジェットをクリックしたまま目的の場所にドラッグします。サイズを変更するには、ウィジェットの端または隅をクリックしたままドラッグします。
3. 新しいウィジェットをダッシュボードに追加するには、ダッシュボードの右上にある歯車アイコンをクリックしてウィジェットを選択します。リストから、追加するウィジェット

を選択します。ダッシュボードからウィジェットを削除するには、編集モードの時にウィジェットの右上隅にある、ウィジェット削除用の [X] アイコンをクリックします。

4. ダッシュボードを正しくレイアウトできたら、ダッシュボードの右上にある歯車アイコンをクリックし、[View Mode] を選択して変更内容を固定します。
5. ウィジェットの動作を変更するには、ウィジェットの右上にある [edit widget configuration] アイコンをクリックします。ドロップダウンリストを使用して、ウィジェットがモニタする特定のデバイス、インターフェイス、ネットワークを選択します。

電子メール設定の実行（オプション）

Cisco Business ダッシュボードは、選択したイベントがネットワーク内で発生した場合に、電子メールで通知することができます。電子メールを生成するイベントを制御するには、通知表示のカスタマイズ （22 ページ）を参照してください。電子メールを設定するには、次の手順を実行します。

1. **[System]** > **[Email Settings]** に移動します。
2. このページで、送信メッセージに使用する電子メールサーバーとポート、暗号化と認証の設定、使用する電子メール アドレスを指定できます。
3. 設定を完了したら [保存] をクリックします。
4. 行った変更をテストするには、[Test Connectivity] をクリックします。

通知表示のカスタマイズ

以下の手順を使用して、通知の動作をカスタマイズできます。

1. **[Administration]** > **[Organizations]** に移動し、通知動作をカスタマイズする組織を選択します。
2. [Notification] をクリックします。
3. [Inherit From Notification Defaults] チェックボックスをオフにします。チェックボックスを使用して、ユーザーインターフェイスにポップアップアラートを生成する通知と、電子メール通知を生成する通知を制御します。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、電子メール設定の実行（オプション） （22 ページ）を参照してください。
4. **[Save]** をクリックします。

[Administration] > **[Notification Defaults]** に移動して、[Notification Defaults] をカスタマイズすることもできます。

ネットワーク プラグ アンド プレイの設定

Cisco Business ダッシュボードは、選択したシスコデバイスのファームウェアおよび設定ファイルを一元管理できる Cisco ネットワーク プラグ アンド プレイ サービスを提供しています。ネットワーク プラグ アンド プレイの詳細については、『PnP Solution Guide』を参照してください。

ネットワーク プラグ アンド プレイを設定するには、次のタスクを実行します。

アップロード ファームウェア

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. 組織を選択し、自分の PC からファームウェアファイルをドラッグして、[Upload File] ウィンドウのターゲット領域にドロップします。または、ターゲット領域をクリックし、アップロードするファームウェア イメージを選択します。
4. [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. [イメージ] 表でイメージのチェックボックスを選択し、[編集] をクリックします。
2. [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。
3. [save] をクリックします。

設定のアップロード（オプション）

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. 組織を選択し、自分の PC から設定ファイルをドラッグして、[Upload File] ウィンドウのターゲット領域にドロップします。または、ターゲット領域をクリックし、アップロードする設定ファイルを選択できます。
4. [Upload] をクリックします。

設定をアップロードする代わりに、Dashboard アプリケーションで提供される付属の設定テンプレートを使用することもできます。必要に応じて、設定ファイルの名前をクリックして内容を表示できます。

ディスカバリの設定

ネットワーク デバイスで**ネットワーク プラグ アンド プレイ**を使用するには、最初にネットワーク デバイスが**ネットワーク プラグ アンド プレイ** サーバーを検出する必要があります。この情報をデバイスに提供するために、次の 3 つのメカニズムを使用できます。

1. **DHCP**：ネットワークデバイスは、DHCP オプション 43 を使用して、ネットワーク プラグアンドプレイ サーバーのアドレスを取得できます。オプション形式の詳細については、『Cisco Business Dashboard Administration Guide』の「*About Network Plug and Play*」のセクションを参照してください。
2. **DNS**：ネットワークデバイスは、DHCP を使用してサーバーアドレスを取得しない場合、ローカルドメイン（*pnpserver.example.com* など）内の既知のホスト名（pnpserver）をルックアップしようとします。この名前が Cisco Business ダッシュボード のアドレスに解決されるように DNS インフラストラクチャを設定できます。
3. **Plug and Play Connect**：シスコは、リダイレクトサービスである **Plug and Play Connect** を提供しています。他の方法でサーバーのアドレスが見つからない場合、デバイスはこのサービスに問い合わせます。ネットワークのリダイレクトサービスを設定するには、『Cisco Business Dashboard Administration Guide』の「*Network Plug and Play*」のセクションを参照してください。

デバイスの登録

設置の準備でデバイスを登録するには、以下を行います。

1. **[Network Plug and Play]** > **[Enabled Devices]** に移動します。
2. [✚]（プラス）アイコンをクリックします。
3. 登録するデバイスの名前、製品 ID（PID）、シリアル番号を入力し、ドロップダウンリストから組織、ネットワーク、デバイスグループ、デバイスタイプを選択します。
4. このデバイスに対して使用するファームウェアイメージ、設定ファイル、またはこれらの両方を選択できます。イメージとして [デフォルト イメージ] を選択した場合、デバイスは、サーバーへの接続時にそのデバイス タイプのデフォルトとして指定されているイメージを使用します。
5. [**Save**] をクリックします。

デバイスの自動要求

サーバーに接続しているにもかかわらずインベントリに存在しないデバイスは、未要求デバイスと見なされます。デバイスの製品 ID に対して自動要求ルールを作成することで、サーバーで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ます。

3. 自動要求するデバイスの製品 ID（PID）を入力し、ドロップダウンリストから組織、ネットワーク、デバイスグループ、デバイスタイプを選択します。
4. この製品 ID に対して使用するファームウェア イメージ、設定ファイル、またはこれらの両方を選択できます。イメージとして[デフォルトイメージ]を選択した場合、自動要求デバイスは、サーバーへの接続時にそのデバイス タイプのデフォルトとして指定されているイメージを使用します。
5. [**Save**] をクリックします。

ネットワークの設定

新しいネットワークをインストールする場合、この機会にネットワークの初期設定を行うとよいでしょう。既存のネットワークであっても、このときに設定変更を行うことができます。

デバイスのファームウェアの更新（オプション）

ネットワーク内のデバイスに利用可能なファームウェアの更新がある場合、Dashboard はユーザーに通知します。また、ユーザーインターフェイスのいくつかのエリアに、デバイスを対象とする [Update Firmware] アイコンが表示されます。

1 つのデバイスのファームウェアを更新するには、以下の手順を実行します。

1. **トポロジ マップ**でデバイスをクリックし、[基本情報] パネルを表示します。
2. [アクション] パネルを開き、[ファームウェアの最新へのアップグレード] ボタンをクリックします。Dashboard は必要なファームウェアをシスコからダウンロードし、デバイスに更新を適用します。デバイスはこのプロセスの一部としてリブートします。

   また、ファームウェアをPCからアップグレードすることもできます。そのためには、[ローカルからのアップグレード] オプションをクリックし、アップロードするファームウェアイメージを指定します。
3. アップグレードの進行状況を表示するには、ユーザーインターフェイスの右上にある [Task Status] アイコンをクリックします。

[インベントリ]ビューから個々のデバイスをアップグレードすることもできます。詳細については、『Cisco Business Dashboard Administration Guide』の「*Viewing Device Inventory*」のセクションを参照してください。

ネットワークのファームウェアの更新

使用可能な最新のファームウェアにネットワーク全体をアップグレードする場合は、以下の手順を実行します。

1. 更新するネットワークの [Topology Map] を開きます。
2. ページ上部の [Network Actions] をクリックし、[Upgrade Firmware] オプションを選択します。Dashboard は、使用可能な更新がある各デバイスに必要なファームウェアファイルを

シスコからダウンロードし、更新を各デバイスに順番に適用します。各デバイスはこのプロセスの一部としてリブートします。

3. アップグレードの進行状況を表示するには、ユーザーインターフェイスの右上にある [Task Status] アイコンをクリックします。

デバイス グループの設定

Dashboard は、デバイスグループの概念を使用して、設定を複数のデバイスに同時に適用したり、ネットワーク全体で設定を一致させたりすることができます。デバイスをデバイス グループに割り当てるには、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）アイコンをクリックして新しいグループを追加します。
3. デバイスグループの組織、名前、説明を入力します。[**Save**] をクリックします。
4. デバイスをデバイスグループに追加するには、[Devices] テーブルの [✚]（プラス）アイコンをクリックします。グループに追加するデバイスを検索するには、検索ボックスを使用します。グループに参加させる 1 つ以上のデバイスを選択します。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。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。デバイスをグループから削除するには、デバイスの横にある [Delete] アイコンをクリックします。デバイスは [Default] デバイスグループに移動されます。デバイス グループには、異なるデバイス タイプを混在させることができます。

設定プロファイルの作成

Dashboard では、複数のネットワークデバイスに共通の設定を簡単に適用できます。[Network Configuration Wizard] を使用して設定の各セクションの設定プロファイルを作成したり、プロファイルを個別に作成したりすることができます。[Network Configuration Wizard] を使用するには、次の手順を実行します。

1. **[Network Configuration]** > **[Wizard]** に移動します。
2. 作成する設定プロファイルの名前を入力して組織を選択し、設定を適用するデバイスグループを 1 つ以上選択します。
3. [Next] をクリックします。
4. このグループの時刻設定を指定します。[時間管理] プロファイルには、タイムゾーン、夏時間、およびNTP の設定が含まれています。このグループの [時間管理] プロファイルを作成しない場合は [スキップ] をクリックし、そうでない場合は [次へ] をクリックします。
5. このグループの [DNS 設定] を指定します。[DNS リゾルバ] プロファイルには、ドメイン名と使用する DNS サーバーの設定が含まれています。このグループの [DNS リゾルバ] プロファイルを作成しない場合は [スキップ] をクリックし、そうでない場合は [次へ] をクリックします。

6. このグループのユーザー認証設定を指定します。[認証] プロファイルには、デバイスのローカルユーザーデータベースの設定が含まれています。このグループの [Authentication] プロファイルを作成しない場合は [Skip] をクリックし、作成する場合は [Next] をクリックします。
7. このグループ用に作成する仮想 LAN を指定します。VLAN プロファイルには、1 つ以上の VLAN の詳細情報を含めます。VLAN プロファイルを作成しない場合は、[Skip] をクリックします。VLAN を複数追加する場合は、各 VLAN を作成した後に [Add Another] をクリックします。[Next] をクリックします。
8. このグループ用に作成するワイヤレス LAN を指定します。ワイヤレス LAN プロファイルには、1 つ以上の SSID の詳細情報を含めます。ワイヤレス LAN プロファイルを作成しない場合は、[Skip] をクリックします。SSID を複数追加する場合は、各 SSID を作成した後に [Add Another] をクリックします。[Next] をクリックします。
9. 行った設定を見直します。変更する場合は [Edit] を使用するか、[Back] を使用して適切な画面に戻ります。満足したら [終了] をクリックしてプロファイルを作成し、選択したデバイス グループのデバイスに適用します。
10. 設定の進行状況を確認するには、ユーザーインターフェイスの右上にある [Task Status] アイコンをクリックします。

デバイス設定のバックアップ

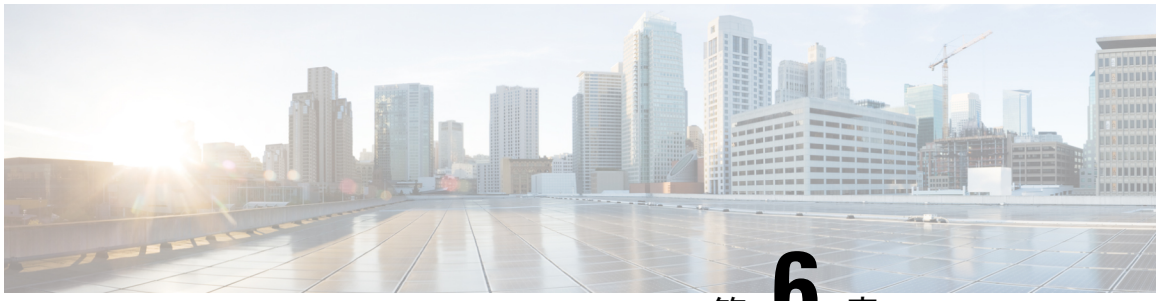
Dashboard では、ネットワークデバイスの設定をバックアップできます。1 つのデバイスの設定をバックアップするには、以下の手順を実行します。

1. **トポロジ マップ**でデバイスをクリックし、[基本情報] パネルを表示します。
2. [アクション]パネルを開き、[バックアップ設定]ボタンをクリックします。必要に応じて、表示されるウィンドウでこのバックアップを説明するメモを追加できます。[Dashboard] にデバイスの設定がコピーされます。
3. バックアップの進行状況を表示するには、ユーザーインターフェイスの右上にある [Task Status] アイコンをクリックします。

個々のデバイスをバックアップすることもできます。そのためには、[インベントリ]ビューで [バックアップ設定] をクリックします。

ネットワーク全体の設定をバックアップするには、以下の手順を実行します。

1. バックアップするネットワークの [Topology Map] を開きます。
2. ページ上部の [アクション]ボタンをクリックし、[バックアップ設定] オプションを選択します。必要に応じて、表示されるウィンドウでこのバックアップを説明するメモを追加します。Dashboard に各デバイスの設定がコピーされます。
3. バックアップの進行状況を表示するには、ユーザーインターフェイスの右上にある [Task Status] アイコンをクリックします。



第 6 章

よく寄せられる質問

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

一般的な FAQ

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

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

- 中国語
- 英語
- フランス語
- ドイツ語
- 日本語

- スペイン語

検出の FAQ

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

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

使用されるプロトコルには以下のものがあります。

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

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

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

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

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

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

設定の FAQ

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

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

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

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

セキュリティ上の留意事項の FAQ

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

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

表 *1 : Cisco Business* ダッシュボード：プロトコルとポート

[ポート（Port）]	方向	プロトコル	使用方法
TCP 22	着信	SSH	Dashboard へのコマンドラインアクセス。Cisco 仮想マシン イメージで SSH はデフォルトで無効になっています。
TCP 80	着信	HTTP	Dashboard への Web アクセス。セキュア Web サーバー（ポート 443）へのリダイレクト。
TCP 443	着信	HTTPS 多重化 TCP	Dashboard へのセキュア Web アクセス。 Probe と Dashboard 間の通信。
TCP 50000 ～ 51000	着信	HTTPS	デバイスへのリモートアクセス。

[ポート（Port）]	方向	プロトコル	使用方法
UDP 53	発信	DNS	ドメイン名解決。
UDP 123	発信	NTP	時刻の同期。
TCP 443	発信	HTTPS	ソフトウェア アップデート、サポート ステータス、サービス終了通知などの情報を得るための、シスコ Web サービスへのアクセス。OS およびアプリケーション更新サービスへのアクセス。
UDP 5353	発信	mDNS	Dashboard をアドバタイズする、ローカルネットワークへのマルチキャスト DNS サービスアドバタイズメント。

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

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

表 *2 : Cisco Business* ダッシュボード：プロトコルとポート

[ポート（Port）]	方向	プロトコル	使用方法
TCP 22	着信	SSH	Probe へのコマンドラインアクセス。Cisco 仮想マシン イメージで SSH はデフォルトで無効になっています。
TCP 80	着信	HTTP	Probe への Web アクセス。セキュア Web サーバー（ポート 443）へのリダイレクト。
TCP 443	着信	HTTPS	Probe へのセキュア Web アクセス。
UDP 5353	着信	mDNS	ローカル ネットワークからのマルチキャスト DNS サービス アドバタイズメントデバイス検出に使用。
UDP 53	発信	DNS	ドメイン名解決。
UDP 123	発信	NTP	時刻の同期

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

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

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

表 *3 : Cisco Business* ダッシュボード - シスコサーバー

ホストネーム	目的
tools.cisco.com	スマートライセンスで使用されます。スマートアカウントの Dashboard に十分なライセンスがあることを確認します。このサーバーは、Dashboard インスタンスが Cisco Smart Licensing に登録されている場合にのみ使用されます。
api.cisco.com	ソフトウェア更新情報と製品ライフサイクル情報を取得するために使用されます。このサーバーは、ソフトウェアの更新またはライフサイクルレポートが [System] > [Privacy Settings] で有効になっている場合にのみ使用されます。

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

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

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

表 *4 : Cisco Business* ダッシュボード - プロセスとシステムサービス

Process	詳細情報
Dashboard の必須プロセス	
/usr/lib/jvm/java-8-openjdk-amd64/bin/java … -jar /usr/lib/ciscobusiness/dashboard/lib/nm-aio-application-x.x.x-SNAPSHOT.jar	Dashboard のメインアプリケーション
/usr/lib/ciscobusiness/dashboard/bin/nginxsvc /usr/lib/ciscobusiness/dashboard/bin/nginx	Web サーバー
/usr/lib/ciscobusiness/dashboard/bin/mongosvc /usr/lib/ciscobusiness/dashboard/bin/mongod	データベース サービス
/usr/lib/ciscobusiness/dashboard/bin/redissvc /usr/lib/ciscobusiness/dashboard/bin/redis-server	インメモリ キャッシュ サービス

Process	詳細情報
Dashboard の必須プロセス	
/usr/lib/ciscobusiness/dashboard/bin/rabbitmqsvc /usr/lib/ciscobusiness/dashboard/bin/rabbitmq-server /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd.smp erl_child_setup	メッセージブローカ
/usr/lib/ciscobusiness/dashboard/bin/bonjoursvc avahi-publish	マルチキャスト DNS アナウンスメント
/bin/sh /usr/share/contuit/contuit /bin/sh /usr/share/contuit-computations/contuit-computations /bin/sh /usr/share/contuit-monorepo/contuit-mop /bin/sh /usr/share/contuit-scheduler/contuit-scheduler /bin/sh /usr/share/contuit-shim/contuit-shim	外部アプリケーションとの統合が有効な場合にのみ必要
Dashboard の必須システムサービス	
/usr/sbin/rsyslog	ロギングサービス
/usr/sbin/cron	スケジューリングサービス
systemd-timesyncd	タイムサービス
avahi-daemon	マルチキャスト DNS リスナー

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

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

表 *5 : Cisco Business* ダッシュボード - プロセスとシステムサービス

Process	詳細情報
Probe の必須プロセス	
/usr/lib/ciscobusiness/probe/bin/cbdprobe chagent	Probe のメインアプリケーション
/usr/lib/ciscobusiness/probe/bin/main /usr/lib/ciscobusiness/probe/bin/publish avahi-publish	マルチキャスト DNS アナウンスメント

Process	詳細情報
Probe の必須プロセス	
nginx	Web サーバー Dashboard サーバーに配置されている場合、Probe は Dashboard Web サーバーを共有します。
Probe の必須システムサービス	
/usr/sbin/rsyslogd	ロギングサービス
/usr/sbin/cron	スケジューリングサービス
systemd-timesyncd	タイムサービス
avahi-daemon	マルチキャスト DNS リスナー
lldpd	LLDP ネイバー探索

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

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

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

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

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

A. Cisco Business ダッシュボードにアクセスするためのログイン情報は、SHA512 アルゴリズムを使用して不可逆的にハッシュ化されます。デバイスと、**Cisco Active Advisor** などのその他のサービスのためのクレデンシャルは、AES-128 アルゴリズムを使用して不可逆的に暗号化されます。

Q. Web UI 用のパスワードをなくした場合、どのようにすれば回復できますか。

A. Web UI のすべての admin アカウントのパスワードをなくした場合は、Probe のコンソールにログインして **cbdprobe recoverpassword** ツールを実行するか、Dashboard のコンソールにログインして **cisco-business-dashboard recoverpassword** ツールを実行することで、パスワードを回復できます。このツールは、cisco アカウントのパスワードをデフォルトの cisco にリセットします。cisco アカウントが削除されている場合は、デフォルトのアカウント

を使用してアカウントを作成します。以下に、このツールを使用してパスワードを回復するために実行するコマンドの例を示します。

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

（注） Cisco Business ダッシュボード for AWS を使用する場合、パスワードは AWS インスタンス ID に設定されます。

Q. 仮想マシンブートローダーのデフォルトのユーザー名とパスワードは何ですか。

A. 仮想マシンブートローダーのデフォルトのログイン情報の場合、ユーザー名は **root** 、パスワードは **cisco**です。これらを変更するには、config_vm ツールを実行し、ブートローダーのパスワードを変更するかどうかを尋ねられたら、「yes」と応答します。

リモート アクセスの FAQ

Q. デバイスの管理インターフェイスに Cisco Business ダッシュボード から接続した場合、セッションはセキュリティ保護されますか。

A. Cisco Business ダッシュボード リモートアクセスセッションを、デバイスとユーザーの間でトンネリングします。Probe とデバイス間で使用されるプロトコルはエンドデバイスの設定によって変わりますが、Cisco Business ダッシュボード は、セキュアなプロトコルが有効になっていれば、必ずそのプロトコルを使用してセッションを確立します（たとえば、HTTPS は HTTP よりも優先されます）。ユーザーが Dashboard を介してデバイスに接続している場合、セッションは、Dashboard と Probe の間を通過するときに、デバイスで有効になっているプロトコルにかかわらず、暗号化されたトンネルを通過します。ユーザーの Web ブラウザと Dashboard の間の接続は常に HTTPS になります。

Q. 別のデバイスとのリモート アクセス セッションをオープンしたときに、デバイスとのリモート アクセス セッションがすぐにログ アウトするのはなぜですか。

A. Cisco Business ダッシュボード を介してデバイスにアクセスすると、ブラウザは各接続を同じ Web サーバー（Dashboard）との接続であると見なすため、各デバイスからの cookie を他のすべてのデバイスに提供します。複数のデバイスが同じ cookie 名を使用する場合、あるデバイスの cookie が別のデバイスによって上書きされる可能性があります。これは、セッション cookie で最も頻繁に発生し、最後に訪れたデバイスに対してのみ cookie が有

効であるという結果になります。同じ cookie 名を使用する他のすべてのデバイスはその cookie を無効と見なし、セッションをログアウトします。

Q. リモート アクセス セッションが以下のようなエラーで失敗するのはなぜですか。**アクセスエラー：リクエストエンティティが大きすぎます。**HTTP ヘッダーフィールドがサポートされているサイズを超えています。

A. 異なるデバイスと多数のリモートアクセスセッションを確立すると、ブラウザにはDashboardドメイン用に大量の cookie が保存されます。この問題を回避するには、ブラウザ コントロールを使用してドメインの cookie をクリアしてから、ページを再ロードしてください。

ソフトウェア アップデートの FAQ

Q. Dashboard のオペレーティングシステムを最新に保つにはどうすればよいですか。

A. Dashboard は、オペレーティングシステムに Ubuntu Linux ディストリビューションを使用しています。パッケージとカーネルは、Ubuntu の標準的なプロセスを使用して更新できます。たとえば、手動更新を行うには、コンソールに cisco ユーザーでログオンし、コマンド `sudo apt-get update` および `sudo apt-get upgrade` を実行します。システムを新しい Ubuntu リリースにアップグレードしてはならず、シスコによって提供されている仮想マシンに含まれているパッケージ、または最小限の Ubuntu インストールの一部としてインストールされたパッケージ以外の追加パッケージをインストールしないことを推奨します。

Q. Dashboard で Java を更新するにはどうすればよいですか。

A. Cisco Business ダッシュボードは Ubuntu リポジトリの OpenJDK パッケージを使用します。OpenJDK はコア オペレーティング システムの更新の一部として自動的に更新されます。

Q. Probe のオペレーティング システムを最新に保つにはどうすればよいですか。

A. Cisco Business ダッシュボードはオペレーティングシステムに Ubuntu Linux ディストリビューションを使用しています。パッケージとカーネルは、Ubuntu の標準的なプロセスを使用して更新できます。たとえば、手動更新を行うには、コンソールに cisco ユーザーでログオンし、コマンド `sudo apt-get update` および `sudo apt-get upgrade` を実行します。システムを新しい Ubuntu リリースにアップグレードしてはならず、シスコによって提供されている仮想マシンに含まれているパッケージ、または最小限の Ubuntu インストールの一部としてインストールされたパッケージ以外の追加パッケージをインストールしないことを推奨します。

Q. Raspberry Pi を使用している場合に Probe のオペレーティングシステムを最新に保つにはどうすればよいですか。

A. Raspbian パッケージおよびカーネルは、Debian ベースの Linux ディストリビューションに使用される標準プロセスを使用して更新できます。たとえば、手動更新を行うには、コンソールに cisco ユーザーでログオンし、コマンド `sudo apt-get update` および `sudo apt-get upgrade` を実行します。システムを Raspbian の新しいメジャーリリースにアップグレードすることはできません。Raspbian ディストリビューションの「Lite」バージョンの一部としてインストールされているパッケージ、および Probe インストーラによって

追加されたパッケージよりも新しいバージョンのパッケージを追加しないことを推奨します。

Q. Cisco Business Dashboard 2.3.0 に Ubuntu 20.04（Focal Fossa）のサポートが追加されました。システムを 2.3.0 にアップグレードした場合、オペレーティングシステムを Ubuntu 16.04 から Ubuntu 20.04 にアップグレードできますか。

A. 残念ながら、2つのオペレーティング システム リリース間の変更は、インプレースアップグレードを実行するには大きすぎます。Ubuntu 16.04 を実行している既存のシステムがある場合は、Dashboard をリリース 2.3.0 にアップグレードしてから、**[System]** > **[Backup]** ページを使用して Dashboard のバックアップを作成する必要があります。次に、Ubuntu 20.04 を使用して Dashboard を再構築するか、Ubuntu 20.04 に基づいて新たに Dashboard インストールを実行します。その後、古い Dashboard から新しい Dashboard にバックアップを復元できます。

Q. Cisco Business Dashboard 2.3.0 に Ubuntu 20.04（Focal Fossa）のサポートが追加されました。システムを 2.3.0 にアップグレードした場合、オペレーティングシステムを Ubuntu 16.04 から Ubuntu 20.04 にアップグレードできますか。

A. 残念ながら、2つのオペレーティング システム リリース間の変更は、インプレースアップグレードを実行するには大きすぎます。Ubuntu 16.04 を実行している既存のシステムがある場合は、Dashboard をリリース 2.3.0 にアップグレードしてから、**[System]** > **[Backup]** ページを使用して Dashboard のバックアップを作成する必要があります。次に、Ubuntu 20.04 を使用して Dashboard を再構築するか、Ubuntu 20.04 に基づいて新しい Dashboard インストールを実行します。その後、古い Dashboard から新しい Dashboard にバックアップを復元できます。