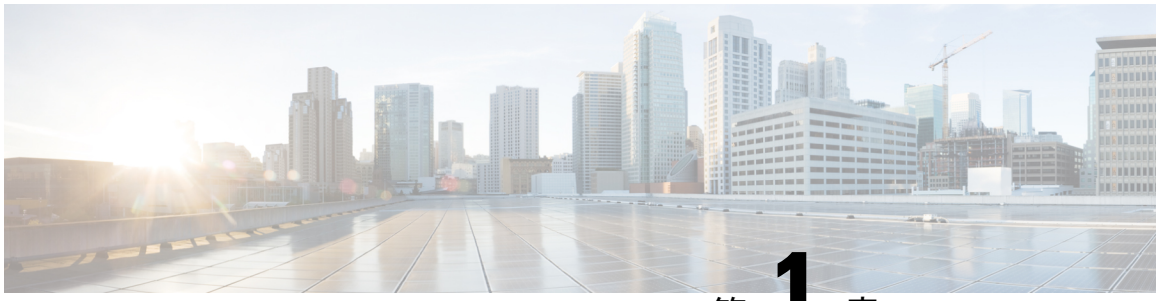
Cisco FindIT Network Manager/Probe バージョン 2.0 クイック スタート ガイド

初版：2019 年 10 月 24 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。

目 次



第 1 章

Cisco FindIT Network Management の概要

この章は、次の項で構成されています。

Cisco FindIT ネットワーク管理 について

Cisco FindIT ネットワーク管理 には Cisco 100 ～ 500 シリーズの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。FindIT ネットワーク管理 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 100 ～ 500 シリーズの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。

FindIT ネットワーク マネージャ は、2 つの個別のコンポーネントまたはアプリケーション（FindIT Network Probe と呼ばれる 1 つ以上のプローブと、FindIT ネットワーク マネージャ と呼ばれる 1 つのマネージャ）から構成される分散アプリケーションです。

FindIT Network Probe 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、ネットワークを検出し各シスコのデバイスと直接通信します。FindIT ネットワーク マネージャ のシングルインスタンスはネットワーク内の扱いやすい場所にインストールされ、各プローブはマネージャと関連付けられます。マネージャインターフェイスからは、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できます。

対象読者

このガイドは主に Cisco FindIT ネットワーク管理 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 FindIT Network Manager/Probe 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。

- **クイック スタート ガイド（本書）**：最も一般的に選択されるオプションを使用した FindIT Network Manager/Probe の初期セットアップ方法について詳しく説明します。
- **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 FindIT 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。

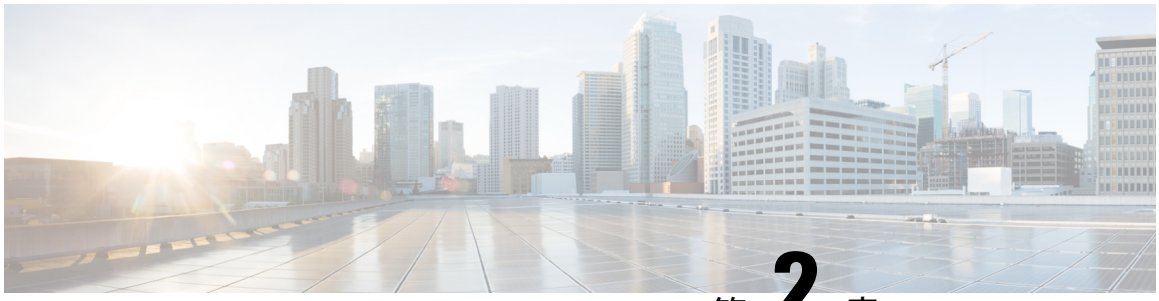
対応プラットフォーム	所在地
Amazon Web Services	Cisco FindIT Network Manager & Probe Installation Guide for Amazon Web Services
Oracle VirtualBox	Cisco FindIT Network Manager & Probe Installation Guide for Oracle VirtualBox
Microsoft Hyper-V	Cisco FindIT Network Manager & Probe Installation Guide for Microsoft Hyper-V
VMWare vSphere、ワークステーション、およびフュージョン	Cisco FindIT Network Manager & Probe Installation Guide for VMWare
Ubuntu Linux（マネージャとプローブ）および Raspbian Linux（プローブのみ）	Cisco FindIT Network Manager & Probe 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に関するリファレンス ガイドです。『Cisco FindIT Network Manager/Probe アドミニストレーション ガイド』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/* 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、*https://www.raspbian.org/* を参照してください。
VirtualBox	Oracle Corporation によって提供されている仮想化プラットフォーム。
Virtual Hard Disk（VHD）	ハード ドライブの完全な内容を格納するためのディスク イメージ ファイル形式。
仮想マシン（VM）	ゲスト オペレーティング システムと関連するアプリケーション ソフトウェアが動作可能な、仮想コンピューティング環境。同一のホスト システム上で同時に複数の VM を実行できます。
• VMWare ESXi • VMWare V5 • vSphere Server • VMWare Workstation	VMWare Inc. によって提供されている仮想化プラットフォーム。

用語	説明
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。



第 2 章

Manager の初期セットアップ

この章は、次の項で構成されています。

Manager の初期セットアップ

Manager が各自の要件を満たすようにするため、実行すべきいくつかの設定作業があります。

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

Manager 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、以下のようにします。

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 Manager 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名とパスワード（cisco）を利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、ログインして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、Manager のホスト名を変更するよう求められます。ホスト名は、Bonjour アドバタイズメントと FindIT ユーザ インターフェイスで Manager 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、FindIT ネットワーク マネージャ for AWS では使用できません。

5. 次に、Web サーバの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 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、FindIT Network Manager for AWS では使用できません。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. 最後に、Manager 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。

これらの設定はいつでも変更できます。そのためには、スクリプトを再度実行するか、Web インターフェイスの **[管理]** > **[プラットフォーム設定]** を使用します。

Manager ユーザ 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. [アドレス（Address）] フィールドに Manager の IP アドレスまたはホスト名を入力して Enter を押します。
3. デフォルトのユーザ名とパスワード（`cisco/cisco`）を入力します。FindIT ネットワーク マネージャ 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。cisco アカウントの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. [次へ（Next）] をクリックします。FindIT ネットワーク マネージャ でどのようにデータが使用されるか、および、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、[完了（Finish）] をクリックします。

FindIT ネットワーク マネージャ のユーザ 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、通常は個別に管理するネットワーク、ユーザ、デバイスを、FindIT Network Manager でグループに分割して管理するために使用します。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、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をより細かく制御できます。Manager 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. **[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 1 ～ 5 の手順を繰り返します。

ユーザの作成とパスワードの変更

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

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（Administration）]** > **[ユーザ（Users）]** に移動します。
2. [ユーザ（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 [ユーザの追加（Add user）] ウィンドウで、作成するユーザの詳細を入力します。このユーザが、管理者、組織管理者、オペレータ、読み取り専用ユーザのいずれであるかを指定します。次に、ユーザ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すべての機能にアクセスできますが、[システム（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、ユーザを管理することはできません。[システム（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：設定は一切変更できず、[管理（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。[システム（System）] メニューにはアクセスできません。
4. [保存（Save）] をクリックして新規ユーザを作成します。

[ユーザ（Users）] ページの [ユーザ設定（User Settings）] タブで、パスワードの複雑度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. ユーザインターフェイスの右上で自分のユーザ名をクリックして、[マイプロファイル（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. [パスワードのリセット（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. [保存（Save）] をクリックします。

ライセンスの設定

（注） これは、FindIT ネットワーク マネージャ for AWS の従量制課金版には適用されません。

FindIT Network Manager には、Cisco Smart Licensing を使用するためのライセンスがあります。Manager を初めてインストールすると、Manager 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 FindIT ライセンスが含まれる Cisco スマート アカウントに Manager を関連付ける必要があります。

Manager 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。[トークンの作成（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. FindIT ネットワーク マネージャ のユーザ インターフェイスに移動し、**[管理（Administration）] > [ライセンス（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。

Manager が Cisco Smart Licensing に登録され、管理対象のネットワーク 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。ライセンス付与プロセスの詳細については、『*Cisco FindIT Network Manager/Probe* アドミニストレーション ガイド』の「ライセンス管理」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） これは、FindIT ネットワーク マネージャ for AWS には適用されません。

Manager の仮想マシン イメージには、Manager 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。

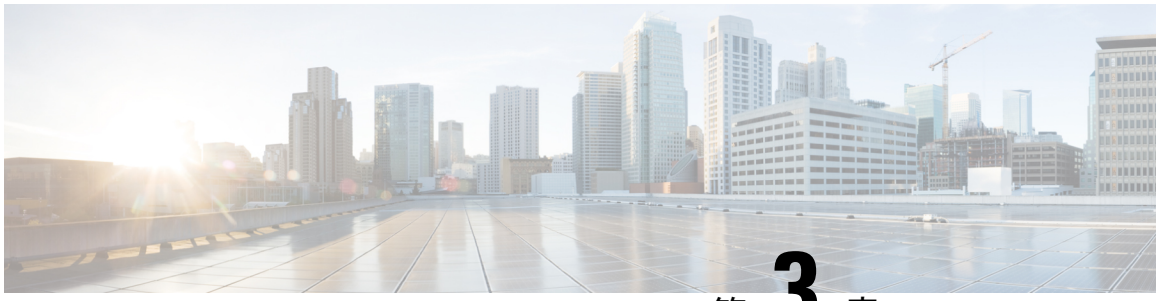
1. **[システム（System）] > [ローカルProbe（Local Probe））]** に移動します。
2. トグル スイッチをクリックして組み込み Probe を無効にします。
3. [保存（Save）] をクリックします。

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、Manager にネットワーク レコードを事前に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、同じサイトに複数のネットワークを配置することができます。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. [ネットワーク（Network）] に移動します。
2. [マップビュー（Map View）] で [ネットワークの追加（Add Network）] をクリックするか、[リストビュー（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. [保存（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。

Manager の初期セットアップ



第 3 章

Probe の初期セットアップ

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

以下では、FindIT Network Probe の使用を開始するまでの手順を詳しく説明します。

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、Bonjour アドバタイズメントと FindIT ユーザ インターフェイスで 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、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 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。

DHCP を使用したデフォルト IP アドレスの設定

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 サーバが稼働しており、到達可能であることを確認します。

Probe の IP アドレスの特定

1. 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。
2. 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。**Apple Mac Safari** ブラウザなどの 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。
3. 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、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。
4. ルータまたは DHCP サーバにアクセスして、DHCP サーバ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 サーバの取り扱い説明書を参照してください。

管理用 GUI を使用した VM イメージでの基本的なシステム設定

1. **Google Chrome** や **Microsoft Edge** などの Web ブラウザを起動します。
2. [アドレス（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、[入力（Enter）] をクリックします。
3. デフォルトのユーザ名とパスワード（`cisco/cisco`）を入力します。[Login] をクリックします。
4. cisco アカウントの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。[保存（Save）] をクリックします。
5. 接続先の Manager のアドレスまたはホスト名を指定し、[次へ（Next）] をクリックします。

6. ブラウザが Manager のログイン画面にリダイレクトされます。Manager の管理者のクレデンシャル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. [完了（FINISH）] をクリックします。

Web ユーザ インターフェイスを使用した Probe の基本的なシステム設定

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 インターフェイスを使用して行うには、以下のようにします。

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、Bonjour アドバタイズメントと FindIT Network Discovery Utility ユーザ インターフェイスで Manager 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 を設定することも、優先する NTP サーバを指定することもできます。デフォルトでは、Probe は公開 NTP サーバ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。

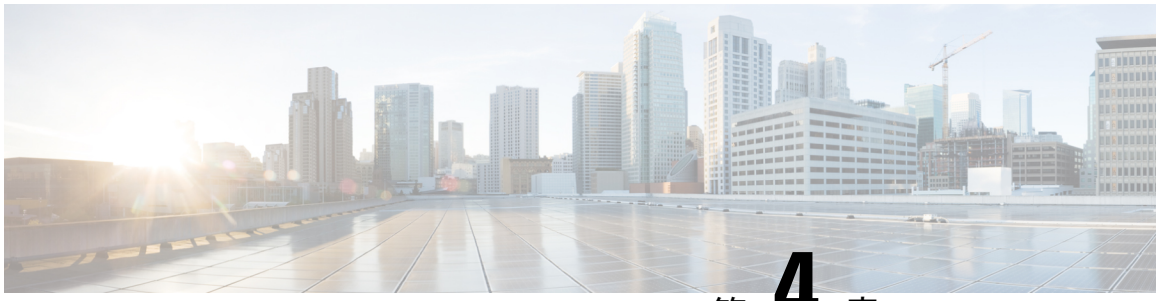
Probe が Cisco 100 ～ 500 シリーズ製品に組み込まれている場合の基本的なシステム設定

Cisco 100 ～ 500 シリーズ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 インターフェイスにアクセスします。Probe と Manager 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 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 Manager 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

バージョン 2.0 以降の Manager と同じホストに共存している Probe には、ユーザ インターフェイスはありません。すべて Manager のユーザ インターフェイスを利用して管理します。

Probe の初期セットアップ



第 4 章

ネットワークの設定

この章は、次の項で構成されています。

Manager のネットワーク設定

デバイス クレデンシャルの設定

FindIT ネットワーク マネージャ 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クレデンシャルを指定する必要があります。

Probe がデバイスを検出すると、まずデフォルトのクレデンシャル（ユーザ名/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、クレデンシャルを必要とする、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、機能しているクレデンシャル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. ユーザ名とパスワードの組み合わせか、SNMP クレデンシャルを、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。さらにクレデンシャルが必要な場合は、[+]（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. **[適用（Apply）]** をクリックします。Probe は、クレデンシャルが必要な各デバイスに対して、それぞれのクレデンシャルをテストします。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。

   有効なクレデンシャルが指定されたら、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

FindIT ネットワーク マネージャ は、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ビューを表示するには次の手順を実施します。

1. 前の項で説明したように、FindIT Network Probe と Manager を関連付けていることを確認します。
2. Manager のナビゲーション パネルで [ネットワーク（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（Map View）] または [リストビュー（List View）] 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。FindIT Network Probe 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、未確認の状態の重要度が最も高いことを示しています。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 [基本情報（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. [基本情報（Basic Info）] パネルの [表示（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。[詳細（More）] をクリックすると、[ネットワーク詳細（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、[インベントリ（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。[インベントリ（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）

Probe に有効なクレデンシャルを指定すると、 各ネットワークを検出して [トポロジ（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. [ネットワーク（Network）] に移動して対象のネットワークを選択します。[表示（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保持されます。FindIT ネットワーク マネージャ 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、[トポロジの再レイアウト（Relayout Topology）] をクリックします。
3. [オーバーレイ（Overlays）] をクリックして、[オーバーレイとフィルタ（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、[フロアプラン（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、[デバイスの追加（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。

ダッシュボードのカスタマイズ

以下の手順を使用して、要件に合わせて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、[編集モード（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、[表示モード（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）

FindIT Network Probe 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 （18 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. **[システム（System）] > [電子メール設定（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. **[管理（Administration）] > [組織（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. [通知（Notification）] をクリックします。
3. [通知のデフォルトを継承する（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 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） （18 ページ）を参照してください。
4. [保存（Save）] をクリックします。

[管理（Administration）] > [通知のデフォルト（Notification Defaults）] に移動して、[通知のデフォルト（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

FindIT ネットワーク マネージャ 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 サーバを提供していま

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 ソリューション ガイド』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、[ファイルのアップロード（Upload File）] ウィンドウの対象エリアにドロップします。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. [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. [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. [保存] をクリックします。

設定のアップロード

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、[ファイルのアップロード（Upload File）] ウィンドウの対象エリアにドロップします。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. [アップロード（Upload）] をクリックします。

設定ファイルの内容を確認する必要がある場合、アップロードした設定ファイルのファイル名をクリックすると、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、

『FindIT Network Manager/Probe アドミニストレーション ガイド バージョン 2.0』の「ネットワーク プラグ アンド プレイについて」の項を参照してください。

2. **DNS**：ネットワーク デバイスがDHCPを使用してサーバアドレスを取得しない場合、ローカル ドメイン内の既知のホスト名（pnpserver。例：*pnpserver.example.com*）をルックアップしようとします。この名前がFindITネットワーク マネージャ 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（**Plug and Play Connect**）を提供しています。他の方法でサーバ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。現在のネットワークにリダイレクト サービスを設定する場合は、Plug & Play Connect 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. **[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. [保存（Save）]をクリックします。

デバイスの自動要求

サーバ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. [保存（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アップデートがある場合、Managerはユーザに通知します。また、ユーザインターフェイスのいくつかの場所で、デバイスに対して[ファームウェアのアップデート（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。Probe は必要なファームウェアをシスコからダウンロードし、デバイスにアップデートを適用します。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 インターフェイスの右上にある [タスクステータス（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、『FindIT Network Manager/Probe アドミニストレーション ガイド バージョン 2.0』の「デバイス インベントリの表示」の項を参照してください。

ネットワークのファームウェアのアップデート

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

1. アップデートするネットワークの [トポロジマップ（Topology Map）] を開きます。
2. ページ上部の [ネットワークアクション（Network Actions）] をクリックし、[ファームウェアのアップグレード] オプションを選択します。Probe は、使用可能なアップデートがある各デバイスについて、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、アップデート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 インターフェイスの右上にある [タスクステータス（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

Manager 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。[保存（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、[デバイス（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 [削除（Delete）] アイコンをクリックします。デバイスは **Default（デフォルト）** 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

Manager 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。[ネットワーク設定ウィザード（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できます。[ネットワーク設定ウィザード（Network Configuration Wizard）] を使用するには、次の手順を実行します。

1. **[ネットワーク設定（Network Configuration）]** > **[ウィザード（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. [次へ（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 データベースの設定が含まれています。このグループの [認証（Authentication）] プロファイルを作成しない場合は [スキップ（Skip）] をクリックし、作成する場合は [次へ（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、[スキップ（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、[さらに追加（Add Another）] をクリックします。[次へ（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、[スキップ（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、[さらに追加（Add Another）] をクリックします。[次へ（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 [編集（Edit）] を使用するか、[戻る（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 インターフェイスの右上にある [タスクステータス（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

Manager 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。

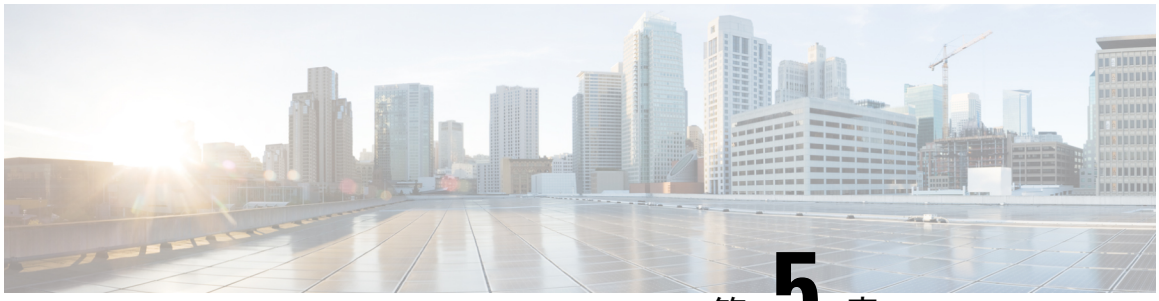
1. **トポロジ マップ**でデバイスをクリックし、[基本情報] パネルを表示します。
2. [アクション] パネルを開き、[バックアップ設定] ボタンをクリックします。必要に応じて、表示されるウィンドウでこのバックアップを説明するメモを追加できます。**Probe** はデバイスの設定をコピーし、Probe 上にローカルに保存します。
3. バックアップの進行状況を表示するには、ユーザ インターフェイスの右上にある [タスクステータス（Task Status）] アイコンをクリックします。

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 [トポロジマップ（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。Probe は各デバイスの設定をコピーし、Manager に保存します。
3. バックアップの進行状況を表示するには、ユーザ インターフェイスの右上にある [タスクステータス（Task Status）] アイコンをクリックします。

ネットワークの設定



第 5 章

よく寄せられる質問（FAQ）

この章では、Cisco FindIT ネットワーク管理 の機能と、発生する可能性がある問題に関するよくあ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）

Q. FindIT ネットワーク管理 ではどのような言語がサポートされていますか。

A. FindIT ネットワーク管理 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. デバイスを管理するために FindIT は何のプロトコルを使用しますか。

A. FindIT 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）
- Simple Network Management Protocol（SNMP）
- RESTCONF（*https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/* を参照）
- スイッチ プラットフォーム用プライベート XML API

Q. FindIT はどうやってネットワークを検出しますか。

A. FindIT Network 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. FindIT はネットワーク スキャンを行いますか。

A. FindIT はネットワークを積極的にスキャンすることはしません。Probe は ARP プロトコルを使用して直接接続されている IP サブネットをスキャンしますが、その他のアドレス範

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

設定の FAQ

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

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

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

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

セキュリティ上の留意事項の FAQ

Q. FindIT Network Manager ではどのポート範囲とプロトコルが必要ですか。

A. 次の表に、FindIT ネットワーク マネージャ が使用するプロトコルとポートのリストを示します。

***表 1 : FindIT Network Manager* - 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	Manager 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	Manager への Web アクセス セキュア Web サービス（ポート 443）へのリダイレクト
TCP 443	インバウンド	HTTPS	Manager へのセキュア Web アクセス

ポート	方向	プロトコル	利用方法
TCP 1069	インバウンド	NETCONF/TLS	リリース 1.x での Probe と Manager 間の通信。 リリース 1.x のプローブが存在する場合に、リリース 2.0 でのみ使用されます。
TCP 50000 ～ 51000	インバウンド	デバイスに応じて異なる	デバイスへのリモート アクセス
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
UDP 5353	アウトバウンド	mDNS	Manager 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. FindIT Network Probe ではどのポート範囲とプロトコルが必要ですか。

A. 次の表に、FindIT Network Probe が使用するプロトコルとポートのリストを示します。

表 *2 : FindIT Network Probe* - 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 アドバタイズメントデバイス検出に使用。

ポート	方向	プロトコル	利用方法
TCP 10000 ～ 10100	インバウンド	デバイスに応じて異なる	デバイスへのリモートアクセス。 この範囲は FindIT Network Probe バージョン 1.x でのみ使用されます。
UDP 53	アウトバウンド	DNS	ドメイン名解決。
UDP 123	アウトバウンド	NTP	時刻同期
TCP 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	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。
TCP 1069	アウトバウンド	NETCONF/TLS	Probe と Manager の間の通信。
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. FindIT Network Manager と FindIT Network Probe の間の通信は、どの程度セキュリティ保護されていますか。

A. Manager と Probe の間の通信は、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 Manager に対して開始されます。Manager と Probe の間の関連付けが最初に確立されるときに、ユーザは Probe から Manager にログオンする必要があります。この時点で、Manager と Probe は証明書を交換し、将来の通信を認証します。

Q. FindIT には、デバイスへの「バックドア」アクセスがありますか。

A. いいえ。FindIT 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出荷時のデフォルト クレデンシャル（ユーザ名/パスワード：`cisco`、または 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、ユーザが正しいクレデンシャルを FindIT に指定する必要があります。

Q. FindIT に保存されているクレデンシャルはどの程度セキュリティ保護されていますか。

A. FindIT にアクセスするためのクレデンシャルは、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、**finditprb recoverpassword** ツールを実行するか、Manager のコンソールにログインし、**finditmgr recoverpassword** ツールを実行することで、パスワードを回復できます。このツールは、cisco アカウントのパスワードをデフォルトの cisco にリセットします。cisco アカウントが削除されている場合は、デフォルトのアカウントを使用してアカウントを作成します。以下に、このツールを使用してパスワードを回復するために実行するコマンドの例を示します。

```
cisco@findit-manager:~$ finditmgr recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword FindIT Manager successful!
cisco@findit-manager:~$
```

（注） FindIT ネットワーク マネージャ 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。

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 FindIT Network Management 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. FindIT Network Management は、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。プローブ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、FindIT 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 Manager を介してデバイスに接続している場合、セッションは、Manager 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 Manager 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. FindIT Network Manager 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（FindIT）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：要求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 Manager 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. Manager 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. バージョン 1.1.0 以降、Manager 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. Manager で Java を更新するにはどうすればよいですか。

A. バージョン 1.1.0 以降、FindIT Network Manager 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. バージョン 1.1.0 以降、Probe はオペレーティング システムに Ubuntu Linux ディストリビューションを使用しています。パッケージとカーネルは、Ubuntu の標準的なプロセスを使用して更新できます。たとえば、手動更新を行うには、コンソールに cisco ユーザでログオンし、コマンド `sudo apt-get update` および `sudo apt-get upgrade` を実行します。システムを新しい Ubuntu リリースにアップグレードしてはならず、シスコによって提供されている仮想マシンに含まれているパッケージ、または最小限の Ubuntu インストールの一部としてインストールされたパッケージ以外の追加パッケージをインストールしないことを推奨します。

Q. Raspberry Pi を使用している際にプローブ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 パッケージとカーネルは、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される場合があります。たとえば、手動更新を行うには、コンソールに cisco ユーザでログオンし、コマンド `sudo apt-get update` および `sudo apt-get upgrade` を実行します。システムを Raspbian の新しいメジャー リリー

スにアップグレードすることはできません。Raspbian ディストリビューションの「Lite」バージョンの一部としてインストールされているパッケージおよび、Probe インストーラによって追加されたパッケージ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。