Cisco FindIT Network Probe アドミニストレーション ガイド

初版：2016 年 09 月 08 日

最終更新：2017 年 02 月 02 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 概要

この章の内容は、次のとおりです。

Cisco FindIT Network Management について

Cisco FindIT Network Management は、Cisco 100 から 500 シリーズのネットワークを監視および管理するうえで役立つツールを提供します。FindIT Network Management 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 から 500 シリーズ 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 Network Manager は、2 つの個別のコンポーネントまたはインターフェイスからなる分散アプリケーションです。それは、FindIT Network Probe と呼ばれる 1 つ以上の Probe と、FindIT Network Manager と呼ばれる単一の Manager 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 デバイスと直接通信します。単一サイトのネットワークでは、FindIT Network Probe のスタンドアロンインスタンスを実行することもできますが、ネットワークが複数のサイトからなる場合は、FindIT Network Manager を便利な場所にインストールし、各 Probe を Manager に関連付けることができます。Manager 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概要を表示できます。また、特定のサイトの詳細情報を表示する場合は、そのサイトにインストールされている Probe に接続することができます。

FindIT Network Manager と FindIT Network Probe は、それぞれの管理ガイドで詳しく説明されています。

FindIT Network Probe の詳細については、本ユーザ ガイドの以下のセクションを参照してください。

対象とする読者

このガイドは、Cisco FindIT Network Management 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主な対象としています。

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 または Application（OVA）ファイル	仮想ファイルを記述するために使用される以下のファイルが格納され、.TAR パッケージングを使用して単一のアーカイブに保存されたパッケージ。 • 記述子ファイル（.OVF） • マニフェスト（.MF）および証明書ファイル（オプション）
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。同じホスト システム上で複数の VM が同時に動作できます。

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 Client	vCenter Server または ESXi に任意の Windows PC からリモートで接続できるようにするためのユーザ インターフェイス。vSphere Client のプライマリ インターフェイスを使用して、VM、そのリソース、およびホストの作成、管理、およびモニタを行うことができます。また、VM へのコンソール アクセスも提供します。

Cisco FindIT Network Management のシステム要件

Cisco FindIT Network Management は、仮想マシン イメージとして配布されます。FindIT Network Probe を実行するには、お使いの環境が以下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 5.0.2 以降
  - VMWare：以下のいずれか
    - ESXi バージョン 5.5 以降
    - Fusion バージョン 7 以降
    - Workstation バージョン 12 以降
- CPU64 ビット インテル アーキテクチャ×1
- メモリ512MB
- ディスク領域2GB

FindIT Network Probe 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 バージョン 9
- Google Chrome バージョン 52
- Microsoft Edge バージョン 38

- Microsoft Internet Explorer バージョン 11
- Mozilla Firefox バージョン 48

（注） Safari を使用する場合は、FindIT Network Probe によって提示される証明書が [常に信頼] に設定されていることを確認してください。そうでないと、[ディスカバリ] や [ダッシュボード] など、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します。これは、Safari Web ブラウザの制限です。

FindIT Network Probe で監視およびアクセスするには、ネットワーク デバイスが次の要件を満たしている必要があります

- FindIT Network Probe が動作している PC と同じサブネットに存在するか、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筆必要があります
- Bonjour サービスが有効な Cisco 100 から 500 シリーズのデバイスであることが必要です

第 2 章

はじめに

この章の内容は、次のとおりです。

FindIT Network Probe のインストール

FindIT Network Probe のインスタンスは、ネットワーク内の管理が必要なサイトごとに必要です。Probe はネットワークを検出し、Cisco 100 から 500 シリーズ ネットワーク デバイスをモニタおよび管理するために使用できる単一のインターフェイスを提供します。

FindIT Network Probe は仮想マシン イメージとして提供され、Distributed Management Task Force の Open Virtualization Format (OVF) と、zip 圧縮された Microsoft Hyper-V 仮想マシンの両方でパッケージ化されています。これらの各展開手順について以下のセクションで説明します。

（注） FindIT Network Probe 仮想マシンのネットワーク インターフェイス カードは、1 つ以上のネットワーク デバイス用の管理インターフェイスが含まれている VLAN にブリッジされている必要があります。Probe が 1 つ以上のネットワーク デバイスに直接接続されていない場合、ネットワークを完全に検出できません。

VirtualBox を使用したインストール

1. FindIT Network Probe ova ファイルをダウンロードするため、*www.cisco.com/go/findit* を参照し、[サポート] ペインの [ソフトウェアのダウンロード] リンクを選択します。
2. VirtualBox を開き、[File] > [Import Appliance...] を選択します。

3 プロンプトに従い、インポートするアプライアンス用のダウンロード済みファイルを選択してあることを確認します。

4 ネットワーク アダプタ 1 が有効になっており、ホスト マシン上の正しい物理インターフェイスにブリッジされていることを確認します。

5 仮想マシンを起動します。

VMWare を使用したインストール

1 FindIT Network Probe ova ファイルをダウンロードするため、*www.cisco.com/go/findit* を参照し、[サポート] ペインの [ソフトウェアのダウンロード] リンクを選択します。

2 仮想マシンをインポートするための手順を確認するには、お使いの製品の VMWare マニュアルを参照してください。たとえば、VMWare Fusion を使用している場合は、VMWare Fusion アプリケーションを開き、[File] > [Import…] を選択して、プロンプトに従います。

3 ダウンロードした ova ファイルをローカル ディレクトリから選択し、インポート プロセスを続行します。

4 新たに作成した仮想マシンのネットワーク インターフェイスが、ホスト マシン上の正しい物理インターフェイスに接続されブリッジされていることを確認します。

5 仮想マシンを起動します。

Hyper-V を使用したインストール

1 FindIT Network Probe Hyper-V 仮想マシン アーカイブをダウンロードするため、*www.cisco.com/go/findit* を参照し、[サポート] ペインの [ソフトウェアのダウンロード] リンクを選択します。

2 アーカイブを、PC 上の便利な場所に解凍します。

3 Hyper-V Manager を開き、[アクション] > [仮想マシンのインポート] を選択します。

4 プロンプトに従い、ステップ 2 でアーカイブを展開したときに作成したディレクトリを選択してあることを確認します。インポートの種類を選択するときに、VM ファイルをコピー、移動、そのままにするかを検討します。

5 ネットワーク アダプタが、ホスト マシン上の正しい外部ネットワークにマッピングされた仮想スイッチに接続されていることを確認します。

6 仮想マシンを起動します。

（注） Linux Integration Services for Hyper-V の使用は、FindIT Network Probe ではサポートされていません。

Probe ユーザ インターフェイスへのアクセス

以下の手順では、FindIT Network Probe を使用開始する方法を詳しく示します。

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。Bonjour プラグインが追加された Microsoft Internet Explorer、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。

   Microsoft Internet Explorer ブラウザ対応の Bonjour は、Apple の Web サイト http://www.apple.com/bonjour/ からダウンロードできます。
3. 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cisco とパスワードciscoを使用してログオンします。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。
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。

Probe ユーザ インターフェイスの起動

1. Microsoft Internet Explorer や Mozilla Firefox などの Web ブラウザを起動します。
2. [アドレス] フィールドにデフォルトの DHCP 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名cisco とパスワードcisco を使用してログオンします。[ログイン] をクリックします。

   FindIT Network Probe のユーザ インターフェイスが表示されます。
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。

初期設定の実行

Probe が各自の要件を満たすように、以下の設定を行うことができます。

基本的なシステム設定の実行（オプション）

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. [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. 必要に応じて、内部クロックを使用して時刻を維持するように Probe を設定するか、望ましい NTP サーバを指定できます。デフォルトでは、Probe は公開 NTP サーバと時刻を同期します。

コマンド ラインを使用した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 コンソールに接続するか、Secure Shell（SSH）を使用して Probe の IP アドレスに接続します。
2. デフォルトのユーザ名とパスワードcisco を使用してログオンします。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 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。

ユーザの作成とパスワードの変更

初期状態の Probe 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] > [ユーザ管理] に移動します。

2 [ローカル ユーザ] 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] ウィンドウで、使用するユーザ名とパスワードを指定します。また、このユーザが管理者なのかオペレータなのかを指定します。管理者はすべての機能にアクセスできるのに対し、オペレータは [ユーザ管理] の各機能にアクセスできません。

4 [OK] をクリックして、新しいユーザを作成します。

[ユーザ管理] ページで、パスワードの複雑さ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 [管理] > [パスワードの変更] に移動します。

2 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。

3 [保存] をクリックします。

ライセンスの設定

（注） ライセンスの設定は、Probe のインスタンスが 1 つしかなく、Manager コンポーネントがネットワークにない場合に必要です。

現在のバージョンの FindIT Network Management では、ライセンス チェックが実装されていません。しかし、管理対象のネットワーク デバイス数に十分な数のライセンスを確実に所有することは、ユーザの責任です。詳細は、*www.cisco.com/go/findit* にある FindIT Network Manager データシートを参照してください。

デバイス クレデンシャルの設定

FindIT ネットワークがネットワーク デバイスを管理するためには、デバイスへのアクセスを可能に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、まずデフォルトのユーザ名`cisco` とパスワード`cisco`、SNMP コミュニティ`public` を使用してデバイスへのアクセスを試みます。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。検出されたデバイスの総数と、クレデンシャルが必要な検出済みデバイスの数を示すステータス メッセージが表示されます。このメッセージをクリックすると、クレデンシャルが必要なデバイスのリストが表示されます。

2 ユーザ名とパスワードの組み合わせか、SNMP コミュニティをそれぞれのフィールドに入力します。さらなる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] をクリックします。Probe は各クレデンシャルを、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。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。

正常に機能するクレデンシャルが指定されると、Probe はネットワークを検出して [トポロジ] マップを生成します。

電子メール設定の実行（オプション）

FindIT Network 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、電子メールを介して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，（11 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 [管理] > [電子メール設定] 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。

トポロジ マップのカスタマイズ（オプション）

正常に機能するクレデンシャルが指定されると、Probe はネットワークを検出して [トポロジ] 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 [ディスカバリ] > [トポロジ] に移動します。

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。レイアウトに対して行ったすべての変更は永続的です。FindIT Network は、アイコンの位置についてさらなる変更を行いません。

3 [Overlays and Filters] パネルを開き、チェックボックスを使用してマップ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）

装置の位置を文書化するために、サイトのフロアプランをアップロードし、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 [ディスカバリ] 画面で [フロア プラン] 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] 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、デバイス名またはIPアドレスを画面下部の検索ボックスに入力します。入力の最中に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てフロア プランに追加し、正しい場所にデバイスをドラッグします。

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。変更を行うには、ダッシュボード ウィンドウの右上にある [enable edit mode] アイコンをクリックします。

2 レイアウトを変更するには、[ダッシュボードの編集]設定アイコンを選択します。使用する画面とウィジェットに最適なレイアウトを選択します。

3 ダッシュボード内で個々のウィジェットを再配置するには、[change widget location] アイコンを押したままにします。ウィジェットを、レイアウト内の目的の位置にドラッグします。

4 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 [新しいウィジェットの追加] □ アイコンをクリックし、リストから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、ウィジェットの右上隅にある [remove widget] □ アイコンをクリックします。

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。

6 変更を終えたら、ダッシュボードの上部にある [保存] アイコンをクリックします。

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 [Notification Center] アイコンをクリックして [Event Log] パネルを開きます。

2 [Event Log Setting] アイコンをクリックします。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イベントと、電子メール通知を生成するイベントを制御します。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），（10 ページ）を参照してください。

3 [Panel Setting] アイコンをクリックして、[イベント ログ] パネルの外観を変更します。

4 パネルの外観をカスタマイズします。

FindIT Network Manager との通信（推奨）

以下の手順を使用して、Probe と FindIT Network Manager のインスタンスとの間の通信を確立できます。

1 [管理] > [サイト情報] に移動します。

2 Probe を説明する名前を入力します。この名前は、このサイトを表示するときに Manager のユーザ インターフェイスに表示されます。

3 サイトの場所を指定し、[保存]をクリックします。サイトの住所を適切なフィールドに入力できます。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。

4 [管理] > [マネージャ接続] に移動します。Manager の DNS 名または IP アドレスを入力し、[接続] をクリックします。

5 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。

6 Manager のステータスが [FindIT Network Manager は接続されています] になっていることを確認します。

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用に利用可能なファームウェアがある場合、Probe はユーザに通知します。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グレード] 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、Probe ユーザ 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、デバイス インベントリの表示, （36 ページ）を参照してください。

ネットワークに対するファームウェアのアップグレード

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 [ディスカバリ] ページに移動します。

2 ページ上部の [アクション] 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、Probeユーザ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

Probe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 グループの名前と説明を指定します。

4 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 [キャンセル] アイコンをクリックします。デバイスはデフォルト デバイス グループに移動されします。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。

5 [保存] アイコンをクリックしてグループを作成するか、[キャンセル] アイコンをクリックしてキャンセルします。

システム設定

Probe では、複数のネットワーク デバイスのシステム設定を行うことができます。[システム設定ウィザード]を使用してシステム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できます。[システム設定ウィザード] を使用するには、以下の手順を実行します。

1 [システム設定] > [ウィザード] に移動します。

2 作成する設定プロファイルの説明を入力し、設定を適用する1つ以上のデバイス グループを選択します。

3 [次へ] 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] 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。

7 行った設定を見直します。変更する場合は[戻る]ボタン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。

8 設定の進行状況を表示するには、Probe ユーザ 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。

ワイヤレス ネットワークと VLAN

Probe では、仮想 LAN を作成し、複数のグループに同時に適用できます。

仮想 LAN を作成するには、次の手順を実行します。

1 [ネットワーク] > [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 VLAN 名と VLAN ID を指定します。

4 適用する 1 つ以上のグループを選択します。

5 [保存] アイコンをクリックして VLAN を作成するか、[キャンセル] ボタンをクリックしてキャンセルします。

[仮想 LAN] ページには、ネットワーク内の FindIT Network Management によって設定されていないすべての VLAN の一覧を示す表が表示されます。表示される VLAN の詳細を参照したり、必要に応じて VLAN を削除できます。Probe が何らかの理由で VLAN を編集できない場合、メッセージが表示され、デバイスの管理インターフェイスで VLAN を編集できます。

Probe では、ワイヤレス LAN を作成することもできます。ワイヤレス LAN を作成するには、以下の手順を実行します。

1 [ネットワーク] > [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 SSID 名、VLAN ID、および認証方式を指定します。

4 適用する 1 つ以上のグループを選択します。

5 [保存]アイコンをクリックしてWLANを作成するか、[キャンセル]ボタンをクリックしてキャンセルします。

[ワイヤレス LAN] ページには、ネットワーク内の FindIT Network Management によって設定されていないすべての SSID の一覧を示す表が表示されます。表示される SSID の詳細を参照したり、必要に応じてSSIDを削除できます。Probeが何らかの理由でSSIDを編集できない場合、メッセージが表示され、デバイスの管理インターフェイスで SSID を編集できます。

デバイス設定のバックアップ

Probe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 コンフィギュレーション] 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、Probe ユーザ 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 コンフィギュレーション] 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. [ディスカバリ] ページに移動します。
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 コンフィギュレーション] 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、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、Probe ユーザ 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 3 章

FindIT Network Probe の使用方法

この章の内容は、次のとおりです。

Cisco FindIT Network Probe GUI の使用方法

[Home] ウィンドウ

Cisco FindIT Network Probe にログインすると、ホーム ページが表示されます。

図 *1* : *Cisco FindIT Network Probe* のホーム ページ

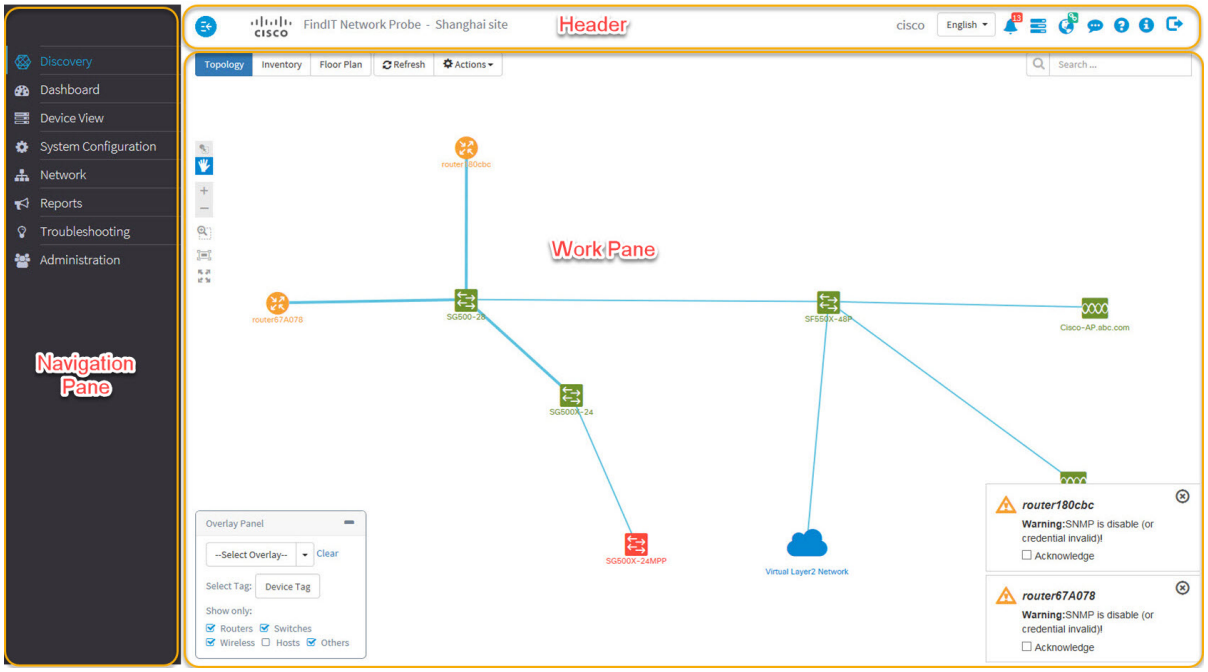

表 *1* : ***Cisco FindIT Network Probe*** のホーム ページ

名前	説明
ナビゲーション ペイン	Cisco FindIT Network Probe の機能へのアクセスを提供します。
作業ペイン	機能インターフェイスが表示される領域です。 **ナビゲーション**ペインでオプションをクリックすると、対応するウィンドウがこの領域に表示されます。
ヘッダー バー	ヘッダーツールバーには以下のオプションが含まれています。 • ナビゲーション ペインを展開および折りたたむためのトグル ボタン • Probe のサイト名を含むヘッダー テキスト • アプリケーションにログインしたユーザのユーザ名 • 言語選択ドロップダウン • 通知、フィードバック、状況依存ヘルプ、ログアウトなどの機能のための一連のアイコン

ナビゲーション ペインのオプション

ナビゲーション ペインには、Cisco FindIT Network Probe 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 *2* : ナビゲーション ペインのオプション

アイコン	名前	説明
	ディスカバリ	FindIT Network Probe によって検出されたネットワーク デバイスのさまざまなビューが含まれています。ビューとしては、ネットワーク トポロジ、インベントリ ビュー、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 ビューなどがあります。

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、ネットワーク トラフィック レベル、接続されているデバイス数、デバイスの全体的な稼働状況をモニタできます。
	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。
	システム設定	[システム設定] ページでは、ネットワーク デバイスのシステム設定を変更できます。
	ネットワーク	[ネットワーク] ページでは、ネットワーク内の VLAN と WLAN を管理できます。
	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。
	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	[管理] ページでは、FindIT Network Probe ネットワーク アプリケーションの保守を行うことができます。

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 *3*：ヘッダー バーのオプション

アイコン	オプション	説明
	トグル ボタン	ヘッダーの左上に位置：このトグル ボタンは、ナビゲーション ペインを展開または折りたたむために使用します。
	言語選択	このドロップダウン リストでは、ユーザ インターフェイスの言語を選択できます。
	Notification Center	このアイコンには、FindIT Network Probe 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、このガイドのデバイス通知の表示とフィルタリング，（73 ページ）を参照してください。
	Task Status	FindIT Network Probe によって実行される操作のタスク ステータスとタスク履歴。このアイコンをクリックすると、進行中のタスクと完了したタスクが表示されます。
	Feedback	Cisco FindIT Network Probe 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 FindIT Network Probe のオンラインヘルプ ドキュメント。
	About FindIT	Cisco FindIT Network Probe のバージョン情報。

アイコン	オプション	説明
	Manager Status	FindIT Network Manager と Probe の間の接続のステータス。このアイコンをクリックすると、Manager GUI が表示されます。
	ログアウト	FindIT Network Probe からログアウトする場合にクリックします。

第 4 章

ディスカバリ

この章の内容は、次のとおりです。

ディスカバリについて

FindIT Network Probe の [ディスカバリ] ページでは、以下に示すネットワークの複数のビューが提供されています。

- [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
- [インベントリ] ビュー：ネットワーク内のすべての Cisco 100 から 500 シリーズのデバイスの一覧と、モデル ID、ファームウェア バージョン、シリアル番号、IP アドレス、MAC アドレスなどの情報を示す表が表示されます。このビューでは、[トポロジ] ビューで提供されているのと同じ操作を行うこともできます。
- [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

[ディスカバリ] 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以下に示します。

- [更新] ボタン：ネットワークを再検出し、トポロジを更新します
- [アクション] ボタン：このボタンを使用すると、選択したアクションを、ネットワーク内のそのタスクをサポートするすべてのデバイスに対して実行できます。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。[アクション]ボタンでは、インベントリを Cisco Active Advisor（*https://www.ciscoactiveadvisor.com*）にアップロードすることもできます。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

FindIT Network Probe 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現（トポロジ）を構築します。Probeによって収集されるデータには、Cisco 100 から 500 シリーズ 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。Probe は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。ネットワークに、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 デバイスが含まれている場合、FindIT Network 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] マップには、[Overlays & Filters] パネルも含まれています。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、ナビゲーション ペインで [ディスカバリ] をクリックします。[ディスカバリ] ウィンドウが表示され、デフォルトではネットワークの [トポロジ] マップが表示されます。

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 4：トポロジ コントロール

引き出し番号	アイコン名	説明
	Zoom in	[トポロジ] ウィンドウのビューを調整します。ネットワーク ホストとデバイスのビューを最大化するには、メニュー バーの + （プラス）アイコンをクリックします。
	Zoom out	[トポロジ] ウィンドウのビューを調整します。ネットワーク ホストとデバイスのビューを最小化するには、- （マイナス）アイコンをクリックします。
	Zoom by selection	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。
	Fit stage	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。
	Enter full screen mode	画面いっぱいに FindIT Network ユーザ インターフェイスを表示します。

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 5：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	シスコ ワイヤレス アクセス ポイントの表現。デバイス名がアイコンの下に表示されます。
	Cloud	FindIT Network Probe で管理されていないネットアークまたはネットワークの一部を表します。

アイコン	ネットワーク要素	説明
	Links	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。
	ルータ	シスコのルータを表します。デバイス名がアイコンの下に表示されます。
	スイッチ	シスコのスイッチを表します。デバイス名がアイコンの下に表示されます。
	ホスト	デバイスの MAC アドレスが表示されます。

[Overlays & Filters] パネル

このパネルは、[トポロジ] マップの左下に表示されます。

表 *6*：*[Overlays & Filters]* パネル

項目	説明
オーバーレイの選択	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。以下のいずれかのビューを選択できます。 • [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わります。緑色の表示は中程度のトラフィックを表し、大量のトラフィックを示すために赤またはオレンジに変わります。 それぞれの色のしきい値を調整するためのフィールドが設けられています。 • [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。 [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。 • [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。
タグの選択	[タグの選択] ラベルの下のテキスト ボックスにデバイス タグを指定すると、目的とする特定のデバイスの存在を確認できます。このデバイス タグは、選択したデバイスに対して [Detailed Info] パネルで割り当てることができます。タグを指定すると、そのタグに一致するデバイスのみがトポロジに表示されます。
表示のみ: • ルータ • スイッチ • ワイヤレス • Hosts • その他	[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。

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，（33 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 [ディスカバリ] ページで、ツールバーの [トポロジ] をクリックします。

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 [サイト情報] バーの下に、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 7：基本的なデバイス情報

項目名	説明
[基本情報] 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。
ファームウェア バージョン	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	*Media Access Control*（*MAC*）アドレスは、標準化されたデータ リンク レイヤ アドレスであり、特定のネットワーク インターフェイス タイプで必要です。これらのアドレスはデバイスごとに固有かつ一意であり、ネットワーク内の他のデバイスでは使用されません。
シリアル番号	デバイスのシリアル番号。
ステータス	デバイスのオンライン/オフライン ステータス。

項目名	説明
通知バー：通知バーに表示される詳細の種類を以下に示します。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、デバイス通知の表示とフィルタリング，（73 ページ）を参照してください。 すべての通知は、イベントの日付と時刻を指定します。デバイスに対して通知がトリガーされるいくつかのケースを以下に示します。 • デバイスが Probe によって初めて検出された • デバイスのファームウェアの更新が利用できる • デバイスのサポート終了案内が発行されている 通知は、重大度を示すために色分けされています。情報メッセージは緑色のバーで、警告はオレンジ色のバーで、アラートは赤いバーで表示されます。 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。	
アクション バー：詳細は、以下を参照してください。 デバイス アクションの実行，（29 ページ）	

いつでも [基本情報] をクリックしてデバイス情報を表示できます。その後、[デバイス アクション]（レンチ）アイコンをクリックすることで、[デバイスアクション] ダイアログボックスに戻ることができます。また、このダイアログボックスの上部にある青いボタンをスライドさせ、[基本情報] ダイアログボックスと [デバイス アクション] ダイアログボックスを切り替えることもできます。

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容易に実行できます。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] マップで、設定タスク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、ウィンドウの右下隅にある [デバイス アクション] アイコンをクリックします。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	最新のファームウェア アップデートをデバイスに適用できます。Probe はシスコからアップデートをダウンロードし、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	ファームウェア アップグレード ファイルをローカル ドライブからアップロードできます。Probe は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はリブートします。
バックアップ コンフィギュレーション	現在のデバイス設定のコピーを Probe に保存できます。 **1** [バックアップ コンフィギュレーション] をクリックします。 **2** [バックアップ コンフィギュレーション] ウィンドウで、実行するバックアップに対してのメモをテキスト ボックスに追加できます。 （注） このメモは、バックアップが GUI で一覧表示されるときに必ず表示されます。 **3** [Save Backup] をクリックしてこのアクションを完了するか、続行しない場合は [キャンセル] をクリックします。 （注） バックアップの実行中は、このボタンは [保存中...] に変わります。 このアクションが完了すると、通知が表示されます。

構成のリストア	以前バックアップした設定をデバイスに復元できます。 [構成のリストア] をクリックします。[Select configuration backup to apply to ***device name***] ウィンドウが表示されます。 このウィンドウに以下のバックアップ設定オプションが表示されます。 • [バックアップ **デバイス名/**：特定のデバイスを設定するために使用可能なすべてのバックアップが一覧表示されます • [他のバックアップ]：同じ種類または同じ製品 ID の他のデバイスを設定するために使用可能なすべてのバックアップが一覧表示されます • [他の互換性のあるデバイスのバックアップ]：選択したデバイスと互換性がある、シリーズ内の他のデバイスを設定するために使用可能なすべてのバックアップが一覧表示されます （注） 各種のオプションは、デバイスに対して該当するバックアップが使用可能な場合のみ表示されます。 バックアップ設定を行うには、以下の手順を実行します。 **1** [Select configuration backup to apply to ***device name***] ウィンドウで、デバイスに復元するバックアップを選択します。 スクロール バーを使用して使用可能なすべてのバックアップを参照し、対応するオプション ボタンをクリックします。これにより、[構成のリストア] ボタンが有効になります。 **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。 このボタンは [復元中...] に変わり、設定が進行中であることを示します。 完了すると、操作の成功または失敗を示す通知が表示されます。 また、設定ファイルをアップロードすることもできます。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、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。[構成のリストア] をクリックして手順を完了します。
リブート	デバイスを再起動します。 （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。

実行コンフィギュレーションの保存	個別の実行コンフィギュレーションとスタートアップ コンフィギュレーションをサポートしているデバイスの場合、このアクションは現在の実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。これにより、デバイスを次回利グーとしたときに、設定変更が保持されます。

（注） いつでも[基本情報]をクリックしてデバイス情報を表示できます。その後、[デバイスアクション]アイコンをクリックすることで、[デバイスアクション]ダイアログボックスに戻ることができます。また、このダイアログボックスの上部にある青いボタンをスライドさせ、[基本情報]ダイアログボックスと [デバイス アクション] ダイアログボックスを切り替えることもできます。

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 トポロジマップで、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 [Open Device GUI] アイコンをクリックします。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） [Open Device GUI] 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 Probe を通じて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、サイトの外からは Probe のみに直接到達できればよいことになります。

これらの接続は同じホスト（Probe）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 マップで、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 3 個のドットのアイコンをクリックします。

ステップ 3 [Detailed Info] 属性パネルには、以下のカテゴリの下にデバイス情報の完全なリストがあります。

- [概要]：デバイスの完全な詳細を参照できます
- [Port Management]：スイッチ ポートの設定を管理できます

  （注） この情報は、スイッチ ポートのあるデバイスでのみ参照できます。

- [WLAN]：デバイスで設定されているワイヤレス LAN を参照できます

  （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]：このデバイスの未確認の通知の一覧が表示されます
- [コンフィギュレーション]：デバイスのバックアップ コンフィギュレーションの一覧を参照し、コンフィギュレーションの復元、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 コンフィギュレーション操作をサポートしているデバイスでのみ参照できます。

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 [概要] をクリックすると、以下の詳細が表示されます。
これらのパネルの右上隅にある矢印をクリックして、表示を展開または折りたたむことができます。

表 *8*：概要

項目名	説明
概要 > 全般：特定のデバイスの詳細情報の一覧が表示されます	
ホスト名	テキスト ボックス内の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。[保存] をクリックして変更内容を保存します。

項目名	説明
TAG	[TAG] フィールドに任意の英数字を入力し、Enter キーを押すと、このデバイスの新しいタグが作成されます。既存のタグを削除するには、タグの □ をクリックします。[保存] をクリックして変更内容を保存します。 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。タグは、FindIT Network Probeの他の場所で、デバイスのサブセットを表示するようにネットワークのビューを制限するために使用できます。
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。
ファームウェア バージョン	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。
PID VID	製品 ID とバージョン ID。
MAC アドレス	*Media Access Control*（*MAC*）アドレスは、標準化されたデータ リンク レイヤ アドレスであり、特定のネットワーク インターフェイス タイプで必要です。これらのアドレスはデバイスごとに固有かつ一意であり、ネットワーク内の他のデバイスでは使用されません。
シリアル番号	デバイスのシリアル番号。
IP	デバイスの IP アドレス。
[概要] > [ダッシュボード]：このデバイス用の単一のダッシュボード ウィジェットが表示されます。	
タイプ	ドロップダウンをクリックして、表示するウィジェットを選択できます。このオプションには、そのデバイスでサポートされているウィジェットのみが一覧表示されます。ダッシュボード ウィジェットの詳細については、ダッシュボードについて, （41 ページ）を参照してください。
[概要] > [通知]：デバイスに関するすべての通知が表示されます。	

項目名	説明
	通知バーに表示される詳細の種類を以下に示します。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、以下を参照してください。 デバイス通知の表示とフィルタリング，（73 ページ） すべての通知は、イベントの日付と時刻を指定します。デバイスに対して通知がトリガーされるいくつかのケースを以下に示します。 • デバイスが Probe によって初めて検出された • デバイスのファームウェアの更新が利用できる • デバイスのサポート終了案内が発行されている 通知は、重大度を示すために色分けされています。情報メッセージは緑色のバーで、警告はオレンジ色のバーで、アラートは赤いバーで表示されます。 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。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。

ステップ 5 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。デバイスのシリアル番号と PID VID 情報は、画像の右上隅に表示されます。

（注） 操作の詳細については、ポート管理について，（45 ページ）を参照してください。

ステップ 6 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 7 このデバイスの未確認の通知の一覧を表示するには、[イベント] をクリックします。フィルタを使用して、表示されるエントリの数を制限できます。詳細については、デバイス通知の表示とフィルタリング，（73 ページ）を参照してください。

ステップ 8 このデバイスのコンフィギュレーションバックアップを表示および管理するには、[コンフィギュレーション]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 *9*：コンフィギュレーションの詳細

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。
コメント	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。

項目	説明
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。 • [Restore configuration to device]：選択したバックアップをデバイスに復元します • [Save configuration to PC]：バックアップを zip ファイルとして PC 上のローカル ドライブに保存します • [Delete configuration]：バックアップを Probe から削除します

デバイス インベントリの表示

[インベントリ] ウィンドウには、ネットワーク デバイスの完全な一覧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、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するためのアクション ボタンも提供されています。インベントリにアクセスするには、[ディスカバリ] ページで [インベントリ] ボタンをクリックします。以下の表に、表示される情報の詳細を示します。

。

表 *10*：インベントリの詳細

項目	説明
ホスト名	デバイスのホスト名が表示されます。
[タイプ]：	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）。
モデル	デバイスのモデル名。
バージョン	デバイスの現在のファームウェア バージョン。
SN	デバイスのシリアル番号。
MAC	Media Access Control（MAC）アドレスは、標準化されたデータ リンク レイヤ アドレスであり、特定のネットワーク インターフェイス タイプで必要です。これらのアドレスはデバイスごとに固有かつ一意であり、ネットワーク内の他のデバイスでは使用されません。

項目	説明
IP	デバイスの Internet Protocol（IP）アドレス。
アクション	デバイスに対して、以下の操作を 1 つ以上実行できます。 • 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 • 構成のリストア • デバイスの再起動 • 実行コンフィギュレーションの保存 （注） これらの操作の詳細については、以下を参照してください。デバイス アクションの実行, （29 ページ）

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. [ディスカバリ] 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 コントロールのすぐ上にある [フロア プラン] リンクをクリックします。
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 デバイスがある各フロアについてステップ 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. [ディスカバリ] 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. 左下にある検索ボックスを使用し、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てフロア プランに追加します。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。デバイスがフロア プランに追加されると、正しい位置にドラッグできるようになります。
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. [ディスカバリ] 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. [ディスカバリ] 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 コントロールのすぐ上にある [フロア プラン] リンクをクリックします。
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. [ディスカバリ] 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 コントロールのすぐ上にある [フロア プラン] リンクをクリックします。
2. 削除するフロア プランを特定し、フロア プラン名の横にある [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

ダッシュボード

この章の内容は、次のとおりです。

ダッシュボードについて

Cisco FindIT Network Probe 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 パフォーマンスを参照でき、データがグラフィカルな形式で表示されます。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。

- [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
- [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

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 [enable edit mode] アイコンをクリックします。

ステップ2 [新しいウィジェットの追加]アイコンをクリックします。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。選択した新しいウィジェットがダッシュボードに表示されます。

ステップ3 [change widget location] アイコンをクリックしたままにし、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ます。

ステップ4 ダッシュボード ウィンドウの右上にある [save changes] アイコンをクリックし、変更内容を保存します。

ウィジェットの変更

ステップ1 ダッシュボード ウィンドウの右上にある [enable edit mode] アイコンをクリックします。

ステップ2 新しいウィジェットの中のドロップダウン リストを使用して、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。

（注） [デバイス ヘルス] ウィジェットの場合、デバイスがウィジェットに一覧表示されます。

ステップ3 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て、ウィジェットの振る舞いを変更します。

ステップ4 ダッシュボード ウィンドウの右上にある [save changes] アイコンをクリックし、変更内容を保存します。

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 [enable edit mode] アイコンをクリックします。

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。

ステップ3 ダッシュボード ウィンドウの右上にある [save changes] アイコンをクリックし、変更内容を保存します。

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をカスタマイズし、新たにカスタマイズしたダッシュボードに名前を付けることができます。

ステップ 1 ダッシュボード ウィンドウの右上にある [enable edit mode] アイコンをクリックします。

ステップ 2 [ダッシュボードの編集] アイコンをクリックし、ポップアップから希望するレイアウトを選択します。ポップアップ内の各オプションには、そのオプションのウィジェット コンテナのレイアウトを示す図が含まれています。

ステップ 3 各ウィジェットの右上にある [change widget location] アイコンをクリックして、ウィジェットを別のウィジェット コンテナに移動します。クリックしたままにして、新しいコンテナにドラッグします。各コンテナには、複数のウィジェットを含めることができます。

ステップ 4 ダッシュボード ウィンドウの右上にある [save changes] アイコンをクリックし、変更内容を保存します。

第 6 章

ポート管理

この章の内容は、次のとおりです。

ポート管理について

ポート管理は、FindIT Network Probe 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フロントパネル 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、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。

ポート管理には、以下の 2 つの異なるデバイスの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、フロー制御、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）マクロを適用できるインターフェイスです。これらのマクロは、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、[Port Management] でその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、ポートの現在の設定、ステータス、トラフィック カウンタが

[物理] ビューに、Smartport の設定とステータスが [Smartport] ビューに表示されます。ポートの設定を変更するには、[基本情報] パネルの [アクション] ボタンをクリックします。

第 7 章

システム設定

この章の内容は、次のとおりです。

システム設定について

[システム設定] ページでは、一般にネットワーク内のすべてのデバイスに適用される各種のシステム レベル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、時刻管理、DNS リゾルバ、認証のそれぞれについて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 [システム設定] > [ウィザード] に移動します。

2 [グループの選択]画面で、この設定の説明を入力し、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] 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。

時刻の設定

[時刻設定] 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。

時刻設定プロファイルの作成

1 [システム設定] > [時刻設定] 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、この設定の説明を入力し、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[夏時間調整]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] をクリックします。

時刻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 [システム設定] > [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、この設定の説明を入力し、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] 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 [システム設定] > [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、この設定の説明を入力し、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] 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。

第 8 章

ネットワーク

この章の内容は、次のとおりです。

ネットワーク設定について

[Network Configuration] ページでは、ネットワークの仮想 LAN（VLAN）とワイヤレス LAN（WLAN）を定義できます。ネットワーク内で複数の VLAN と WLAN を使用することにより、物理トポロジではなくビジネス ニーズに基づいて、ネットワークを複数の論理的なネットワークに分割することができます。これにより、ネットワークのパフォーマンスとセキュリティが向上します。各 WLAN は 1 つの VLAN に関連付ける必要がありますが、1 つの VLAN には任意の数の WLAN を関連付けることができます。

VLAN 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。ネットワーク内の、Probe で設定されていない既存の VLAN も個別の表に表示されます

仮想 LAN の作成

1. [ネットワーク] > [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. 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 ～ 4095 の範囲の数値であり、ネットワーク内ですでに使用されていないことが必要です。

4 1 つ以上のデバイス グループをドロップダウン リストから選択します。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。

5 [保存] アイコンをクリックします。

VLAN の変更

1 変更する VLAN の横のチェックボックスをオンにし、[編集] アイコンをクリックします。

2 VLAN 設定に必要な変更を加え、[保存] アイコンをクリックします。

VLAN の削除

削除する 1 つ以上の VLAN の横のチェックボックスをオンにし、[削除] アイコンをクリックします。

Probe で作成されていない VLAN の削除

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

（注） VLAN 1 は削除できません。

ワイヤレス LAN の設定

[ワイヤレス LAN] ページでは、環境内のワイヤレス ネットワークを管理できます。ネットワーク内の、Probe 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。

ワイヤレス LAN の作成

1 [ネットワーク] > [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 WLAN を追加します。

3 WLAN のわかりやすい名前と、関連付ける 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。

4 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。

5 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。

6 1 つ以上のデバイス グループをドロップダウン リストから選択します。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。

7 [保存] アイコンをクリックします。

ワイヤレス LAN の変更

1 変更する WLAN の横のチェックボックスをオンにし、[編集] アイコンをクリックします。

2 WLAN 設定に必要な変更を加え、[保存] アイコンをクリックします。

ワイヤレス LAN の削除

1 つ以上のチェックボックスをオンにして削除する WLAN を選択し、[削除] アイコンをクリックします。

（注） WLAN を作成するときに VLAN が自動的に作成された場合、WLAN を削除しても VLAN は削除されません。VLAN は [仮想 LAN] ページで削除できます。

Probe で作成されていないワイヤレス VLAN の削除

検出されたワイヤレス LAN の表で、WLAN の横の [削除] アイコンをクリックするか、複数のチェックボックスをオンにして、削除する複数の WLAN を選択します。場合によっては、特定のデバイスから WLAN を削除できないことがあります。その場合は、デバイス設定を直接変更することが必要です。

第 9 章

レポート

この章の内容は、次のとおりです。

レポートについて

Cisco FindIT Network Probe は、ネットワーク デバイスに関する一連のレポートを生成します。これらのレポートには以下のものが含まれます。

- [サマリー レポート]：ネットワーク デバイスのサマリーの概要を提供します
- [EoX 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示します。
- [メンテナンス レポート]：すべてのデバイス、保証ステータス、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

各レポートの上部にある [検索] ボックスを使用すると、結果をフィルタリングできます。[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す。表に表示される結果は、入力に伴って自動的に更新されます。

各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オンにすると、レポートに含める列を選択できます。

サマリー レポートの表示

サマリー 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 *11*：サマリー レポート

フィールド	説明
ホスト名	デバイスのホスト名。
デバイス タイプ	デバイスの種類。
ファームウェア バージョン	デバイス上で動作している現在のファームウェア バージョンを表示します。
ファームウェアの更新	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。
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。

EoX レポートの表示

EoX 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 *12* : ***EoX*** レポート

フィールド	説明
製品 ID	デバイスの製品 ID またはパーツ番号。
名前	デバイスのホスト名。
デバイス タイプ	デバイスの種類。
現在のステータス	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。
サポートの最終日	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。
製品案内	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。

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 *13* : メンテナンス レポート

フィールド	説明
名前	デバイスのホスト名。
デバイス タイプ	デバイスの種類。
モデル	デバイスのモデル番号。
シリアル番号	デバイスのシリアル番号。
ステータス	デバイスの現在のサポート ステータス。
サポート対象終了日	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。

第 10 章

トラブルシューティング

この章の内容は、次のとおりです。

トラブルシューティングについて

FindIT Network Probe の [トラブルシューティング] ページには、ネットワークの問題を診断するのに役立つツールが用意されています。

[Network Show Tech] はそのようなツールの 1 つであり、ネットワークの診断情報を容易に取得し、解析のためにサポート エンジニアに送信することができます。詳細については、ネットワーク診断情報の取得，（59 ページ）を参照してください。

ネットワーク診断情報の取得

[Network Show Tech] ページでは、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、容易に取得できます。診断情報を取得するには、以下の手順を実行します。

1. [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。次のオプションが選択できます。
   - 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

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。

第 11 章

管理

この章の内容は、次のとおりです。

管理について

FindIT Network Probe の [管理] ページを使用すると、Probe ソフトウェアを管理することができます。以下のページには、各種の管理タスクを実行するためのオプションが含まれています。

- [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、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
- [CAA Credentials]：Cisco Active Advisor に使用するクレデンシャルを指定します

- [ユーザ管理]：FindIT Network へのユーザ アクセスを定義します
- [パスワードの変更]：現在ログインしているユーザのパスワードを変更します
- [サイト情報]：サイトの場所とサイトに関するその他の詳細情報を指定します
- [マネージャ接続]：Probe と FindIT Network Manager を関連付けます
- [電子メール設定]：Probe の電子メールを設定します
- [プラットフォーム設定]：Probe のネットワーク設定を管理します
- [ログ設定]：Probe のシステム ロギングを管理します
- [バックアップと復元]：Probe の設定をバックアップおよび復元します

デバイス グループの管理

FindIT Network Probe 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に適用されます。たとえば、デバイス グループにワイヤレス アクセス ポイント、スイッチ、ルータが含まれている場合、新しいワイヤレス SSID の設定はワイヤレス アクセス ポイントに適用され、スイッチには適応されず、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。

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. グループの名前と説明を入力します。
4. ドロップダウン リストを使用して、グループに追加するデバイスを選択します。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。
5. [保存] アイコンをクリックします。

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のチェックボックスをオンにし、[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。

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。デバイスは[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。

5 [保存] アイコンをクリックします。

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 1つ以上のチェックボックスをオンにして削除するグループを選択し、[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

FindIT Network 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 Probe に必要です。最初にデバイスが検出されると、Probe はデフォルトのユーザ名cisco とパスワードcisco、SNMP コミュニティpublic を使用してデバイスでの認証を試みます。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。

2 [Add New Credential] 見出しの下に、検出されたデバイスの総数と、クレデンシャルが必要なデバイスの数を示すステータス メッセージが表示されます。このメッセージをクリックすると、検出されたデバイスの一覧と、各デバイスに有効なクレデンシャルがあるかどうかを示す表が表示されます。

3 [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。

4 [適用] をクリックします。Probe は各クレデンシャルを、その種類のクレデンシャルが必要な各デバイスに対してテストします。クレデンシャルが有効な場合、そのデバイスに対して後で使用するためにクレデンシャルが保存されます。

5 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4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 検出されたデバイスの表でデバイスに対して表示されている、赤い□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] 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。保存されているクレデンシャルを表示するには、[Show Password] ボタンをクリックします。クレデンシャルを再度非表示にするには、[Hide Password] ボタンをクリックします。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。

CAA クレデンシャルの設定

Cisco Active Advisor（CAA）は、ネットワークの検出とネットワーク インベントリの分析を自動化する、無償のオンライン サービスです。Cisco Active Advisor は、以下の情報を最新に保つことで、ネットワーク管理の全体的なリスクを軽減します。

- 保証とサービス契約のステータス
- Product Security Incident Response Team 通知（PSIRT）やフィールド通知などの製品アドバイザリ
- ハードウェアとソフトウェアのサービス終了マイルストーン

レポートは Web ベースのインターフェイスとセットアップ アラートで表示できます。

FindIT Network Management では、検出したデバイスを CAA に容易にアップロードできます。そのためには、[ディスカバリ] ページで [CAA へのアップロード] アクションを選択します。CAA

クレデンシャルを保存しておけば、データをアップロードするたびにクレデンシャルを入力する必要がなくなり、このプロセスを単純化できます。CAA クレデンシャルを設定するには、以下の手順を実行します。

1 [管理] > [CAA クレデンシャル] に移動します。

2 ユーザ名、パスワード、確認用のパスワードを適切なフィールドに入力します。CAA クレデンシャルは、通常は *Cisco.com* のクレデンシャルと同じです。

3 [保存] をクリックしてクレデンシャルを保存するか、[リセット] をクリックして別のクレデンシャル セットを入力します。

ユーザの管理

[ユーザ管理] ページでは、FindIT Network にアクセスできるユーザを定義したり、それらのユーザに対するパスワード複雑さ要件を実装することもできます。

FindIT Network は、2 種類のユーザをサポートします。それは admin と operator です。管理者は FindIT Network の機能にフル アクセスでき、オペレータはユーザの管理、システム設定のバックアップまたは管理、およびプラットフォーム設定の変更以外のすべてのことが行えます。

FindIT Network Probe を最初にインストールすると、デフォルトの admin ユーザが、ユーザ名とパスワードの両方に `cisco` が設定された状態で作成されます。

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] > [ユーザ管理] に移動します。

2 +（プラス） アイコンをクリックして新しいユーザを作成します。

3 各フィールドに、ユーザ名、パスワード、ユーザの種類を入力します。

4 [OK] をクリックします。

ユーザの変更

既存のユーザを変更するには、以下のようにします。

1 [管理] > [ユーザ管理] に移動します。

2 変更するユーザのチェックボックスをオンにした後、編集 アイコンをクリックします。

3 必要に応じてユーザの種類とパスワードを変更します。

4 [OK] 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、以下のようにします。

1 [管理] > [ユーザ管理] に移動します。

2 削除するユーザのチェックボックスをオンにした後、削除アイコンをクリックします。操作を確認する通知が表示されます。

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、以下のようにします。

1 [管理] > [ユーザ管理] に移動します。

2 必要に応じて [Local User Password Complexity] 設定を変更します。

パスワードの変更

現在ログインしているユーザのパスワードを変更するには、以下のようにします。

1 [管理] > [パスワードの変更] に移動します。

2 現在のパスワード、新しいパスワード、確認用の新しいパスワードを、適切なフィールドに指定します。

3 [保存] をクリックします。

サイト情報の管理

[サイト情報] ページでは、この Probe があるサイトを識別したり、サイトの地理的な場所を指定できます。この情報は、この Probe からの情報を表示するときに、FindIT Network Manager によって使用されます。ID と場所を設定するには、以下の手順を実行します。

1 [管理] > [サイト情報] に移動します。

2 サイトを識別する名前を [名前] フィールドに入力します。

3 サイトの住所をフィールドに入力します。部分的な住所を最初の [場所] フィールドに入力して Enter キーを押すと、マップが更新され指定した場所が表示されます。次に、マップをクリックして目的の場所を指定できます。

4 [保存] をクリックします。

Manager への接続

Probe と Manager の間の接続を確立するには、以下の手順を実行します。

1 [管理] > [マネージャ接続] に移動します。

2 Manager の DNS 名または IP アドレスをフィールドに入力します。

3 [接続] をクリックします。Manager のログイン画面が表示されます。

4 Manager の有効なクレデンシャルを使用してログインします。これにより、Probe が Manager に対して認証され、関連付けが確立されます。

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 FindIT Network によって Probe に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 *14*：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。
Email Encryption	使用する暗号化方式。 オプションには以下のものがあります。 • なし • TLS • SSL
認証	使用する認証方式。 オプションには以下のものがあります。 • なし • Clear text • MD5
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。
電子メールを 1 に送信	通知の送信先となる1つ目の電子メールアドレス。
電子メールを 2 に送信	通知の送信先となる2つ目の電子メールアドレス。

フィールド	説明
送信元電子メール 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、[Test Connectivity] ボタンをクリックします。これにより、テスト用の電子メールが、指定した宛先に生成されます。

ログ設定の管理

[ログ設定]ページでは、Probeがログファイルに保存する情報を制御します。この情報は、FindIT Network Managementの問題を診断するサポートエンジニアが主に関心を持つものであり、サポートエンジニアが必要な設定を提供するのに役立ちます。使用可能な設定には以下のパラメータがあります。

表 *15*：ログ設定

フィールド	説明
ログ レベル	ログに記録する詳細レベル。次のオプションが選択できます。 • [エラー]：エラー レベルのメッセージのみ • [警告]：警告とエラー • [Info]（デフォルト）：情報メッセージ以上 • [Debug]：低レベルのデバッグ メッセージ含むすべてのメッセージ
ログ モジュール	メッセージを保存するモジュール。次のオプションが選択できます。 • [すべて]（デフォルト）：すべてのモジュール • [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 • [ディスカバリ]：デバイス検出イベントとトポロジ検出 • [モニタ]：ダッシュボードのアクティビティ • [NETCONF]：NETCONF および RESTCONF のプロセス • [デバイス設定]：すべてのデバイス設定アクティビティ • [レポート]：レポート生成のためのデータ取得と関連付け • [Show tech]：Network Show Tech 用のデータ収集と処理 • [管理]：Probe の設定および管理操作 必要に応じて複数のモジュールを選択できます。

Probe のログ ファイルは、[Network Show Tech] コンテンツに含まれます。[Network Show Tech] オプションの詳細については、ネットワーク診断情報の取得, （59 ページ）を参照してください。

プラットフォーム設定の管理

Probe のネットワーク設定を変更するには、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. 表示されたフィールドに、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を生成したり電子メールを送信したりするときに、Probe を識別するために使用されます。
3. IPv4 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。
4. 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。
5. [保存] をクリックします。

Probe 設定のバックアップと復元

ディザスタ リカバリのためや、Probe を新しいホストに容易に移行するために、Probe 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。

バックアップを行うには、以下の手順を実行します。

1. [管理] > [バックアップと復元] 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、[バックアップ]ボックスの[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] 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。

Probe に設定バックアップを復元するには、以下のようにします。

1. 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、[復元] ボックスの [パスワード] フィールドに入力します。

2 バックアップ ファイルを PC からアップロードし、Probe に設定を復元するには、[アップロードと復元] をクリックします。

第 12 章

通知

この章の内容は、次のとおりです。

通知について

FindIT Network Probe は、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、ホームページ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はログに表示されなくなります。

サポートされる通知

以下の表に、FindIT Network でサポートされている通知の一覧を示します。

表 *16*：ログ設定

イベント	レベル	説明	自動的にクリアされるか
デバイス通知			
デバイスが検出されました	情報	新しいデバイスが検出されたか、オフラインデバイスが再検出されました。	いいえ

イベント	レベル	説明	自動的にクリアされるか
到達不可能なデバイス	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接続が回復したとき）
必要なデバイス クレデンシャル	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（Probe が認証されたとき）
SNMP が無効になっています	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 オフライン	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）
重大なヘルス	警告	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）
無効化された Web サービス	警告	web サービス API 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）
シスコ サポート通知			
使用可能な新しいファームウェア	情報	新しいバージョンのファームウェアが cisco.com で入手できます	はい（デバイスが最新版にアップデートされたとき）
サポート/販売終了通知	警告	デバイスのサポート終了案内が見つかりました。	いいえ
メンテナンス有効期限	警告	デバイスは保証対象外であり、現在有効な保守契約が結ばれていません。	いいえ

デバイス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の通知を表示するには、以下の手順を実行します。

ステップ 1 [Home] ウィンドウで、グローバル ツールバーの右上隅にある [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。
発生した通知は、[イベント ログ] ダイアログボックスのアイコンの下に一覧表示されます。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：マイナー（緑色の八角形のアイコン）
- 警告：メジャー（オレンジ色の三角形のアイコン）
- アラート：クリティカル（赤い三角形のアイコン）

ステップ 2 [イベント ログ] ダイアログボックスで、以下のアクションを実行できます。

- 通知の確認：イベントのチェックボックスをオンにして、通知を確認します。表示内のすべてのイベントを確認するには、[すべて確認] 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。

ステップ 3 [フィルタ] アイコンをクリックして [フィルタ] パネルを開きます。以下の表に示す詳細を指定します。

表 *17* : *[フィルタ]* パネル

フィールド	説明
イベントの表示：終了：	通知を表示する時刻と日付の範囲。
重大度	表示する通知の重大度。以下のいずれかになります。 • 情報 • 警告 • アラート
イベント タイプ	表示する通知のイベント タイプ。たとえば、サポート終了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 [サポート終了] を選択します。
デバイス	通知を表示するデバイス。

フィールド	説明
確認済みのすべての通知を表示するには、ウィンドウの [確認済みイベントを含む] チェックボックスをオンにします。	

ステップ 4 [イベントログ] ウィンドウで使用できる追加オプションの一部を以下に示します。これらのアイコンは、このウィンドウの右上隅にあります。

- [Event Log Setting]：このアイコンをクリックすると、[イベント設定] ウィンドウが表示されます。特定のイベント タイプについて、[ポップアップ通知] や [電子メール] 設定などの適切なオプションのチェックボックスをオンにできます。システムは、この設定に基づき、イベントが発生したときに通知をポップアップしたり、電子メールを送信します。[保存] をクリックして設定を保存するか、[デフォルトの復元] をクリックしてデフォルト設定を復元します。
- [Panel Setting]：このアイコンは、パネル設定を変更し、画面の表示を調整して見やすくする場合にクリックします。以下の表に、このオプションの詳細を示します。

表 *18*：通知センター - パネル設定

フィールド	説明
Icon Opacity	画像アイコンに設定する不透明度。
Panel Opacity	表示パネルに設定する不透明度。
パネル高さ	パネルの高さ（ピクセル単位）。
パネル幅	パネルの幅（ピクセル単位）。
[保存] をクリックして設定を保存するか、[リセット] をクリックしてデフォルト値を復元します。	

（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。

第 13 章

よく寄せられる質問

この章では、Cisco FindIT Network Management 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. FindIT Network Management ではどの言語がサポートされていますか。

A. FindIT Network Management 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; シンプル ネットワーク管理プロトコル）
- RESTCONF（*https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/* を参照）

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 アドレス範囲を積極的にスキャンすることはしません。特定のネットワーク プロトコルのパッシブ モニタリングを組み合わせて使用し、ネットワーク デバイスに積極的に情報を問い合わせます。

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. 以下の表に、FindIT Network Manager が使用するプロトコルとポートの一覧を示します。

表 *19*：*FindIT Network Manager* - プロトコルとポート

ポート	方向	プロトコル	用途
TCP 22	インバウンド	SSH	Manager へのコマンドライン アクセス
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
TCP 1069	インバウンド	NETCONF/TLS	Probe と Manager の間の通信
TCP 9443	インバウンド	HTTPS	Probe GUI へのリモート アクセス
TCP 50000 ～ 51000	インバウンド	デバイス依存	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. 以下の表に、FindIT Network Probe が使用するプロトコルとポートの一覧を示します。

表 *20* : ***FindIT Network Manager*** **- プロトコルとポート**

ポート	方向	プロトコル	用途
TCP 22	インバウンド	SSH	Probe へのコマンドライン アクセス
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
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。
TCP 10000 ～ 10100	インバウンド	デバイス依存	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
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

ポート	方向	プロトコル	用途
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デフォルトのクレデンシャルを使用してデバイスにアクセスしようとします。このとき、ユーザ名とパスワード`cisco`か、SNMP コミュニティ`public`が使用されます。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 または Manager のコンソールにログインし、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@FindITProbe:~# recoverpassword
Are you sure? (y/n) y
Reset the cisco account to default password
cisco@FindITProbe:~#
```

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。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 プロトコルが有効になっていれば、必ずそれ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。

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 Management 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。

A. Access Error:Request Entity Too Large

HTTP Header Field exceeds Supported Size

A. 異なるデバイスと多数のリモート アクセス セッションを実行した後、ブラウザには Probe 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. Manager はオペレーティング システムに CentOS 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、CentOS 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 yum -y update` を実行します。システムを新しい CentOS 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もの以外の追加パッケージをインストールしてはなりません。

Q. Manager で Java を更新するにはどうすればよいですか。

A. Java に対するアップデートは Oracle からダウンロードし、以下のコマンドを使用して手動でインストールします。

新しい Java パッケージを Manager に直接ダウンロードするには、以下の手順を実行します。

```
curl -L -O -H "Cookie: oraclelicense=accept-securebackup-cookie"
-k http://download.oracle.com/otn-pub/java/jdk/<version>-<build>/jre-<version>-linux-x64.rpm
```

例：

```
curl -L -O -H "Cookie: oraclelicense=accept-securebackup-cookie"
-k “http://download.oracle.com/otn-pub/java/jdk/8u102-b14/jre-8u102-linux-x64.rpm”
```

アップデートされた Java バージョンをインストールするには、以下の手順を実行します。

1. コマンド sudo yum –y remove jre1.8.0_102 を実行して古いバージョンを削除します
2. コマンド sudo yum –y localinstall jre-<version>-linux-x64.rpm を使用して新しいバージョンをインストールします

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. Probe はオペレーティング システムに OpenWRT を使用しています。含まれているパッケージは、opkg ツールを使用して更新できます。たとえば、システム上のすべてのパッケージを更新するには、コンソールに cisco ユーザでログインし、コマンド update-packages を入力します。必要に応じて、カーネルのアップデートが Probe の新しいバージョンの一部としてシスコから提供されます。シスコから提供される仮想マシン イメージに含まれているもの以外の追加パッケージをインストールしてはなりません。