デバイスの管理

この項では、IoT FND でデバイスを管理する方法について説明します。次の項目を取り上げます。

- ルータの管理
- エンドポイントの管理
- ヘッドエンド ルータの管理
- サーバの管理
- 共通のデバイス操作
- ルールの設定
- デバイスの設定
- ゲスト OS の管理
- ワーク オーダーの管理
- デバイス プロパティ

デバイスをモニタ、追加、削除したり、デバイス設定以外の他のデバイス管理を実行するには、IoT FND の次のページを使用してします。

- FAR およびエンドポイント（ME）を使用するには、[Field Devices] ページ（[Devices] > [Field Devices]）を使用します。
- HER を使用するには、[Head-End Routers] ページ（[Devices] > [Head-End Routers]）を使用します。
- データベースおよび NMS サーバを使用するには、[Server] ページ（[Devices] > [Servers]）を使用します。
- ルータのデバイス プロパティおよび ME を設定するには、[Device Configuration] ページ（[Config] > [Device Configuration]）を使用します。

ルータの管理

ルータの管理は、[Field Devices] ページ（[Devices] > [Field Devices]）で行います。デフォルトで、ページは [Default] ビューでデバイスを表示します。この項では、次のトピックについて取り上げます。

- ルータの各ビューの使用
- ワーク オーダーの作成
- ルータ フィルタの使用
- ルータ メッシュ キーの更新
- Cisco C819 および Cisco IR829 ISR の組み込みアクセス ポイントの管理
- ルータ設定グループの表示
- ルータ ファームウェア グループの表示
- ルータ トンネル グループの表示

ルータの各ビューの使用

ユーザ設定(「ユーザ プリファレンスの設定」を参照)で [Default to map view] を選択していない限り、[Field Devices] ページはデフォルトでデバイスの基本的なプロパティを含む [List] ビューで表示されます。メイン ペインにタブを表示するには、[Browse Devices] ペイン(左ペイン)でルータまたはルータ グループを選択します。選択したルータ(1 つまたは複数)により表示されるタブが決まります。

(注)以下は、表示可能なタブです。

- Cellular-CDMA
- Cellular-GSM
- Config
- DHCP Config
- デフォルト
- Ethernet Traffic
- ファームウェア
- LoRaWAN
- Mesh
- Mesh Config
- 物理
- Tunnel
- WiMAX

上記タブのビューに、それぞれ異なるデバイス プロパティ セットが表示されます。たとえば、[Default] ビューにはデバイスの基本的なプロパティが表示され、[Cellular-GSM] ビューにはセルラー ネットワークに特有のデバイス プロパティが表示されます。

ルータのビューをカスタマイズする方法については、「デバイス ビューのカスタマイズ」を参照してください。

各ビューに表示されるデバイス プロパティの詳細については、「デバイス プロパティ」を参照してください。

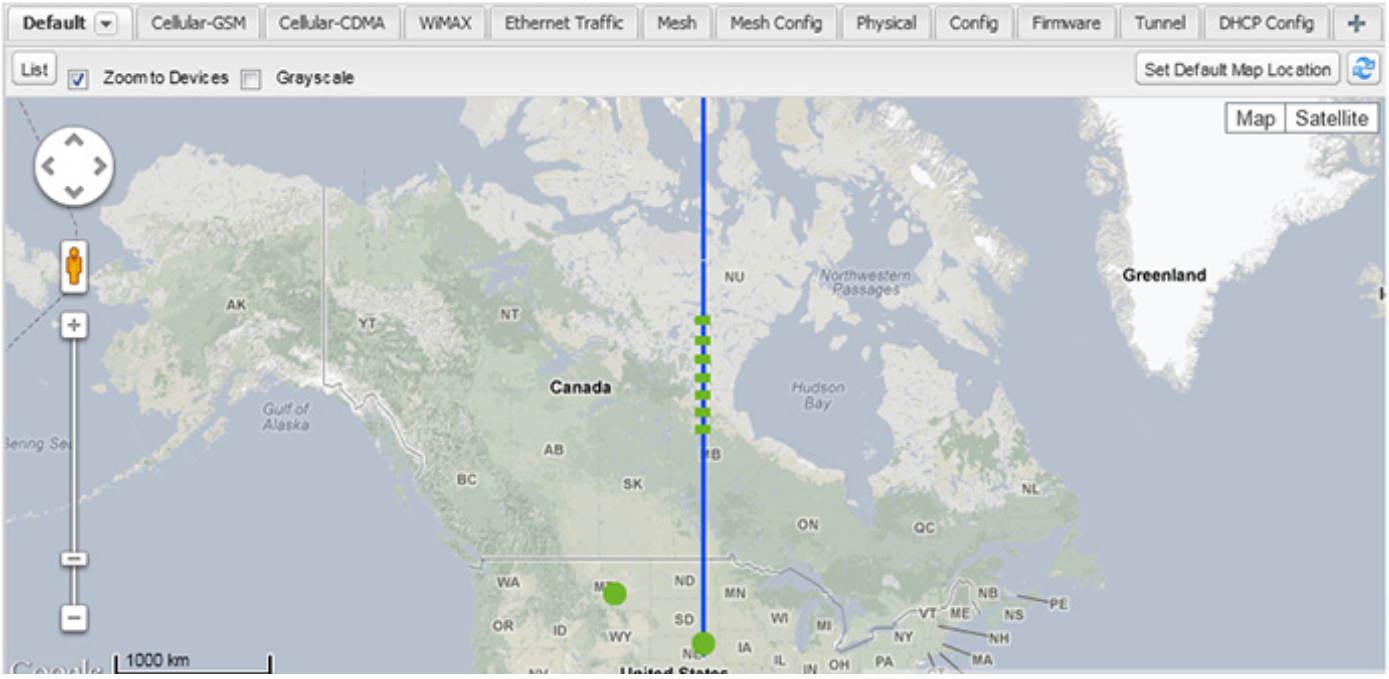
これらのビューで実行する共通アクション(たとえば、ラベルの追加やデバイス プロパティの変更)の詳細については、「共通のデバイス操作」を参照してください。

[Map] ビューでのルータの表示

[Map] ビューにルータを表示するには、[<user>] > [Preferences] で [Enable map] チェックボックスをオンにし、メイン ペインの [Map] タブをクリックします(「ユーザ プリファレンスの設定」を参照)。[Map] ビューで、デバイスをクリックしてから情報ポップアップ ウィンドウを閉じることで、任意の RPL ツリーを表示できます。RPL ツリー接続には、次のように、青色またはオレンジ色の線でデータ トラフィック フローが示されます。

- オレンジ色の線は、リンクがマップの上方向のアップリンク データ トラフィック フローであることを示します。
- 青色の線は、リンクがマップの下方向のダウンリンク データ トラフィック フローであることを示します。

図 1　[Map] ビュー:ダウンリンク データ フローの RPL ツリー



ルータのオペレーティング システムの移行

「OS の移行」の手順を使用し、[Config] > [Firmware Update] ページで、CG-OS から IOS に CGR のオペレーティング システムを移行します。

ワーク オーダーの作成

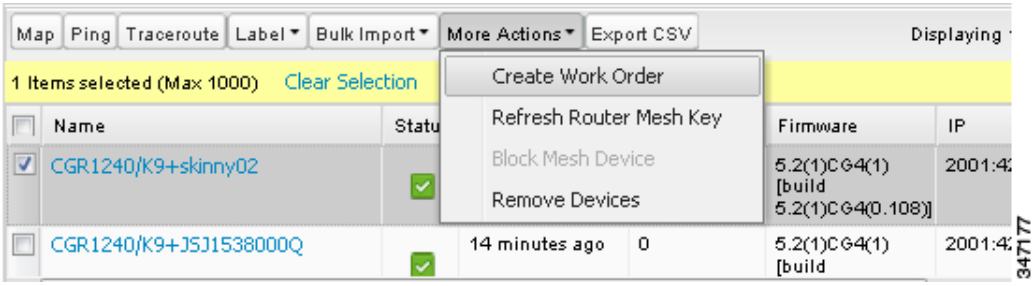
デバイス検査のためにフィールド技術者を配置するには、IoT FND でワーク オーダーを作成します。フィールド技術者は、IoT-DM クライアントを使用して IoT FND に接続し、ワーク オーダーをダウンロードします。

(注) ワーク オーダー機能は、リリース 3.0 以降の Device Manager(IoT-DM)でのみ使用できます。CG-OS インストールのための統合の手順については、『*Cisco Connected Grid Device Manager Installation and User Guide, Release 3.1*』の「*Accessing Work Authorizations*」を参照してください。Cisco IOS のインストール方法については、『*Cisco Connected Grid Device Manager Installation and User Guide, Release 4.0*』、またはそれ以降の同マニュアルを参照してください。

(注) ワーク オーダーを作成するには、ユーザ アカウントで [Work Order Management] 権限が有効になっている必要があります。ロールの管理を参照してください。

CGR のワーク オーダーを作成するには、[Browse Devices] ペインでルータまたはルータ グループを選択し、[Default] ビューで以下の手順を実行します。

1. 障害が発生している CGR のチェックボックスを選択します。
2. [More Actions] > [Create Work Order] を選択します。



[Work Orders] ページが表示されます([Config] > [Device Configuration] > [Work Orders])。IoT FND により、このページの [List of FAR Names] フィールド(カンマ区切りのリスト)に選択した FAR の名前が追加されます。

3. 「ワーク オーダーの作成」の手順に従ってワーク オーダーを作成します。

ワーク オーダーの詳細については、「ワーク オーダーの管理」を参照してください。

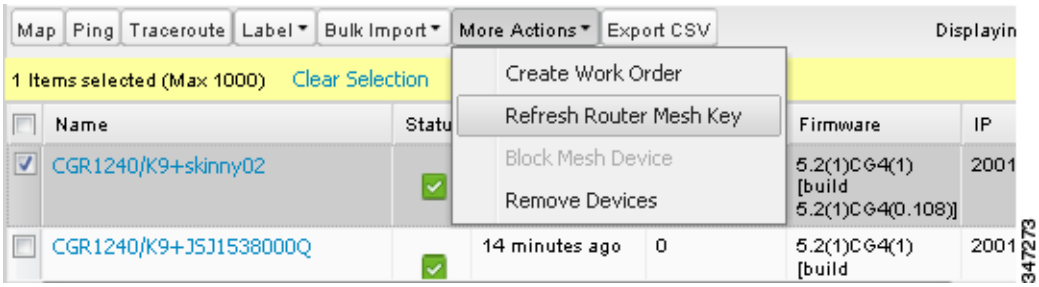
ルータ メッシュ キーの更新

FAR への不正なアクセスが試行されていると思われる場合は、メッシュ キーを更新します。

注意: ルータ メッシュ キーを更新すると、ME が FAR に(自動的に)再登録されるまでの一定期間、ME と FAR の通信が切断される場合があります。

ルータ メッシュ キーを更新するには、[Browse Devices] ペインでルータまたはルータ グループを選択し、[Default] ビューで以下の手順を実行します。

1. 更新する FAR のチェックボックスを選択します。



2. ドロップダウン メニューから、[More Actions] > [Refresh Router Mesh Key] を選択します。
3. [Yes] をクリックして続行します。

Cisco C819 および Cisco IR829 ISR の組み込みアクセス ポイントの管理

IoT Field Network Director では、C819 および IR829 ISR の次の組み込アクセス ポイント(AP)の属性を管理できます。

(注) IoT Field Network Director が AP を管理できるのは、[Autonomous] モードで動作しているときのみです。

- Discovery
- AP の設定
- 定期的なインベントリ収集
- AP のファームウェア アップデート([Autonomous] モードでの動作時)
- SNMP 上のイベント管理

(注)すべての C800 シリーズおよび IR800 ルータに AP が組込まれているわけではありません。C800 ISR の機能マトリクスはこちらを参照してください。IR800 ISR の機能マトリクスはこちらを参照してください。

ルータ フィルタの使用

表示されるルータのリストを変更するには、[Browse Devices] ペインの [ROUTERS] の下の組込みルータのフィルタを使用するか、または [Quick View] ペイン(左ペイン)内の保存済みカスタム検索を使用します。たとえば、すべての稼働中の FAR を表示するには、[Browse Devices] ペインの [ROUTERS] の下の [Up] グループをクリックします。フィルタをクリックすると、[Search Devices] フィールドに対応する検索文字列が挿入されます。たとえば、[ROUTERS] の下の [Up] グループをクリックすると、[Search Devices] フィールドに検索文字列 **status:up** が挿入されます。

ルータ設定グループの表示

[Browse Devices] ペインを使用して、[ROUTERS] の下にリスト表示されているグループのいずれかに属するルータ デバイスを表示します。

ルータ ファームウェア グループの表示

[Browse Devices] ペインを使用して、[ROUTER FIRMWARE GROUPS] の下にリスト表示されているグループのいずれかに属するルータ デバイスを表示します。

ルータ トンネル グループの表示

[Browse Devices] ペインを使用して、[ROUTER TUNNEL GROUPS] の下にリスト表示されているグループのいずれかに属するルータ デバイスを表示します。

エンドポイントの管理

エンドポイントを管理するには、[Devices] > [Field Devices] ページを表示します。デフォルトで、ページは [List] ビューで ME を表示します。この項では、次のトピックについて取り上げます。

- [Default] ビューでのエンドポイントの表示
- [Map] ビューでのメッシュ エンドポイントの表示
- メッシュ デバイスのブロッキング
- メッシュ エンドポイント設定グループの表示
- メッシュ エンドポイント ファームウェア グループの表示

[Default] ビューでのエンドポイントの表示

[Field Devices] ページを [Default] ビューで開くと、IoT FND は、すべての FAN デバイスと基本的なデバイス プロパティをリスト表示します。[Browse Devices] ペインで ENDPOINT デバイスまたはデバイス グループを選択すると、エンドポイントの追加プロパティのビューを表示する次のタブが IoT FND によって提供されます。

- マップ
- Config
- デフォルト
- ファームウェア

- PLC Mesh
- RF Mesh
- セキュリティ
- Cellular Endpoints

これらのビューにはそれぞれ異なるデバイス プロパティ セットが表示されます。たとえば、[Firmware] ビューには、[Hardware ID]、[Firmware Group]、および [FW Uploaded Version] など、ファームウェアのカテゴリに属するデバイス プロパティが表示されます。

ME のビューをカスタマイズする方法については、「デバイス ビューのカスタマイズ」を参照してください。

各ビューに表示されるデバイス プロパティについては、「デバイス プロパティ」を参照してください。

他のデバイスにも適用される、これらのビューでの共通アクション（ラベルの追加やデバイス プロパティの変更など）については、「共通のデバイス操作」を参照してください。

[Map] ビューでのメッシュ エンドポイントの表示

[Map] ビューで ME を表示するには、[<user>] > [Preferences] で [Enable map] を選択し、[Map] タブをクリックします。

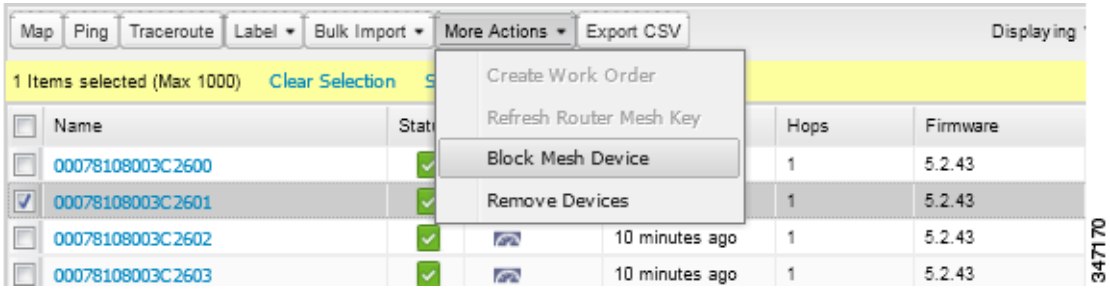
メッシュ デバイスのブロッキング

メッシュ デバイスへの不正なアクセスが試行されていると思われる場合は、メッシュ デバイスを IoT FND へのアクセスからブロックします。

注意: ME をブロックした場合、IoT FND を使用してブロック解除することはできません。ME を IoT FND に再登録にするには、エスカレーションを行って ME 管理者に作業してもらう必要があります。

ME デバイスをブロックするには、[Default] ビューで次の手順を実行します。

1. 更新するメッシュ デバイスのチェックボックスを選択します。
2. ドロップダウン メニューから、[More Actions] > [Block Mesh Device] を選択します。



3. [Confirm] ダイアログボックスで [Yes] をクリックします。
4. デバイスがメッシュ ネットワークに再接続することを防ぐため、NPS サーバからメッシュ エンドポイントを削除します。

メッシュ エンドポイント設定グループの表示

[Browse Devices] ペインを使用して、[MESH DEVICE CONFIGURATION GROUPS] の下にリスト表示されているグループのいずれかに属する ME デバイスを表示します。

メッシュ エンドポイント ファームウェア グループの表示

[Browse Devices] ペインを使用して、[ENDPOINTS] の下にリスト表示されているグループのいずれかに属する ME デバイスを表示します。

産業用ルータの管理

設定テンプレートを使用して、DSCP および raw ソケットの設定を IR509 および産業用ルータに適用できます。

DSCP 設定

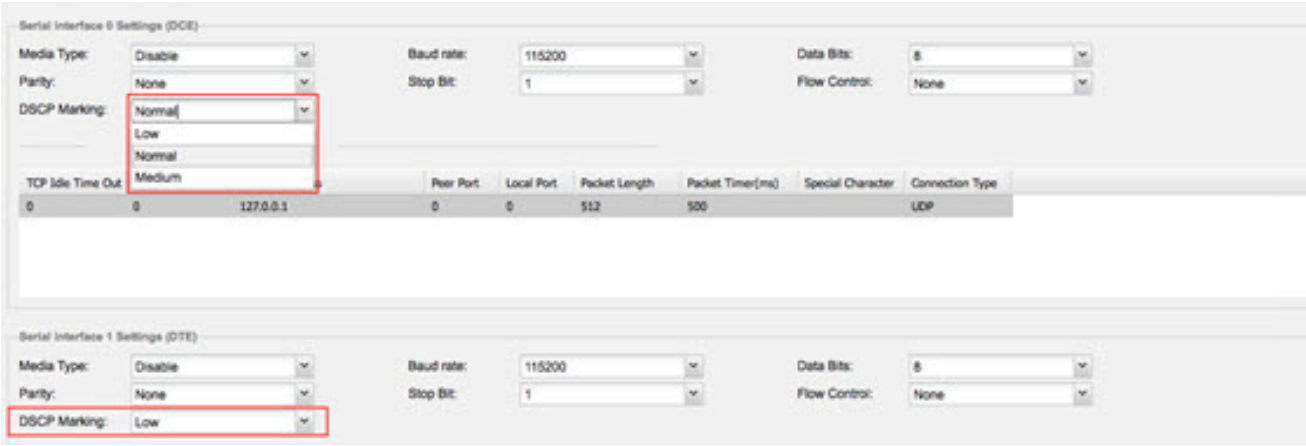
IR509 で DSCP を設定するには次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. 左ペインの [ENDPOINT] の下に表示されているデフォルトの ir500 を選択します。
3. [Edit Configuration Template]（図 2 および図 3）を選択します。

（注）設定オプションの概要については、表 1 を参照してください）。

図 2　　イーサネット インターフェイスでの DSCP マーキングの設定

図 3　　DCE および DTE での DSCP マーキングの設定



設定に関する注意事項：

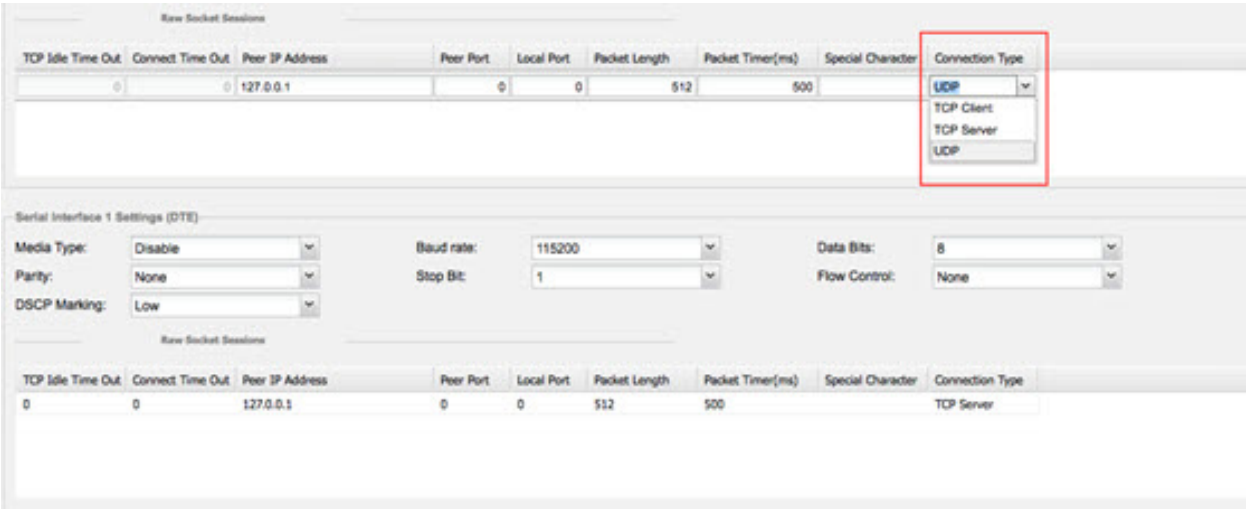
- すべてのインターフェイス（イーサネット、DTE、および DCE）で DSCP（QoS）マーキングを設定してください。オプション：Low Priority (0)、Normal Priority (10)、Medium Priority (18)。
- DSCP はインターフェイスで適用されます。DCE および DTE のデフォルト値は、Low Priority (0) です。イーサネットにはデフォルト値はありません。[Configuration Template] の値を設定していない場合、トラフィックはマーキングされていない状態でフローします。
- DCE および DTE インターフェイスでは、一度に 1 つの raw ソケット セッションのみフローできます。DSCP 値は、全体を通じて変化しません。

raw ソケットの設定

IR509 で raw ソケットを設定するには次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. 左ペインの [ENDPOINT] の下に表示されているデフォルトの ir500 を選択します。
3. [Edit Configuration Template] を選択します。

(注)設定オプションの概要については、表 1 を参照してください)。



設定に関する注意事項:

- UDP ソケットをサポートするために raw ソケットの設定を更新してください。
- シリアル デバイスのビット値を設定してください。値は 1 ～ 4 です。
- デバイスに対する定期的な通知の最小間隔を設定してください。値は 1 ～ 5 分です。

表 1　　IR509 の設定オプション

インターフェイス	Settings
イーサネット	1. [Ethernet Settings] パネルのオプション(および必要な値)は次のとおりです。 ■ Enable Ethernet:無効にします(チェックをはずす) ■ Disable Ethernet on Disconnect:無効にします(チェックをはずす) ■ DSCP Markings:プルダウン メニューから [NONE] を選択します。 2. [MAP-T Settings] パネルのオプションは次のとおりです。 – Default Mapping IPv6 Prefix:0:0:0:0:0:0:0:1 – IPv6 Prefix Length:64

表 1　　IR509 の設定オプション（続き）

インターフェイス	Settings
DCE	[Serial Interface 0 Settings (DCE)] パネルのオプション（および必要な値）は次のとおりです。 ■ Media Type：Disable ■ ボー レート：115200 ■ Data Bits：8 ■ Parity：Normal ■ Stop Bit：1 ■ フロー制御：なし ■ DSCP Marking：Normal
DTE	[Serial Interface 1 Settings (DTE)] パネルのオプション（および必要な値）は次のとおりです。 ■ Media Type：Disable ■ ボー レート：115200 ■ Data Bits：8 ■ パリティ：なし ■ Stop Bit：1 ■ フロー制御：なし ■ DSCP Marking：Low

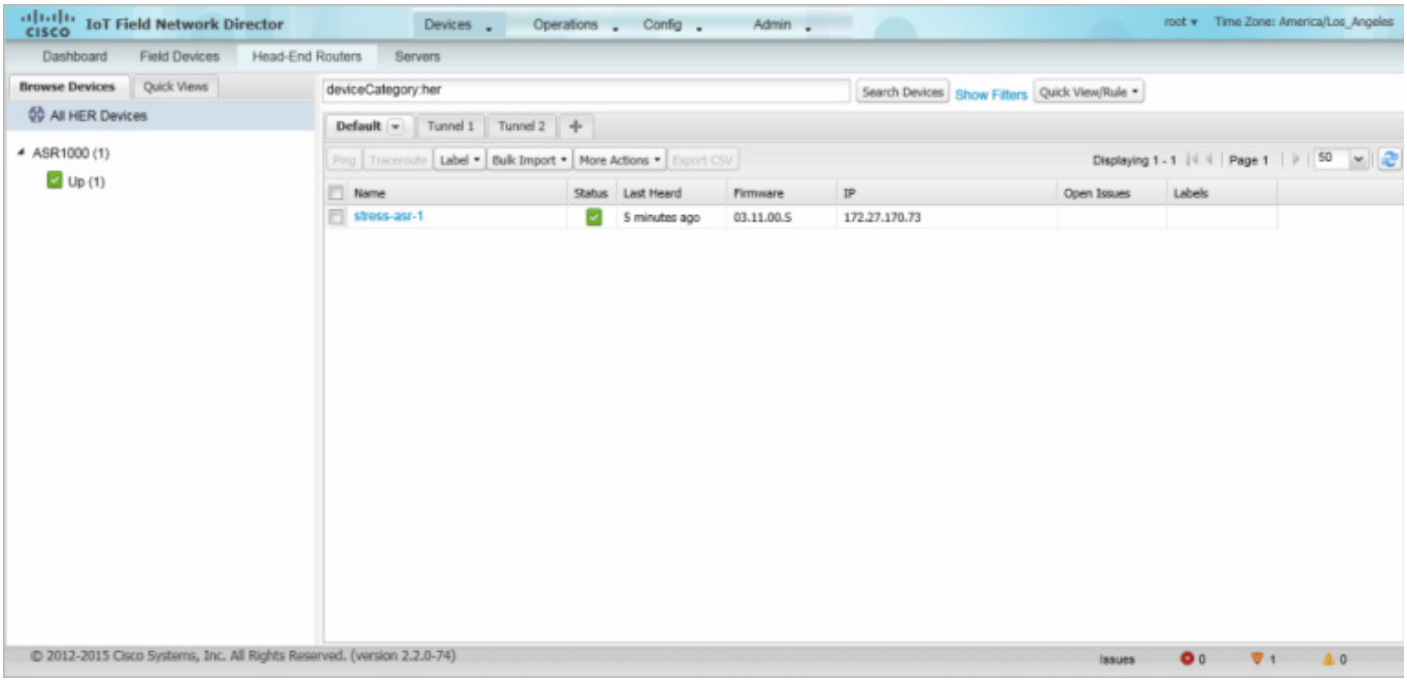
ヘッドエンド ルータの管理

ヘッドエンド ルータ（HER）を管理するには、[Devices] > [Head-End Routers] を選択して、[Head-End Routers] ページを開きます（図 4）。ユーザ設定で [Enable Map] が選択されていない限り、デフォルトで、ページは [List] ビューで HER を表示します。[Head-End Routers] ページを [List] ビューで 開くと、IoT FND は [Default list] ビューを表示します。このビューには、HER デバイスの基本的なプロパティが表示されます。さらに、HER の追加プロパティのビューを表示する次のタブが IoT FND によって提供されます。

- Tunnel 1
- Tunnel 2

これらのビューにはそれぞれ異なるデバイス プロパティ セットが表示されます。これらのビューには、HER トンネルに関する情報が表示されます。

図 4　[Head-End Routers] ページ



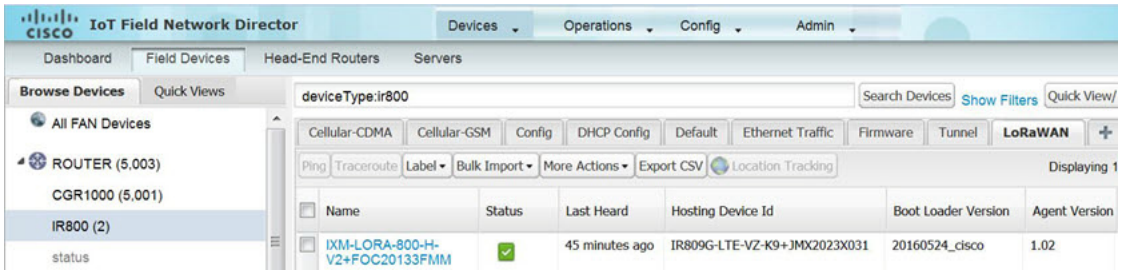
HER のビューをカスタマイズする方法については、「デバイス ビューのカスタマイズ」を参照してください。

各ビューに表示されるデバイス プロパティについては、「デバイス プロパティ」を参照してください。

他のデバイスにも適用される、これらのビューでの共通アクション（ラベルの追加やデバイス プロパティの変更など）については、「共通のデバイス操作」を参照してください。

外部モジュールの管理

ルータなど、Field Devices に接続しているデバイスを管理するには、[Devices] > [Field Devices] を選択します。デフォルトで、ページは [List] ビューですべての認識された FAN デバイスを表示します。



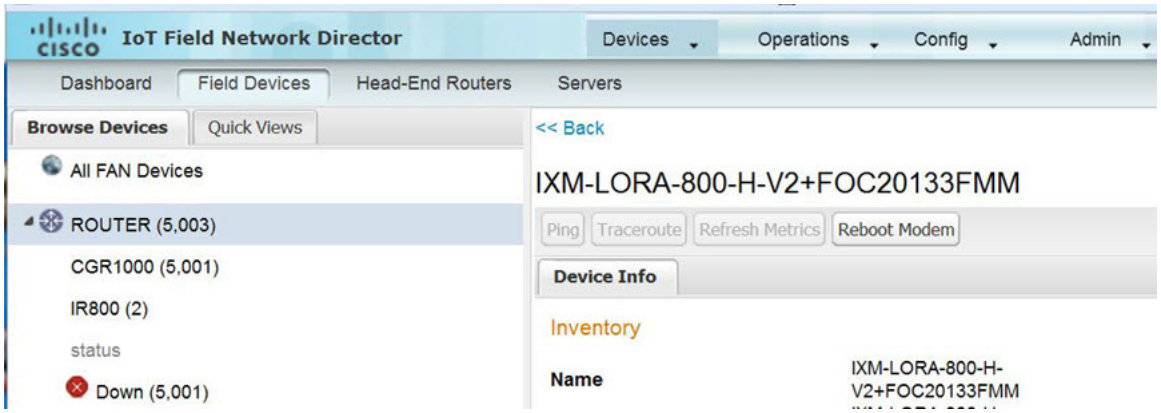
- LoRaWAN

LoRaWAN モジュールの LRR イメージを IR800 ルータにアップロードする方法は 2 つあります。ゼロ タッチ展開（ZTD）時と、オンデマンド設定転送による方法です。

（注）シスコでは、LoRaWAN モジュールの検出をサポートしていません。代わりに、IoT FND は IR800 モジュールとして認識し、Cisco IOS 経由で通信します。

- LoRaWAN モジュールをデバイス リストに表示するには、[Browse Devices] リストで IR800 ルータを選択し、[LoRaWAN] タブを選択します。
- LoRaWAN モジュール上のモデムを再起動するには、次の手順を実行します。

  a. [Name] 列の下の関連の IXM-LORA のリンクをクリックして、以下に示す情報を表示します。



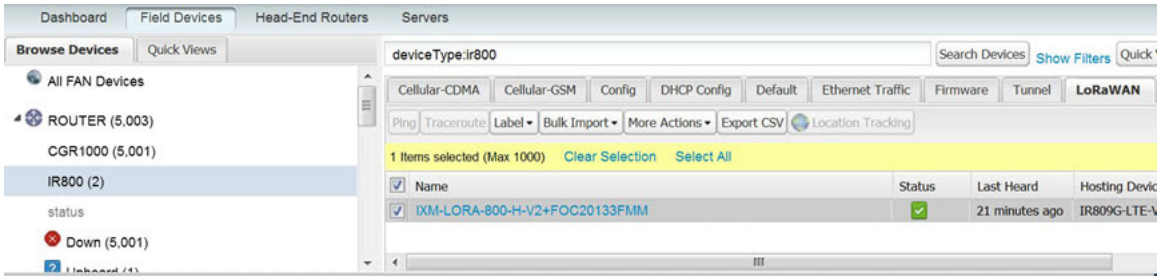
  b. [Reboot Modem] をクリックします。再起動が完了すると、LoRaWAN モジュールの [Device Info] ペインの [Last Reboot Time] フィールドに日付と時刻が表示されます。一度に処理できるモデムの再起動は 1 つだけです。

  [Reboot Modem] の操作により、LoRa モデム再起動開始と LoRa モデム再起動成功の 2 つのイベントが生成されます。

- IR800 ルータ インベントリから LoRaWAN モジュールを削除するには、次の手順を実行します。

  a. [Browse Devices] ペインで、インベントリから無効にして削除する必要がある LoRA モジュールがある IR800 を選択します。

  b. [LoRaWAN] タブを選択し、削除する LoRaWAN モジュールの横にあるチェックボックスをオンにします。



  c. [More Actions] ドロップダウン メニューで、[Remove Devices] を選択します。

サーバの管理

サーバを管理するには、[Devices] > [Servers] を選択して [Servers] ページを開きます。デフォルトで、ページは [List] ビューでサーバを表示します。[Servers] ページを [List] ビューで 開くと、IoT FND は [Default list] ビューを表示します。このビューには、サーバ デバイスの基本的なプロパティが表示されます。サーバに関する情報を取得するには、名前をクリックします。

他のビューを追加するには、「デバイス ビューのカスタマイズ」を参照してください。

各ビューに表示されるデバイス プロパティについては、「デバイス プロパティ」を参照してください。

このビューでの共通アクションについては、「共通のデバイス操作」を参照してください。

NMS サーバの管理

[Browse Devices] ペインで、NMS サーバは、[NMS Servers] の下に表示されます。単一の NMS サーバの導入では、[NMS Servers] の下に 1 つのサーバだけが表示されます。クラスタ導入では、[NMS Servers] の下に複数の NMS サーバが表示されます。リスト ペインのフィルタリングをするには、次の手順を実行します。

- すべての NMS サーバを表示するには、[Browse Devices] ペインで [NMS Servers] をクリックします。
- 稼働中のサーバのみを表示するには、[Up] をクリックします。
- 稼働していないサーバのみを表示するには、[Down] をクリックします。

データベース サーバの管理

[Browse Devices] ペインで、IoT FND データベース サーバは、[Database Servers] の下に表示されます。単一のサーバの導入では、[Database Servers] の下に 1 つのデータベース サーバだけが表示されます。セカンダリ データベースが設定されている場合、同じエントリの下にセカンダリ データベースも表示されます。

- [List] ビューにすべてのデータベース サーバを表示するには、[Browse Devices] ペインで [Database Servers] をクリックします。
- 稼働中のサーバのみを表示するには、[Up] をクリックします。
- 稼働していないサーバのみを表示するには、[Down] をクリックします。

共通のデバイス操作

この項では、IoT FND を使用してデバイスを管理したりデバイスの情報を表示する方法について説明します。次の項目を取り上げます。

デバイスの選択

IoT FND では、[List] ビューを使用して、単一ページまたは複数ページからデバイスを選択できます。デバイスを選択すると、選択しているデバイスのカウントを示す黄色いバーが表示されます。このバーでは、**[Clear Selection]** および **[Select All]** を指定できます。選択できるデバイスの最大数は 1000 です。デバイスを選択するには、次の手順を実行します。

- 全ページにわたるデバイスを選択するには、[Select All] をクリックします。
- 1 つのページにリスト表示されているすべてのデバイスを選択するには、[Name] の横のチェックボックスを選択します。
- 一群のデバイスを選択するには、1 つまたは複数ページで、リスト表示されている個々のデバイスのチェックボックスを選択します。デバイスを選択するたびにカウントが増え、全ページの選択が保持されます。

デバイス ビューのカスタマイズ

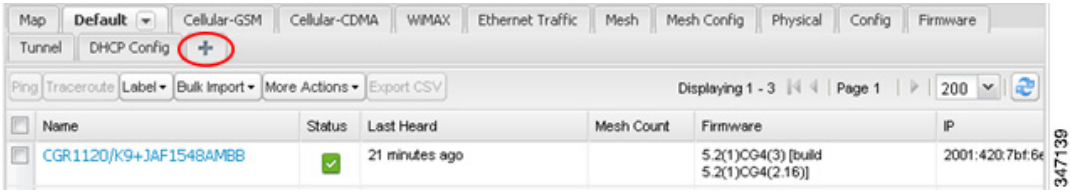
IoT FND では、デバイス ビューをカスタマイズできます。[List] ビューでは、次の操作を実行できます。

- タブを追加および削除する
- 各ビューのカラムに表示するプロパティを指定する（使用可能なプロパティについては、「カテゴリ別デバイス プロパティ」を参照）
- カラムの順序を変更する

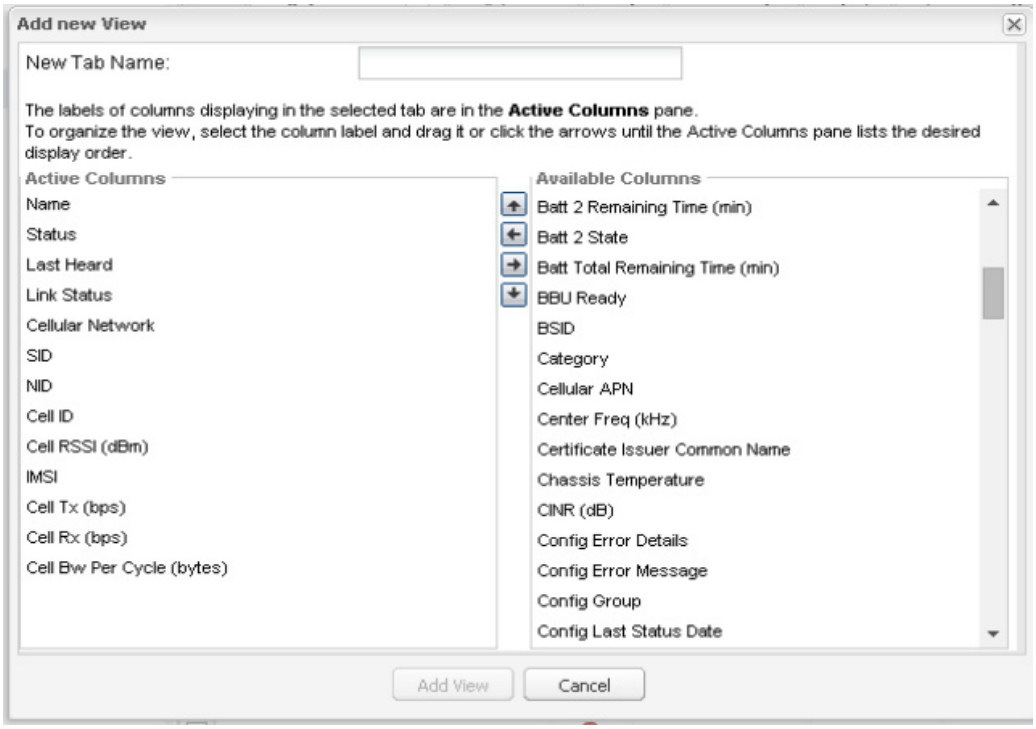
デバイス ビューの追加

[List] ビューで、デバイス ページにデバイス ビューのカスタム タブを追加するには、次の手順を実行します。

1. [+] タブをクリックします。



2. [Add New View] ダイアログボックスに新しいタブの名前を入力します。



3. [Available Columns] リストからプロパティを選択し、左矢印ボタンをクリックするか、またはドラッグして [Active Columns] リスト内に移動することにより、それらのプロパティを [Active Columns] リストに追加します。

   - カラムの順序を変更するには、上矢印または下矢印ボタンを使用するか、またはにドラッグして適切な位置に移動します。
   - [Active Columns] リストからプロパティを削除するには、それらのプロパティを選択し、右矢印ボタンをクリックするか、ドラッグしてリストの外に移動します。

   ヒント:複数のカラム ラベルを選択していずれかのリストに移動するには、Shift キーを使用します。

4. [Save View] をクリックします。

デバイス ビューの編集

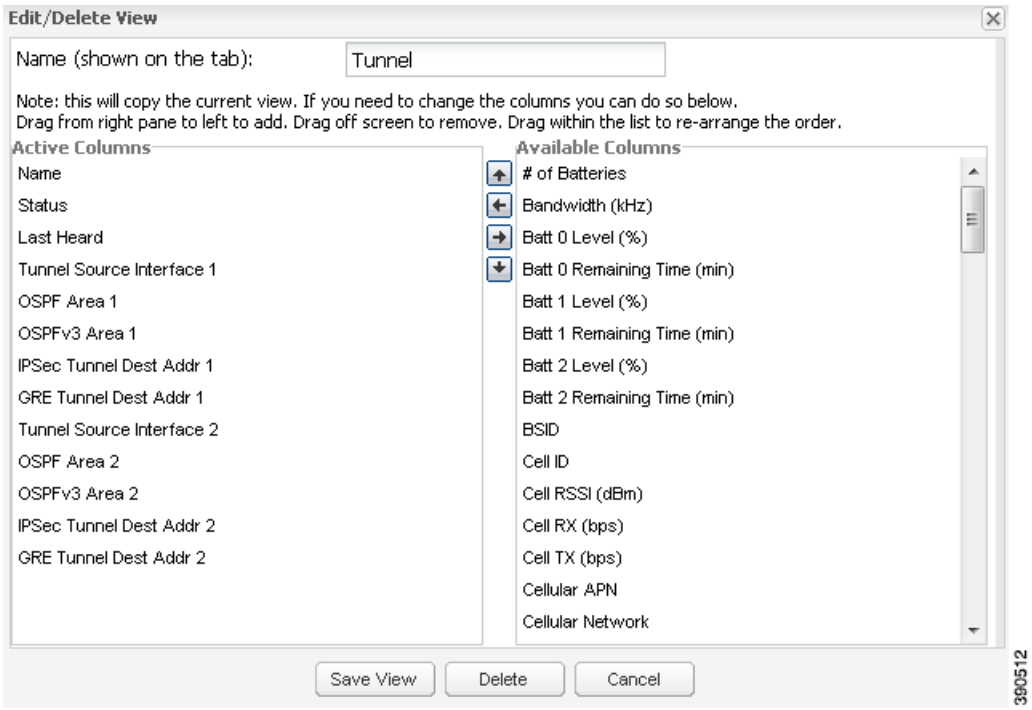
デバイス ビューを編集するには、次の手順を実行します。

1. 目的のタブでドロップダウン矢印をクリックします。
2. [Edit/Delete View] ダイアログボックスで、次の操作を実行できます。

   a. [Active Columns] リストからプロパティを削除するには、それらのプロパティを選択し、右矢印ボタンをクリックするか、ドラッグして [Active Columns] リストの外に移動します。

   b. プロパティを [Active Columns] リストに追加するには、それらのプロパティを [Available Columns] リストから選択し、左矢印ボタンをクリックするか、またはドラッグして [Active Columns] リスト内に移動します。

   c. アクティブなカラムの順序を変更するには、上矢印または下矢印ボタンを使用するか、またはにドラッグして適切な位置に移動します。

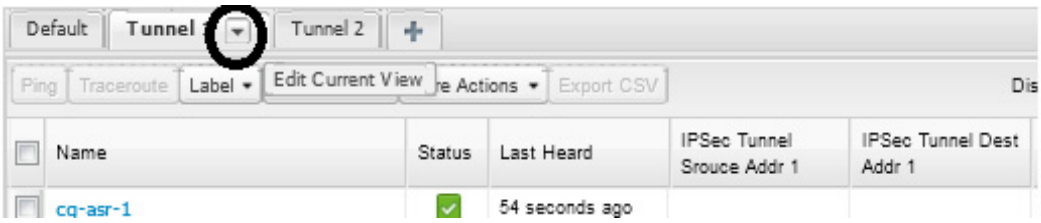


3. [Save View] をクリックします。

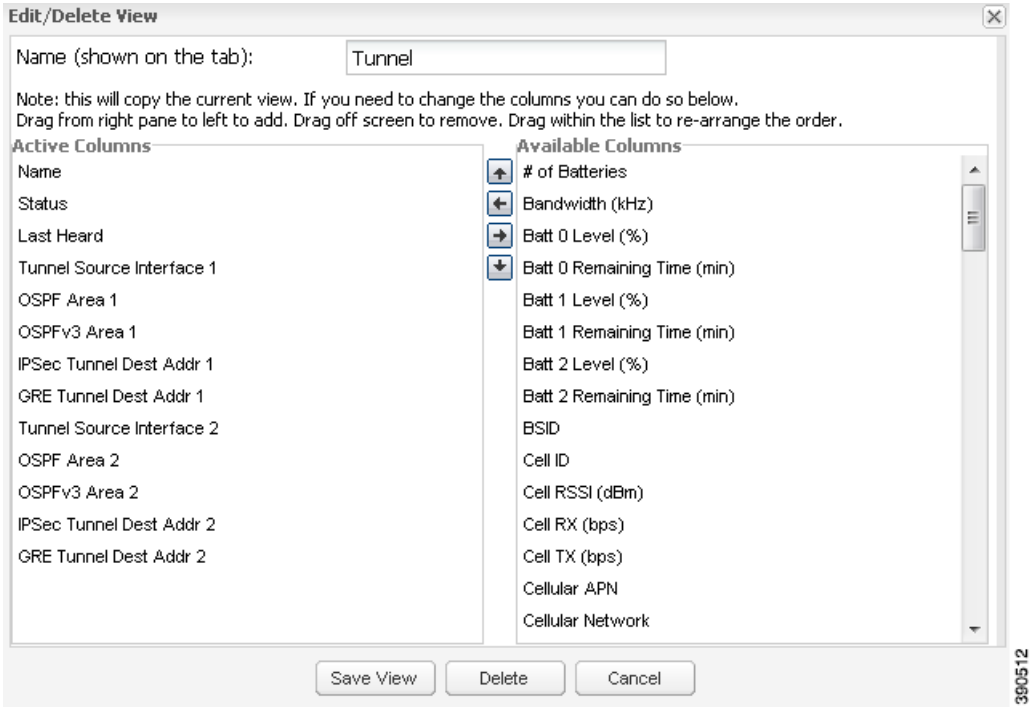
デバイス ビューの削除

デバイス ビューを削除するには、次の手順を実行します。

1. 削除するデバイス ビューのタブで矢印をクリックします。



2. [Edit/Delete View] ダイアログボックスの [Active Columns] ペインで、目的のラベルを選択します。



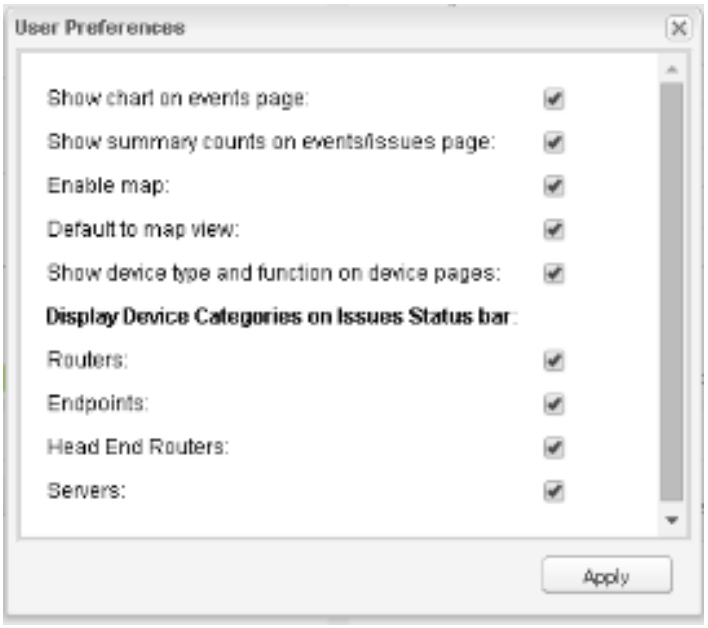
3. [Delete] をクリックします。

[Map] ビューでのデバイスの表示

IoT FND は、地理的な位置に基づいてデバイス情報を視覚化するための [Map] ビューを提供しています。IoT FND は [Map] ビューで地理情報システム（GIS）マップを表示し、GIS マップ サービスを使用して、デバイスの緯度情報と経度情報に基づきマップ上にデバイス アイコンを表示します。この情報がデバイスで定義されていない場合、IoT FND はマップ上にデバイスを表示しません。

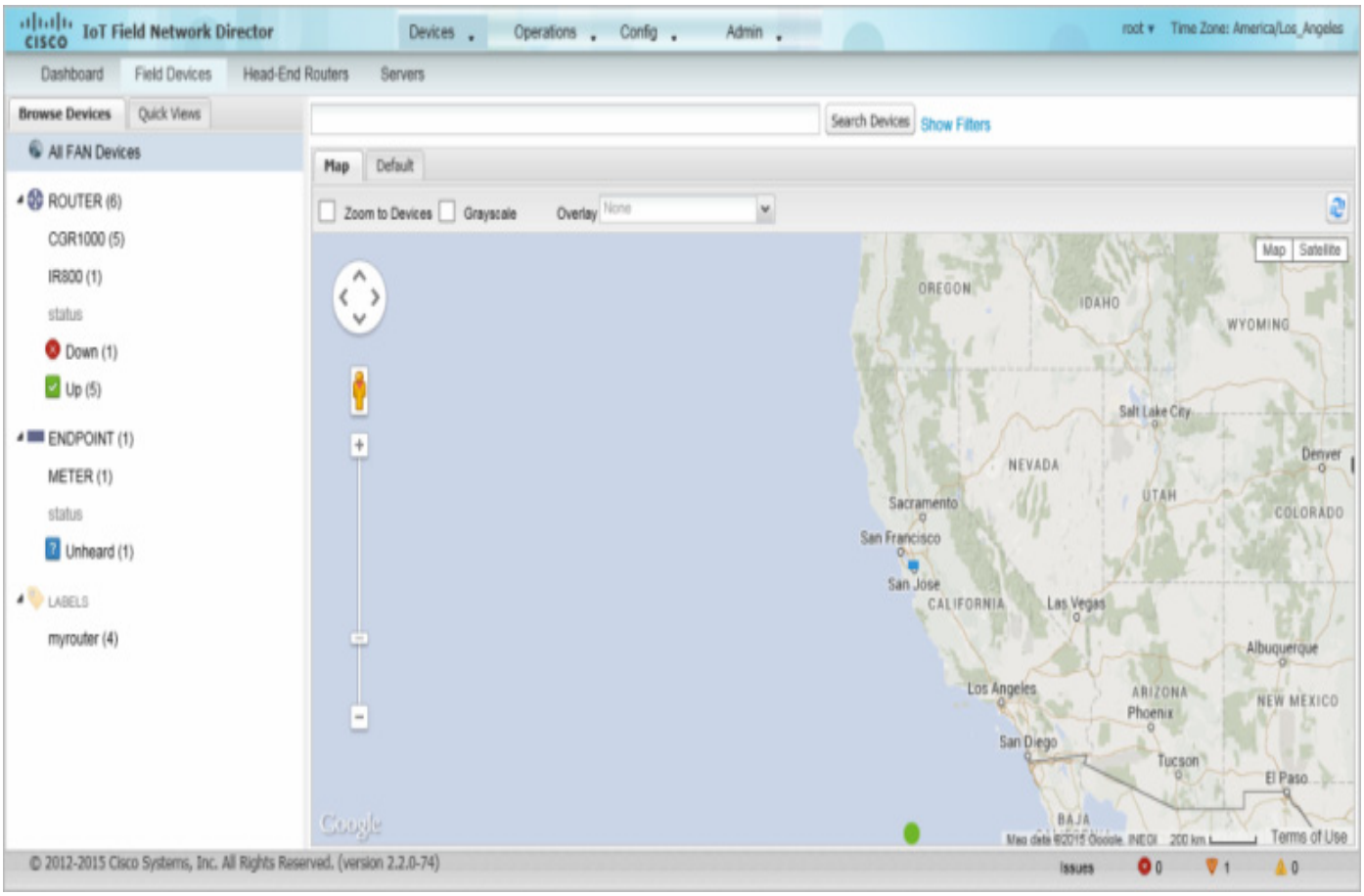
[Map] ビューにデバイスを表示するには、次の手順を実行します。

1. [<user>] > [Preferences] を選択して [Enable map] チェックボックスをオンにし、[Apply] を適用します。

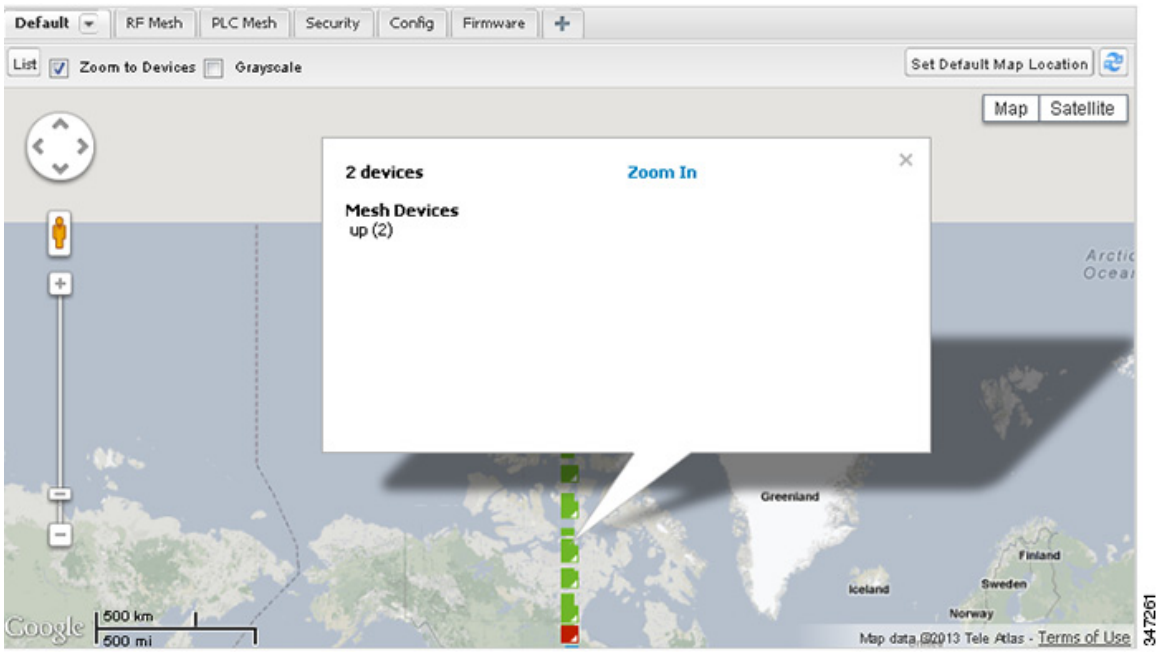


2. [Devices] > [Field Devices] を選択します。
3. [Map] タブをクリックします。

   デフォルトで、IoT FND は、マップ上のデータベースに登録されているすべてのデバイスを表示します。マップのズーム レベルおよびデバイス カウントによっては、個々のデバイス アイコンが表示されない場合があります。代わりに、IoT FND はデバイス グループ アイコンを表示します。



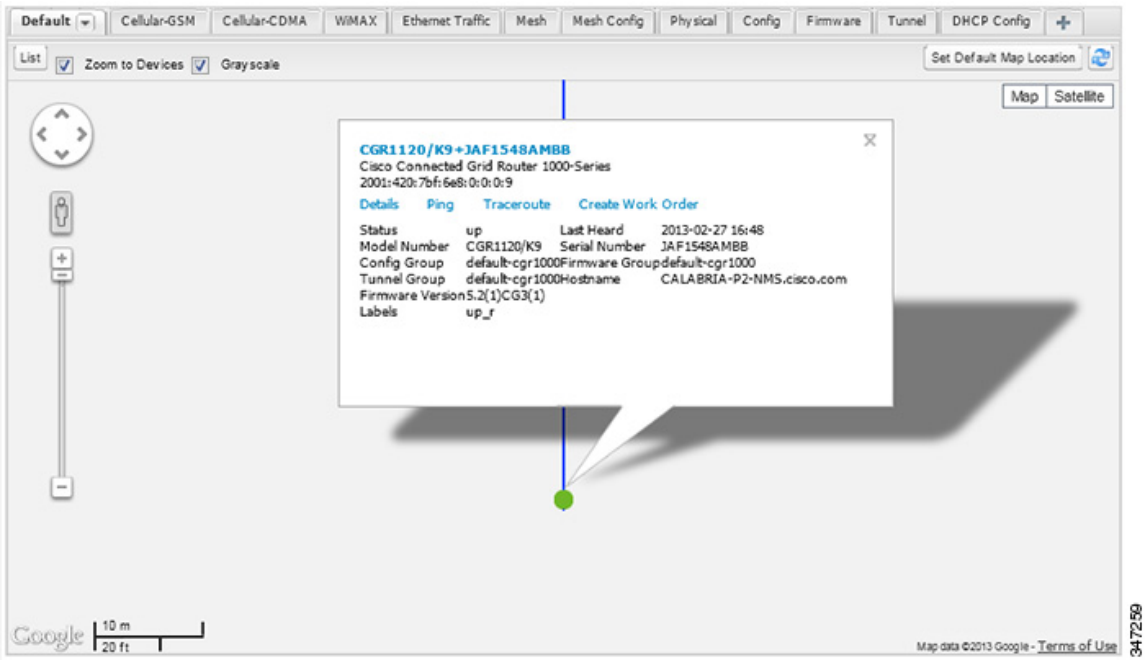
個々のデバイスを確認するには、デバイス アイコンが見えるまでズーム インします。また、デバイスをクリックして [Zoom In] リンクを含むポップアップ ウィンドウを表示し、マップ表示をデバイス レベルに移動することもできます。



IoT FND は、[Browse Devices] ペイン（左ペイン）内の各デバイス グループまたはカテゴリの横にデバイス カウントを表示します。

- すべてのデバイスのサブセットを表示するには、[Browse Devices] ペインにリスト表示されているフィルタの 1 つをクリックします。

  IoT FND は、選択に基づいてマッピング領域を変更し、フィルタにより検出されたデバイスを表示します。たとえば、[Routers] > [Up] を使用して、起動して動作しているすべての FAR を表示できます。[Quick View] ペイン（左ペイン）で保存済みのカスタム フィルタを使用して、デバイス ビューをフィルタリングすることもできます。カスタム フィルタの作成については、「[Quick View] フィルタの作成」を参照してください。
- デバイスまたはグループに関する情報を表示するには、マップ上で該当のアイコンをクリックします。

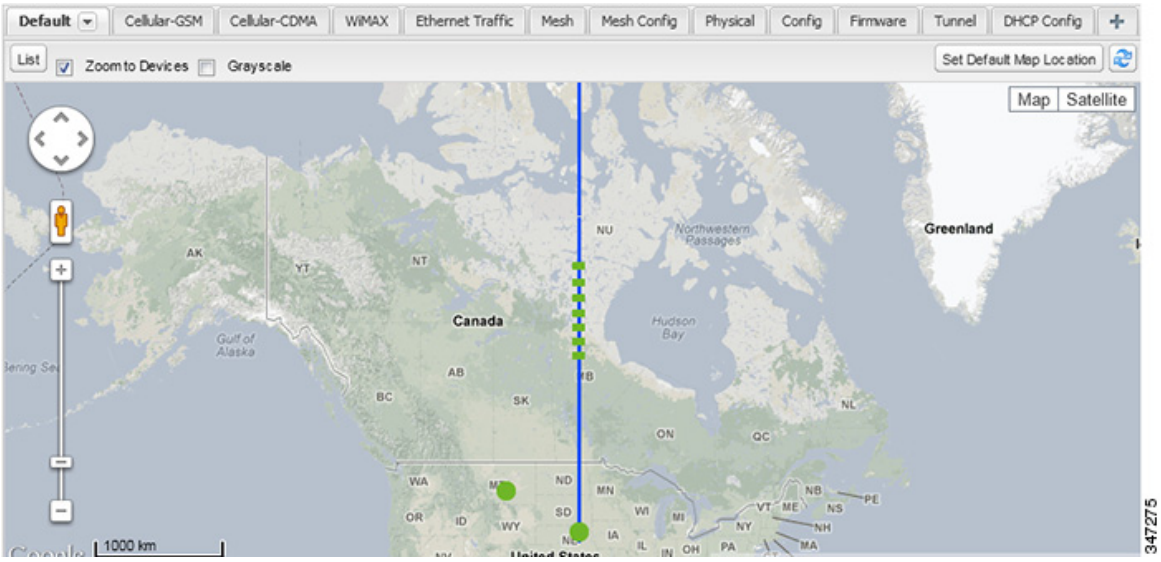


デバイスまたはグループの基本的な情報がリスト表示されたポップアップ ウィンドウが表示されます。

- デバイス仕様を確認するには、[Device] ポップアップ ウィンドウで、[Details] またはデバイスの EID リンクをクリックします。

このウィンドウでは、デバイスの ping、トレース ルートの実行、およびワーク オーダーの作成もできます。

4. デバイスに関連付けられている RPL ツリーを表示するには、[Device] ポップアップ ウィンドウを閉じます。RPL ツリー ポーリングの設定を参照してください。



RPL ツリー接続が青色またはオレンジ色の線で表示されます。青色の線はリンクが下方向であることを示し、オレンジ色の線はリンクが上方向であることを示します。

5. [Map] ビューを更新するには、更新ボタン( )をクリックします。

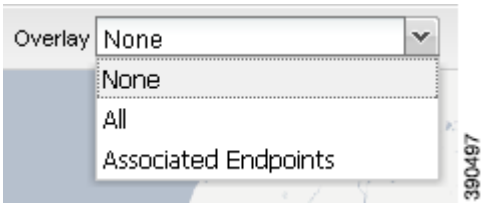
マップの設定

IoT FND では、[Map] ビューでマップに関する次の項目を設定できます。

- デバイスの自動ズーム
- マップのグレースケール表示
- デフォルトのマップ ロケーション（デフォルトで北米に設定）

マップを設定するには、次の手順を実行します。

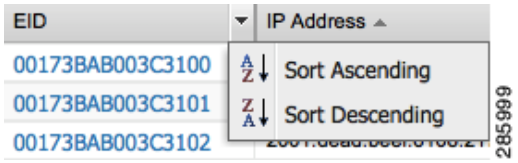
1. [Devices] > [Field Devices] を選択します。
2. [Map] タブをクリックします。
   - デバイスを自動ズームするには、[Zoom to Devices] チェックボックスをオンにします。
   - マップをグレースケール表示するには、[Grayscale] チェックボックスをオンにします。
   - すべての関連付けられているワイヤレス パーソナル エリア ネットワーク（WPAN）をマップ上にオーバーレイするには、[Overlay] ドロップダウン メニューから [Associated WPAN Endpoints] を選択します。



   - マップ ロケーションを常に特定のエリアに対してオープンに設定するには、マップのそのエリアがデフォルトで表示されるようにし、[Set Default Map Location]（右上）をクリックします。
3. [OK] をクリックします。

デバイスのソート順序の変更

デバイスのソート順序を変更するには、カラム見出しの右側をクリックし、ドロップダウン メニューからソート コマンドを選択します。



デバイス情報のエクスポート

IoT FND では、[List] ビューで選択したデバイスのデバイス プロパティをエクスポートできます。IoT FND がエクスポートできるのは、現在のビューのプロパティのみです。

現在のビューに表示されているデバイス情報をエクスポートするには、[List] ビューで次の手順を実行します。

1. 対応するチェックボックスをオンにして、エクスポートするデバイスを選択します。
2. [Export CSV] をクリックします。
3. 確認ダイアログボックスで [Yes] をクリックします。

IoT FND は、CSV ファイルの export.csv を作成します。これには、[List view] ペインに表示される情報が含まれます。デフォルトで、IoT FND はこのファイルをデフォルトのダウンロード ディレクトリに保存します。同じ名前のファイルが存在する場合、IoT FND はデフォルトのファイル名に数字を追加します（export-1.csv、export-2.csv など）。

export.csv ファイルは、エクスポートするフィールドを定義する 1 つの見出し行と、それに続くデバイスを表す 1 つ以上の行から構成されます。[Field Devices] ページから選択したデバイスのエクスポート例を次に示します。

```
name,lastHeard,meshEndpointCount,uptime,runningFirmwareVersion,openIssues,labels,lat,lng
CGR1240/K9+JSJLABTES32,2012-09-19 00:58:22.0,,,,Door Open|Port Down,,50.4,-130.5
sgbuA1_cgr0,,,,,,,42.19716359,-87.93733641
sgbuA1_cgr1,,,,,,,44.3558597,-114.8060403
```

デバイスの ping

デバイスの問題をトラブルシューティングする場合は、ネットワーク接続の問題を排除するために、登録済みデバイスを ping します。デバイスを ping できれば、ネットワーク経由でそのデバイスにアクセスできます。

選択したデバイスを ping するには、[List] ビューで次の手順を実行します。

1. ping するデバイスのチェックボックスを選択します。

   （注）デバイスのステータスが [Unheard] の場合、ping は応答されていません。

2. [Ping] をクリックします。

   ping の結果がウィンドウに表示されます。[Auto Refresh] チェックボックスをオンにした場合、IoT FND はウィンドウを閉じるまで事前定義された間隔でデバイスを ping します。任意の時点で、[Refresh] ボタンをクリックしてデバイスを ping します。

3. 終了したら、[Close] をクリックします。

デバイスへのルートのトレース

Traceroute コマンドにより、デバイスの IP アドレスに到達するために使用するルートを決定することができます。

（注）Traceroute コマンドは、Itron OpenWay RIVA CAM モジュールまたは Itron OpenWay RIVA 電気デバイスおよび Itron OpenWay RIVA G-W（ガス水道）デバイスでは使用できません。

選択したデバイスへのルートをトレースするには、[List] ビューで次の手順を実行します。

1. トレースするデバイスのチェックボックスを選択します。

   （注）IoT FND に登録済みのデバイスへのルートだけをトレースできます。ステータスが [Unheard] のデバイスへのルートはトレースできません。

2. [Traceroute] をクリックします。

   ルート トレースの結果がウィンドウに表示されます。

[Result] カラムを展開して、完全なルーティング情報を表示します。

[Refresh] ボタンをクリックして、Traceroute コマンドを再送信します。ウィンドウを閉じるまで事前定義した間隔で Traceroute コマンドを再送信するには、[Auto Refresh] チェックボックスをオンにします。

3. 終了したら、[Close] をクリックします。

デバイス ラベルの管理

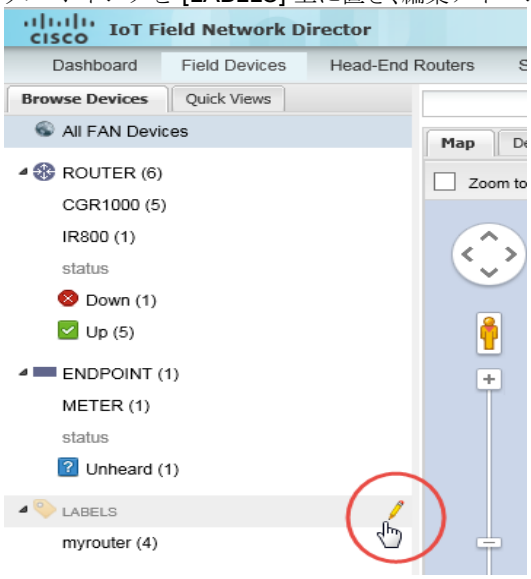
デバイスの配置およびデバイスの管理を容易にするには、ラベルを使用してデバイスの論理グループを作成します。

ラベルの管理

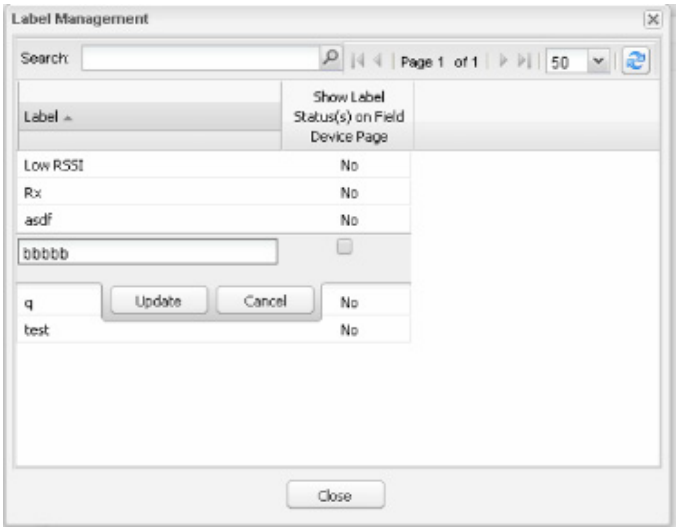
[Label Management] ウィンドウを使用して、すべてのカスタム ラベル、ラベル プロパティ、およびカスタム ラベルの検索を表示します。

ラベルを管理するには、任意のデバイス ページの [Browse Device] ペインで次の手順を実行します。

1. マウス ポインタを [LABELS] 上に置き、編集アイコン( )をクリックします。



- 特定のラベルを検索するには、[Search] フィールドにラベルの名前を入力します。



ヒント:ラベル名のソート順序を逆にするには、[Label] カラムの見出しをクリックします。

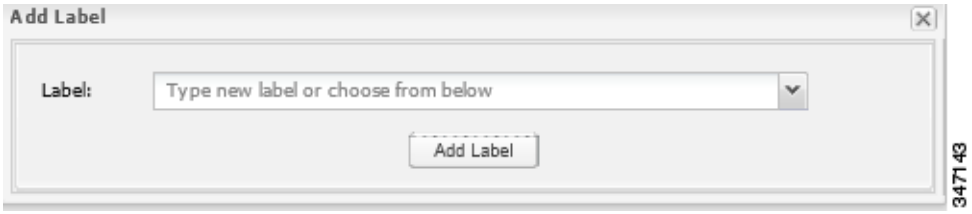
- ラベル プロパティを変更するには、ラベル行をダブルクリックし、ラベル名およびデバイス ステータスの表示設定を編集します。

2. [Update] をクリックしてラベル プロパティの変更内容を承諾するか、または [Cancel] をクリックしてラベル プロパティを保持します。
3. [Close] をクリックします。

ラベルの追加

選択したデバイスにラベルを追加するには、[List] ビューで次の手順を実行します。

1. ラベルを追加するデバイスのチェックボックスを選択します。
2. [Label] > [Add Label] を選択します。



3. ラベルの名前を入力するか、ドロップダウン リストから既存のラベルを選択します。
4. [Add Label] をクリックします。

   ヒント:1 つのデバイスに複数のラベルを追加できます。
5. [OK] をクリックします。

ラベルを一括して追加する場合は、「ラベルの一括追加」を参照してください。

ラベルの削除

選択したデバイスからラベルを削除するには、[List] ビューで次の手順を実行します。

1. ラベルを削除するデバイスのチェックボックスを選択します。
2. [Label] > [Remove Label] を選択します。
3. [OK] をクリックします。

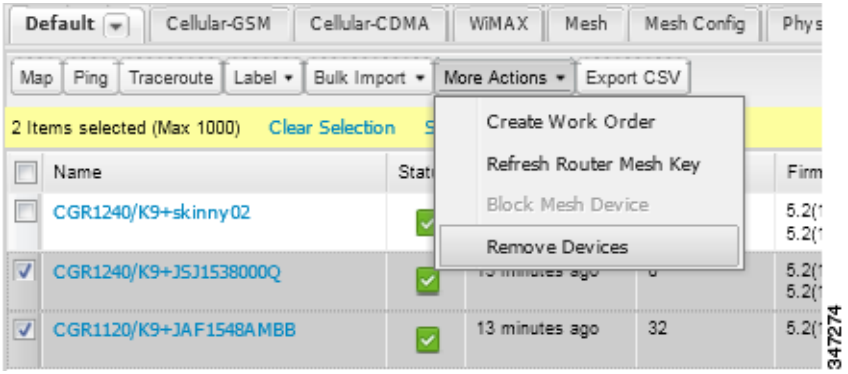
ラベルを一括して削除する場合は、「ラベルの一括削除」を参照してください。

デバイスの削除

注意：FAR を削除すると、IoT FND は、これらのデバイスに関連付けられているすべてのリースされた IP アドレスを Cisco Network Registrar（CNR）サーバに返し、HER から対応するトンネルを削除します。

デバイスを削除するには、[List] ビューで次の手順を実行します。

1. 削除するデバイスのチェックボックスを選択します。



2. [More Actions] > [Remove Devices] を選択します。
3. [Yes] をクリックします。

デバイスの詳細情報の表示

IoT FND は、すべてのデバイスに関する詳細情報をシステム内に保持します。デバイスに関する詳細情報にアクセスするには、デバイスの名前または EID をクリックします。

- 表示される詳細情報
- [Detailed Device Information] ページから実行できるアクション

表示される詳細情報

- Server Information
- HER、FAR、およびエンドポイントの情報

（注）IoT FND は、ページをリロードしなくても、自動的に詳細情報を更新します。

Server Information

IoT FND は、NMS サーバおよびデータベース サーバが稼働しているシステムについて、次の情報を表示します。

表 2　[NMS Server] ペインのエリア

エリア名とフィールド名	説明
Host System Information	
Hostname	IoT FND サーバのホスト名。
ホスト オペレーティング システム	オペレーティング システム。
CPU	CPU の規格。
メモリ合計	システムで使用可能な RAM メモリの合計量（GB）。
Current System Time	現在のシステム時間
Host Disk Information	
ファイル システム	ファイル システム。
サイズ	ファイル システムのディスク領域のサイズ（GB）。
Used	使用されているファイル システムのディスク領域の量（GB）。
Available	使用可能なファイル システムのディスク領域（GB）。
Use %	使用されているファイル システムのディスク領域（パーセント）。
Mounted On	ファイル システムが配置されているディレクトリ。
IoT FND Application Information	
EID	サーバの EID。
Start Time	IoT FND サーバが開始された時刻。
Number of Restarts	IoT FND アプリケーションが再起動した回数。
Memory Allocation	IoT FND アプリケーションのメモリ領域の割り当て（GB）。

HER、FAR、およびエンドポイントの情報

IoT FND は、HER、FAR、およびエンドポイントに関して表示する詳細なデバイス情報を、次のカテゴリにグループ化します。

情報のカテゴリ	説明
Device Info	デバイス情報の詳細を表示します（「デバイス プロパティ」を参照）。 FAR および ME については、IoT FND はグラフも表示します（「デバイス グラフの表示」を参照）。
Event	デバイスに関連付けられているイベントに関する情報を表示します。
Config Properties	デバイスの設定可能なプロパティを表示します（「デバイス プロパティ」を参照）。 これらのプロパティは、設定するプロパティとその新しい値を指定している CSV ファイルをインポートすることで設定できます（「デバイス設定プロパティの変更」を参照）。
Running Config（FAR）	デバイスの実行コンフィギュレーションを表示します。
Mesh Routing Tree（FAR および ME）	メッシュ ルーティング ツリーを表示します。 FAR の場合、[Mesh Routing Tree] ペインには ME から FAR への使用可能なすべてのルータが表示されます。 ME の場合、[Mesh Routing Tree] ペインには FAR へのメッシュ ルートが表示されます。
Mesh Link Traffic（FAR）	メッシュ リンク トラフィックのタイプをビット/秒単位で経時的に表示します。
Router Files（FAR）	.../managed/files/ ディレクトリにアップロードされたファイルをリスト表示します。

情報のカテゴリ	説明
Raw Sockets（FAR）	TCP raw ソケット（表 29（252 ページ）を参照）のメトリックおよびセッション データをリスト表示します。
Embedded AP（IR829）	接続されているアクセス ポイントのインベントリ（設定）の詳細およびメトリックをリスト表示します。
AP Running Config（C800 および IR800）	接続されているアクセス ポイントの実行設定ファイルをリスト表示します。

[Detailed Device Information] ページから実行できるアクション

[Detailed Device Information] ページでは、デバイス タイプによって次のアクションを実行できます。

Action	説明
Show on Map （ME のみ）	デバイスのマップ ロケーションを含むポップアップ ウィンドウを表示します。[Map] ビューで検索フィールドに「**eid:***Device_EID*」と入力しても、同じ結果になります。
ping	デバイスに ping を送信し、そのネットワーク接続を確認します。デバイスの pingを参照してください。
traceroute	デバイスへのルートをトレースします。デバイスへのルートのトレースを参照してください。
Refresh Metrics （HER と FAR のみ）	デバイスに IoT FND へのメトリックを送信するよう指示します。 (注)IoT FND各デバイスのメトリックに履歴値を割り当ててください。メトリックの履歴値にアクセスするには、GetMetricHistory North Bound API コールを使用します。
Refresh Router Mesh Key （FAR のみ）	ルータ ME キーを更新します。ルータ メッシュ キーの更新を参照してください。
Create Work Order （FAR と DA ゲートウェイのみ）	ワーク オーダーを作成します。ワーク オーダーの作成を参照してください。
Sync Config Membership （ME のみ）	このデバイスの設定メンバーシップを同期します。エンドポイント メンバーシップの同期を参照してください。
Sync Firmware Membership （ME のみ）	[Sync Firmware Membership] をクリックしてこのデバイスのファームウェア メンバーシップを同期し、その後、[Yes] をクリックしてプロセスを完了します。
Block Mesh Device （ME のみ）	ME デバイスをブロックします。 **注意:** これは、破壊的な操作です。 (注) [Block Mesh Device] は、Itron OpenWay RIVA CAM モジュールまたは Itron OpenWay RIVA 電気デバイスおよび Itron OpenWay RIVA G-W（Gas-Water）デバイスでは使用できません。

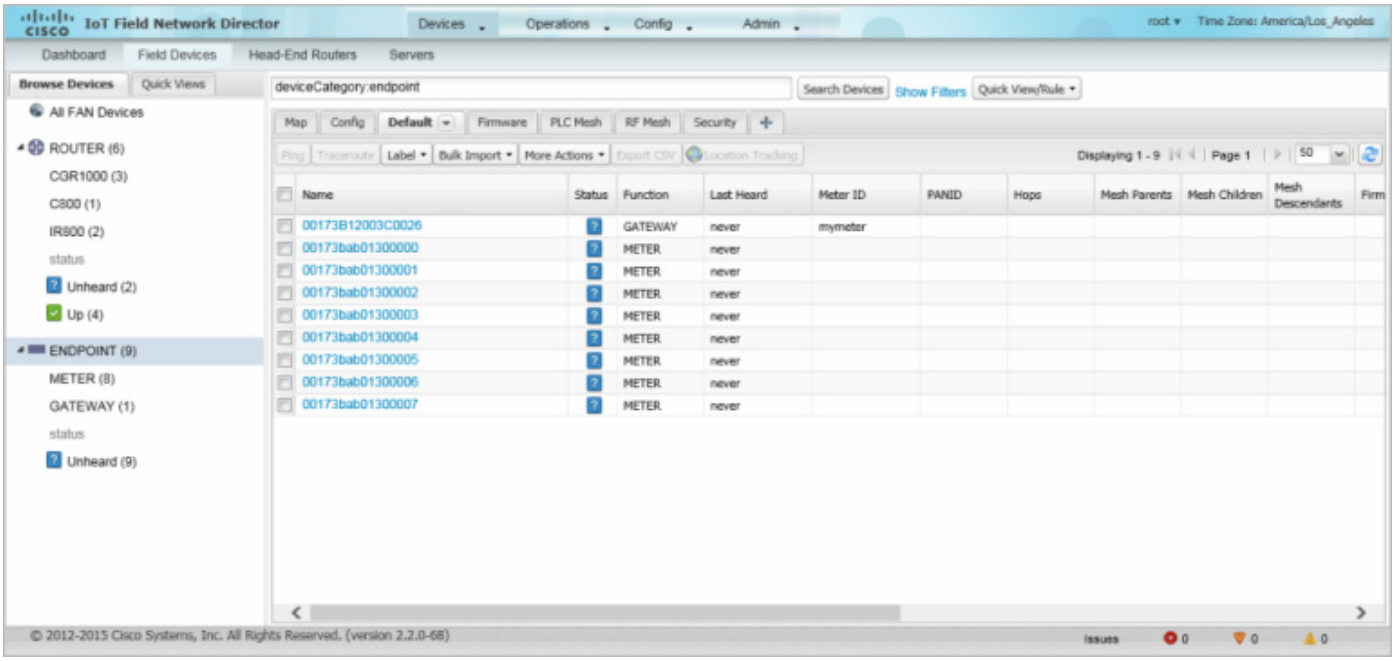
フィルタを使用したデバイス表示の制御

導入によっては、IoT FND により管理されるデバイスの数が膨大になる場合があります（IoT FND は最大 10,000,000 のデバイスを管理します）。[Map] ビューおよび [List] ビューでのデバイスの配置や表示を容易にするために、IoT FND はフィルタを提供しています。カスタマイズされたフィルタを追加することもできます。フィルタは、[Browse Devices] タブおよび [Quick View] タブに表示されます。

[Browse Devices] フィルタ

[Browse Devices] ペインには、組み込みのデバイス フィルタが表示されます。これらのフィルタは、[List] ビューおよび [Map] ビューでのデバイスの表示を制御します。各フィルタ エントリに対し、IoT FND はデバイス カウントをカッコ内に表示します。IoT FND は、ページをリロードしなくても、自動的にデバイス カウントを更新します。図 5 の例では、最上位のエンドポイント ラベルが選択されており、これにより、次の組み込みフィルタが [Search Devices] フィールドに挿入されます：*deviceType:cgmesh firmwareGroup:default-cgmesh*。

図 5　　ME を検索するための組み込みフィルタ



[Quick View] フィルタの作成および編集

[Quick View] ペインには、カスタム フィルタが表示されます。このペインでフィルタをクリックすると、フィルタで定義されている検索基準を満たすデバイスが表示されます。

[Quick View] フィルタの作成

[Quick View] フィルタを作成するには、次の手順を実行します。

1. 任意のデバイス ページで [Show Filters] をクリックし、[Search] フィールドにフィルタを追加します。

   フィルタの追加の詳細については、「フィルタの追加」を参照してください。

2. [Quick View/Rule] ドロップダウン メニューから、[Create Quick View] を選択します。
3. [Save Quick View] ダイアログボックスの [Name] フィールドに、[Quick View] フィルタの名前を入力します。
4. [Save（保存）] をクリックします。

[Quick View] フィルタの編集

[Quick View] フィルタを編集または削除するには、次の手順を実行します。

1. [Quick View] タブをクリックし、編集するフィルタを選択します。
2. [Quick View/Rule] ドロップダウン メニューから、[Edit Quick View] を選択します。

3. [Update Quick View] ダイアログボックスで、必要な変更を行い、[Save] をクリックします。
4. [Quick View] を削除するには、[Delete] ボタンをクリックします。

フィルタの追加

[Search] フィールドにフィルタを追加するには、次の手順を実行します。

1. [Search] フィールドの下に [Add Filter] フィールドがない場合は、[Show Filters] をクリックします。
2. [Label] ドロップダウン リストからフィルタを選択します。

   ドロップダウン メニューでは、すべてのデバイス情報カテゴリのフィルタが定義されています。これらのカテゴリの詳細については、「ルータの各ビューの使用」を参照してください。
3. [Operator (:)] ドロップダウン メニューから演算子を選択します。

   演算子の詳細については、表 3を参照してください。[Label] メニューから数値メトリック（たとえば [Transmit Speed]）を選択すると、追加するフィルタに一定範囲の値を指定できます。Date/Time のフィルタについては、Between 演算子を使用します。カレンダー ボタンを使用して、フィルタの日付範囲を指定します。
4. [Value] フィールドに、一致させる値、または数値メトリックの場合は値の範囲を入力するか、またはドロップダウン メニューから使用可能な値を選択します。
5. 追加（[+]）ボタンをクリックし、[Search] フィールド内の既存のフィルタ構文にフィルタを追加します。
6. （任意）フィルタを追加し続ける場合は、このプロセスを繰り返します。

フィルタ演算子

表 3 に、フィルタの作成に使用できる演算子を示します。

表 3　　フィルタ演算子

演算子	説明
:	等しい
>	より大きい
>=	以上
<	より小さい
<=	以下
<>	等しくない

検索構文

IoT FND は、次の簡易なクエリ言語構文をサポートします。

Search := filter [filter ...]

Filter := fieldname operator value

operator := < | <= | > | >= | <> | = | :

[Search] フィールド対するフィルタを作成するときは、次の点に注意してください。

- 各フィールドには、データ型（String、Number、Boolean、および Date）が指定されます。
- [String] フィールドには文字列を含めることができ、これらを検索するには、文字列等価（「:」）を使用します。

- [Numeric] フィールドには、10 進数（倍精度浮動小数点として保存される）を含めることができ、これらを検索するには、数値比較演算子（「>」、「>=」、「<」、「<=」、「<>」）を使用します。
- [Boolean] フィールドには、「true」または「false」の文字列を含めることができます。
- [Date] フィールドには、yyyy-MM-dd HH:mm:ss:SSS の形式で日付を含めることができます。日付を検索するには、数値比較演算子を使用します。

表 4 にフィルタの例を示します。

表 4　　フィルタの例

フィルタ	説明
`configGroup:"default-cgr1000"`	default-cgr1000 グループに属するすべてのデバイスを検出します。
`name:00173*`	名前が 00173 で始まるすべての FAR を検出します。
`deviceType:cgr1000 status:up label:"Nevada"`	起動して動作している Nevada グループ内のすべての CGR 1000 を検出します。

一括インポート アクションの実行

IoT FND では、次の一括インポート アクションを実行できます。

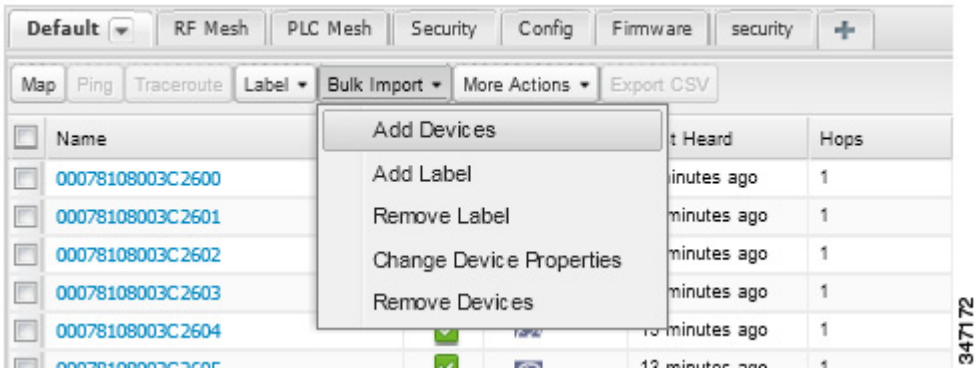
- デバイスの一括追加
- デバイスの一括削除
- デバイス プロパティの一括変更
- ラベルの一括追加
- ラベルの一括削除

デバイスの一括追加

[Bulk Import] ドロップダウン メニューで [Add Devices] オプションを選択すると、CSV ファイルを使用して FAR および HER を一括して IoT Field Network Director に追加できます。

デバイスを一括して追加するには、次の手順を実行します。

1. 任意のデバイス ページで、[Bulk Import] ドロップダウン メニューから [Add Devices] を選択します。



2. [Browse] をクリックし、インポートするデバイスの情報を含む CSV ファイルを検索し、[Open] をクリックします。

   HER の追加の詳細については、「IoT FND への HER の追加」を参照してください。

FAR の追加の詳細については、「IoT FND への FAR の追加」を参照してください。

(注) FAR については、シスコ パートナーが提供する Notice-of-Shipment XML ファイルを使用して FAR をインポートすることもできます。

3. [Add] をクリックします。
4. [Close] をクリックします。

IoT FND への HER の追加

IoT FND への追加前の HER の設定

HER を IoT FND に追加する前に、次のように、SSH で Netconf を使用して、HER を IoT FND で管理できるよう設定します。

```
hostname <her_hostname>
ip domain-name <domain.com>
aaa new-model
no ip domain-lookup
ip ssh time-out 120
ip ssh version 2
crypto key gen rsa
netconf ssh
netconf max-sessions 16
```

この場合、*<her_hostname>* は IoT FND サーバのホスト名または IP アドレス、*<domain.com>* は HER および IoT FND が常駐するドメインの名前です。大規模ネットワークでは、タイムアウト値 120 が必要です。

HER を IoT FND により管理できるよう設定したら、次のことができることを確認します。

- HER の管理インターフェイスを ping できる。
- SSH で HER の管理インターフェイスにアクセスでき、その逆も可能である。

HER の追加

HER を追加するには、見出し行とそれに続くそれぞれ HER を表す 1 つ以上の行から構成される、次の例のような CSV ファイルを作成します。

```
eid,deviceType,lat,lng,ip,netconfUsername,netconfPassword
ASR1001+JAE15460070,asr1000,40.0,-132.0,172.27.166.57,admin,cisco
ASR1001+JAE15460071,asr1000,40.0,-132.0,172.27.166.58,admin,cisco
```

表 5 に、CSV ファイルに含めるフィールドを示します。

(注) デバイス設定フィールドの記述については、「デバイス プロパティ」を参照してください。

表 5　　HER インポートのフィールド

フィールド	説明
eid	デバイスの要素識別子（EID）。製品 ID（PID）、プラス記号、および HER のシリアル番号（SN）から構成されます（例：*HER_PID+HER_SN*）。
deviceType	デバイス タイプは、asr1000 または isr3900 にする必要があります。
lat	（任意）HER の場所（緯度と経度）。
lng	

表 5　HER インポートのフィールド（続き）

フィールド	説明
ip	HER の IP アドレス。このアドレスは、IoT FND サーバから到達可能である必要があります。
netconfAddress	
netconfUsername	IoT FND が HER に接続するために使用する SSH ユーザ名およびパスワード。
netconfPassword	

HER を追加すると、IoT FND のステータスは [Unheard] と表示されます。HER のポーリング後、IoT FND のステータスは [Up] に変更されます。IoT FND は、15 分ごとにバックグラウンドで HER をポーリングしてデバイスのメトリックを収集します。したがって、HER を IoT FND に追加した後に HER のステータスが {Up} になるまでに 15 分以上かかることはありません。ただし、[Refresh Metrics]（Refresh Metrics）をクリックすることで、HER のポーリングをトリガーできます。

IoT FND への FAR の追加

通常、IoT FND に FAR を追加するには、シスコ パートナーからユーザに送信される Notice-of-Shipment XML ファイルを使用します。このファイルには、ユーザに出荷されたすべての FAR の R レコードが含まれています。CGR の R レコードの例を示します。

```
<AMI>
    <Relays>
        <DCG deviceClass=?10.84.82.56?>
            <PID>CGR1240/K9</PID>
            <R>
                <ESN>2.16.840.1.114416.3.2286.333498</ESN>
                <SN>FIXT:SG-SALTA-10</SN>
                <wifiSsid>wifi ssid 1</wifiSsid>
                <wifiPsk>wifi psk 1</wifiPsk>
                <adminPassword>ppswd 1</adminPassword>
                <type6PasswordMasterKey>secret 1</type6PasswordMasterKey>
                <tunnelSrcInterface1>Ethernet2/3</tunnelSrcInterface1>
            </R>
        </DCG>
    </Relays>
</AMI>
```

（注）XML 設定テンプレートを使用して設定可能なすべてのデバイス プロパティのリストは、デバイス プロパティ、239 ページを参照してください。

この例で使用されている R レコードで定義されている FAR のプロパティを表 6 に示します。

表 6　FAR インポートのフィールド

フィールド	説明
PID	シスコにより提供されている製品 ID。製品には印刷されていません。
SN	FAR のシリアル番号。 （注）IoT FND は、PID と SN を組み合わせて FAR EID を作成します。
ESN	シスコ パートナーにより FAR 内の WPAN メッシュ カードに割り当てられたシリアル番号。このフィールドは、IoT FND では使用されません。
wifiSsid	この情報は、製造コンフィギュレーションのプロセス中にシスコ パートナーによって FAR に対して設定されます。IoT FND は、この情報を将来の使用のためにデータベースに保存します。 （注）CG-OS CGR では、最大 2 つの SSID が許可されます。
wifiPsk	
adminPassword	
adminUsername	
type6PasswordMasterKey	
tunnelSrcInterface1	

FAR の HER へのマッピング

トンネルのプロビジョニングに必要な FAR の HER へのマッピングを決定した後は、IoT FND で、次の 2 つの方法のいずれかを使用してマッピングを設定できます。

- Notice-of-Shipment XML ファイル内のすべての FAR レコードにマッピング情報を追加する。
- FAR の HER へのマッピングを指定する CSV ファイルを作成する。

Notice-of-Shipment XML ファイルへの FAR の HER へのマッピングの追加

FAR を HER にマッピングするには、Notice-of-Shipment XML ファイル内の FAR レコードに、HER プロパティの tunnelHerEid および ipsecTunnelDestAddr1 を追加します。

- tunnelHerEid プロパティは、HER の EID を指定します。
- ipsecTunnelDestAddr1 プロパティは、HER のトンネル IP アドレスを指定します。

次に例を示します。

```
...
        <tunnelHerEid>ASR1001+JAE15460070</tunnelHerEid>
        <ipsecTunnelDestAddr1>172.27.166.187</ipsecTunnelDestAddr1>
    </R>
</DCG>
```

FAR の HER へのマッピングの CSV ファイルへの追加

CSV ファイルを使用して FAR を HER にマッピングするには、FAR の HER へのマッピングのそれぞれについての行を追加します。この行では、次に示す CGR の例のように、FAR の EID、対応する HER の EID、および HER のトンネル IP アドレスを指定する必要があります。

```
eid,tunnelHerEid,ipsecTunnelDestAddr1
CGR1240/K9+FIXT:SG-SALTA-10,ASR1001+JAE1546007O,172.27.166.187
```

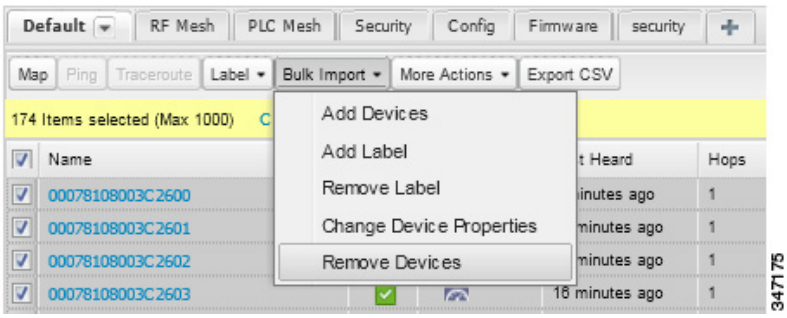
デバイスの一括削除

削除するデバイスの EID をリスト表示している CSV ファイルを使用して、デバイスを一括して削除することができます。

注意: FAR を削除すると、IoT FND は、これらのデバイスに関連付けられているすべてのリースされた IP アドレスを CNR に返し、HER から対応するトンネルを削除します。

デバイスを一括して削除するには、次の手順を実行します。

1. [Devices] > [Device Type] を選択します。
2. [Bulk Import] > [Remove Devices] を選択します。



3. [Browse] をクリックし、削除するデバイスの情報を含む CSV ファイルを検索し、[Choose] をクリックします。

   以下に、予想される CSV フォーマットの例を示します。この場合、CSV ファイルは、3 つの CGR と 1 つの HER を指定しています。

   ```
   eid
   cgr1000-CA-107
   cgr1000-CA-108
   cgr1000-CA-109
   asr1000-CA-118
   ```

4. [Remove] をクリックします。

   [Remove Devices] ウィンドウの [Status] セクションに、この操作のステータスが表示されます。[History] セクションには、この操作に関すその他の情報が示されます。障害があった場合は、[Failure#] カラム内の対応するリンクをクリックし、エラーに関する詳細情報を取得します。

5. 終了したら、[Close] をクリックします。

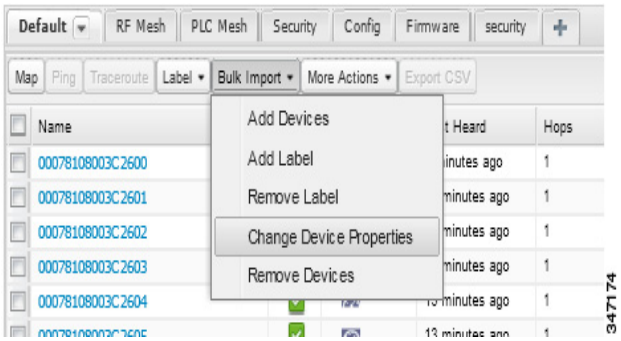
デバイス プロパティの一括変更

IoT FND では、CSV ファイルを使用してデバイス プロパティを一括して設定できます。たとえば、次の CSV ファイルは、指定した HER の緯度と経度を変更します。

```
eid,lat,lng,ip,
ASR1001+JAE1546007O,42.0,-120.0
```

デバイス プロパティを一括して設定するには、次の手順を実行します。

1. 任意のデバイス ページで、[Bulk Import] > [Change Device Properties] を選択します。



2. [Browse] をクリックし、設定するデバイスと対応するプロパティのリストを含む CSV ファイルを検索し、[Open] をクリックします。

3. [Change] をクリックします。

4. 終了したら、[Close] をクリックします。

ラベルの一括追加

デバイスにラベルを割り当てることで、デバイスを論理的にグループ化できます。ラベルはデバイス タイプに無関係であり、任意のタイプのデバイスに、任意のラベルを割り当てることができます。また、1 つのデバイスに複数のラベルを割り当てることができます。設定グループおよびファームウェア グループとは異なり、ラベルに関連付けられているポリシーやメタデータはありません。

IoT FND では、CSV ファイルを使用してラベルを一括して追加できます。CSV ファイルで、ラベルを追加するデバイスのリストを指定します。

デバイス ラベルを追加するには、次の手順を実行します。

1. 任意のデバイス ページで、[Bulk Import] > [Add Label] を選択します。

2. [Browse] をクリックし、ラベルを追加するデバイスのリストを含む CSV ファイルを検索し、[Open] をクリックします。

   以下に予想される CSV フォーマットの例を示します。

```
eid
cgr1000-CA-107
cgr1000-CA-108
cgr1000-CA-109
asr1000-CA-118
```

3. [Label] フィールドで、ラベルを入力するか、ドロップダウン メニューからラベルを選択します。
4. [Add Label] をクリックします。

   [LABELS] の下の [Browse Devices] タブ（左ペイン）にラベルが表示されます。

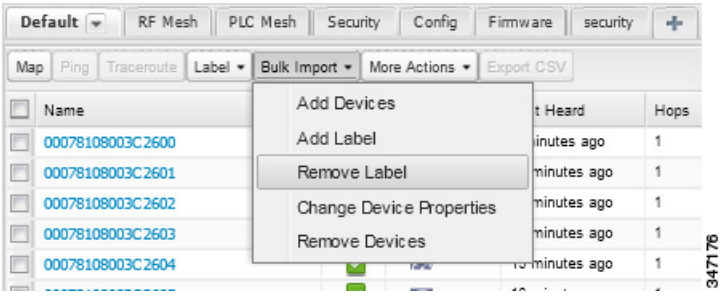
5. 終了したら、[Close] をクリックします。

ラベルの一括削除

IoT FND では、CSV ファイルを使用してラベルを一括して削除できます。

デバイス ラベルを削除するには、次の手順を実行します。

1. 任意のデバイス ページで、[Bulk Import] > [Remove Label] を選択します。



2. [Browse] をクリックし、ラベルを削除するデバイスのリストを含む CSV ファイルを検索し、[Open] をクリックします。
3. ドロップダウン メニューで、削除するラベルを選択します。
4. [Remove Label] をクリックします。
5. [Close] をクリックします。

ルールの設定

IoT FND のルールは、フィルタ、およびイベント後またはフィルタで定義されている検索基準に一致するメトリックの受信後に IoT FND が実行するアクションを定義します。ルールにより、イベント条件およびメトリックしきい値を確認できます。

たとえば、設定グループ内の FAR のステータスが [Up] に変更したらいつでも、サーバ ログ(server.log)にカスタム メッセージを追加してデバイスに適切なラベルを追加することができます。これにより、デバイスにラベルを追加するプロセスを自動化することができます。

ルールを使用する際には以下を行うことができます。

- 条件とアクションを含むルールを追加する。
- プロパティとメトリックに従ってデバイスを照合させるデバイス検索クエリを使用して、条件を含むルールを定義する。
- 一致するデバイスまたは一致するイベントを送信するデバイスにラベルを追加するアクションを含むルールを定義する。
- 一致するデバイスまたは一致するイベントを送信するデバイスからラベルを削除するアクションを含むルールを定義する。
- ユーザ定義のメッセージなど、*user alert* イベントをログに配置するアクションを含むルールを定義する。

ルールの表示および編集

ルールを表示するには、次の手順を実行します。

1. [Config] > [Rules] を選択します。

   IoT FND は、データベースに保存されているルールのリストを表示します。表 7 に、このリストに表示されるフィールドを示します。

表 7　　ルールのフィールド

フィールド	説明
名前	ルールの名前。
Active?	ルールがアクティブかどうかを示します。ルールは、アクティブ化されない限り適用されません。
Rule definition	ルールの構文。 たとえば、次のルールは、デバイスのバッテリ 0 レベルが 50 % 未満に下がったときに IoT FND で実行されます。 `battery0Level<50`
規則アクション	ルールによって実行されるアクション。次に例を示します。 `Log Event With: CA-Registered , Add Label: CA-Registered` この例では、次のアクションが実行されます。 ■ このルールにより生成されたルール イベントの eventMessage プロパティを CA-Registered に設定する。 ■ CA-Registered ラベルを一致するデバイスに追加する。
Updated By	ルールを最後に更新したユーザのユーザ名。
Updated At	ルールが最後に更新された日時。

2. ルールを編集するには、名前をクリックします。

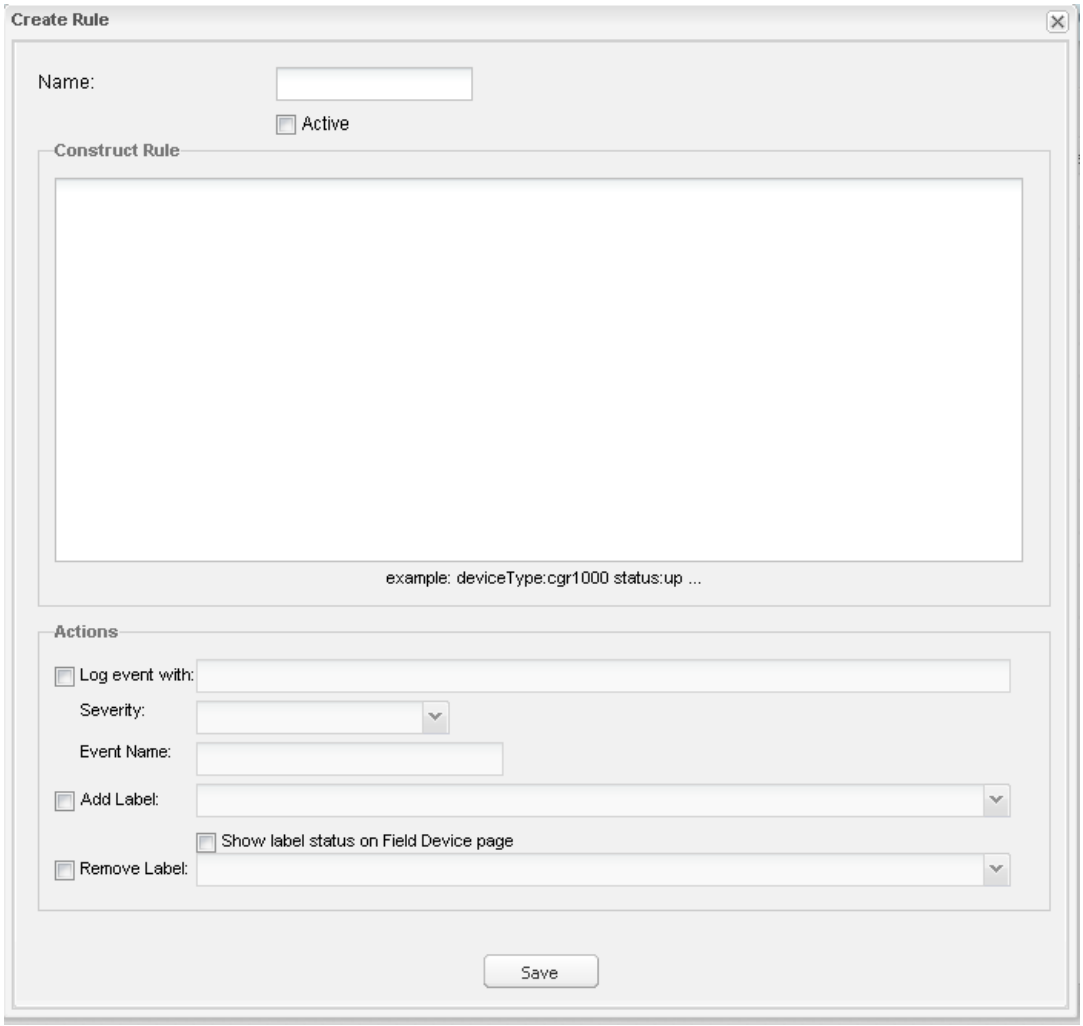
   ルールの編集方法の詳細については、「ルールの追加」を参照してください。

ルールの追加

ルールを追加するには、次の手順を実行します。

1. [Config] > [Rules] を選択します。
2. [Add] をクリックします。
3. ルールの名前を入力します。

   (注) 無効な文字(「=」、「+」、「~」など)を入力すると、IoT FND は赤色のアラート アイコンを表示し、該当するフィールドを赤色で強調表示し、さらに [OK] ボタンを無効にします。
4. ルールをアクティブにするには、[Active?] チェックボックスをオンにします。



5. ルールの構文を入力します。

   フィルタの作成に使用した構文と同じ構文を使用します。検索構文を参照してください。

6. 次のアクションの少なくとも 1 つのチェックボックスをオンにします。

   - Log event with：サーバ ログ、重大度、およびイベント名のイベント ログ エントリに追加するメッセージを指定します。
     - Severity：イベントに割り当てる重大度レベルを選択します。
     - Event Name：イベントに割り当てるイベント名を入力します（イベント名での検索、327 ページを参照）。

     たとえば、このフィールドに「Red Alert」と入力し、[Severity] を [CRITICAL] に設定して、[Event Name] に「CHECK ROUTER」と入力した場合、ルールに一致するイベントについてロギングされたエントリでは、サーバ ログ（server.log）からの次のエントリ例に示すように、eventMessage フィールドが Red Alert に設定されます。

     ```
     16494287: NMS-200-5: May 02 2012 22:32:41.964 +0000: %CGMS-7-UNSPECIFIED:
     %[ch=EventProducer][sev=DEBUG][tid=com.espertech.esper.Outbound-CgmsEventProvider-1]: Event
     Object which is send = EventObject [netElementId=50071, eventTime=1335997961962,
     eventSeverity=0, eventSource=cgr1000, eventType=UserEventType, eventMessage=Red Alert,
     eventName=CHECK ROUTER, lat=36.319324, lng=-129.920815, geoHash=9n7weedx3sdydv1b6ycjw,
     eventTypeId=1045, eid=CGR1240/K9+JAF1603BBFF]
     ```

     IoT FND では、[Log event with] フィールドで定義したメッセージが、[Events] ページ（[Operations] > [Events]）にリスト表示される一致するイベント エントリの [Message] フィールドに表示され、新しい [Event Name] が新たな検索フィルタになります。
   - Add Label：新しいラベルの名前を入力するか、[Add Label] ドロップダウン メニューからラベルを選択します。
   - Show label status on Field Devices page：[Browse Devices] ペインの [LABELS] セクションに、このルールをトリガーしたデバイスのステータスを表示します。
   - Remove Label：[Remove Label] ドロップダウン メニューから削除するラベルを選択します。

7. [Save（保存）] をクリックします。

ルールのアクティブ化

IoT FND では、アクティブ化されていない場合、ルールは適用されません。

ルールをアクティブ化するには、次の手順を実行します。

1. [Config] > [Rules] を選択します。
2. アクティブ化するルールのチェックボックスを選択します。
3. [Activate] をクリックします。
4. [Yes] をクリックしてルールをアクティブ化します。
5. [OK] をクリックします。

ルールの非アクティブ化

ルールは非アクティブ化されると、IoT FND で適用されません。

ルールを非アクティブ化するには、次の手順を実行します。

1. [Config] > [Rules] を選択します。
2. 非アクティブ化するルールのチェックボックスを選択します。
3. [Yes] をクリックしてルールを非アクティブ化します。
4. [OK] をクリックします。

ルールの削除

ルールを削除するには、次の手順を実行します。

1. [Config] > [Rules] を選択します。
2. 削除するルールのチェックボックスを選択します。
3. [Delete] をクリックします。
4. ルールを削除する場合は [Yes] をクリックします。
5. [OK] をクリックします。

デバイスの設定

この項では、IoT FND でデバイスを設定する方法について説明します。次の項目を取り上げます。

- デバイス グループの設定
- ROUTER 設定テンプレートの編集
- ENDPOINT 設定テンプレートの編集
- FAR への設定のプッシュ
- メッシュ エンドポイントへの設定のプッシュ

デバイス グループの設定

IoT FND では、デバイスを一括して管理するためにグループを使用します。IoT Field Network Director に FAR を追加すると、IoT FND は FAR を適切なデフォルトの ROUTER 設定グループ（**default-cgr1000**）に自動的に追加します。Me（メータおよび Range Extender）を追加すると、IoT FND はそれらをデフォルトの ENDPOINT 設定グループである **default-cgmesh** に追加します。

- デバイス グループの作成
- デバイス設定プロパティの変更
- 別のグループへのデバイスの移動
- 設定グループ内のデバイスのリスト表示
- 定期的なインベントリ通知とマーク ダウン タイマーの設定
- デバイス設定グループの名前変更
- デバイス グループの削除

デバイス グループの作成

デフォルトで、IoT FND は [Devices] > [Field Devices] ページ左側のツリーに記載されている次のデバイスグループを次のように定義します。

グループ名	説明
default-act	デフォルトで、すべての Itron OpenWay RIVA 電気デバイス（METER）はこのグループのメンバーです。 ■ [Group] 見出しの下にリストされる個々の RIVA 電気デバイスは次のように表示されます。 *OW Riva CENTRON*
default-bact	デフォルトで、すべての Itron OpenWay RIVA G-W（ガス水道）デバイス（METER）はこのグループのメンバーです。 ■ [Group] 見出しの下にリストされる個々の RIVA 水道メーターは次のように表示されます。 *OW Riva G-W* ■ [Group] 見出しの下にリストされる個々の RIVA ガス メーターは次のように表示されます。 *OW Riva G-W*
default-cam	デフォルトで、すべての Itron OpenWay RIVA CAM モジュール（ROOT）はこのグループのメンバーです。 ■ [CAM] 見出しの下にリストされる個々の RIVA CAM モジュールは次のように表示されます。 *OW Riva CAM*
default-c800	デフォルトで、すべての C800 および ISR（ルータ）はこのグループのメンバーです。
default-cgmesh	デフォルトで、すべての cgmesh エンドポイント（METER）はこのグループのメンバーです。
default-cgr1000	デフォルトで、すべての CGR（ルータ）はこのグループのメンバーです。
default-ir800	デフォルトで、すべての IR800（ルータ）はこのグループのメンバーです。

各デフォルト グループは、そのグループ内のすべてのデバイスにプッシュ可能なデフォルト設定テンプレートを定義します。ただし一群のデバイスに別のテンプレートを適用する必要がある場合は、新しいグループを作成し、必要に応じて、そのデフォルト設定テンプレートを変更します。

(注) デフォルト グループは削除できませんが、その名前は変更できます。ただし、これは推奨されません。また、デフォルトの ROUTER グループおよび ENDPOINT グループには同じアイコンが使用され、一方、カスタム グループには異なるアイコンが使用されます。アイコンの定義については、表 5 を参照してください。

- ROUTER グループの作成
- ENDPOINT グループの作成

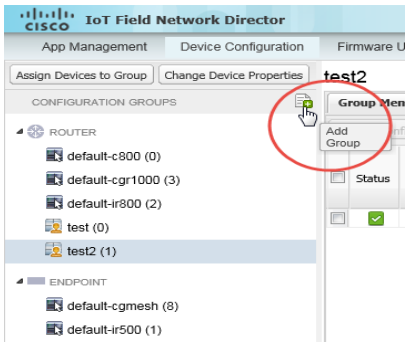
ROUTER グループの作成

(注) CGR、IR800、および ISR800 は 1 つのネットワーク上に共存できます。ただし、すべてのルータ タイプを含むカスタム テンプレートを作成する必要があります。

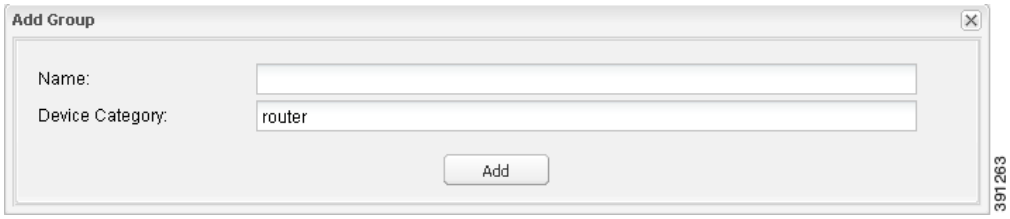
ROUTER 設定グループを作成するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. デフォルト グループの **default-cgr1000default-ir800** を選択します。

3. **[Add Group]** ボタンをクリックします。



4. グループの名前を入力します。



デバイス カテゴリがデフォルトで選択されています。

(注) 無効な文字(「=」、「+」、「~」など)を入力すると、IoT FND は赤色のアラート アイコンを表示し、該当するフィールドを赤色で強調表示し、さらに [OK] ボタンを無効にします。

5. [Add] をクリックします。

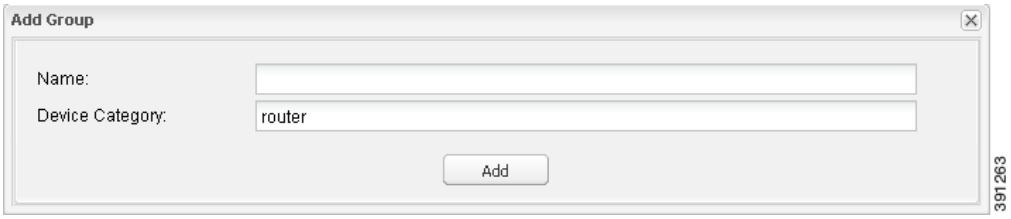
[ROUTERS] リスト(左ペイン)に新しいグループ エントリが表示されます。

- グループの名前を変更する場合は、「デバイス設定グループの名前変更」を参照してください。
- グループを削除するには、「デバイス グループの削除」を参照してください。

ENDPOINT グループの作成

ENDPOINT グループを作成するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. デフォルト グループを選択します(**default-cgmesh**、**default-act**、**default-cam**)。
3. [Add Group]()ボタンをクリックします。
4. グループの名前を入力します。



(注) 無効な文字(「=」、「+」、「~」など)を入力すると、IoT FND は赤色のアラート アイコンを表示し、該当するフィールドを赤色で強調表示し、さらに [OK] ボタンを無効にします。

5. [Add] をクリックします。

   [ENDPOINT] リスト(左ペイン)に新しいグループ エントリが表示されます。

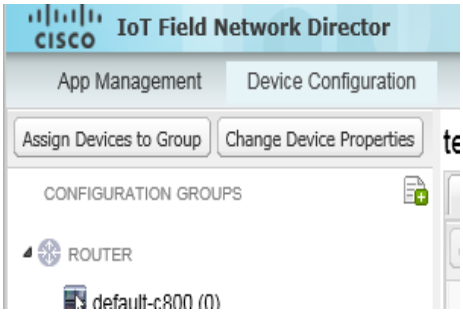
- グループの名前を変更する場合は、「デバイス設定グループの名前変更」を参照してください。
- グループを削除するには、「デバイス グループの削除」を参照してください。

デバイス設定プロパティの変更

デバイスの値を変更した Device Properties CSV ファイルをアップロードすることで、デバイスの設定可能なプロパティを変更できます。

デバイス設定プロパティを変更するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. [Change Device Properties] をクリックします。



3. [Browse] をクリックし、アップロードする Device Properties CSV ファイルを選択します。
4. [Change] をクリックします。
5. 終了したら、[Close] をクリックします。

- IoT FND の設定可能なデバイス プロパティのリストについては、「デバイス プロパティ」を参照してください。

別のグループへのデバイスの移動

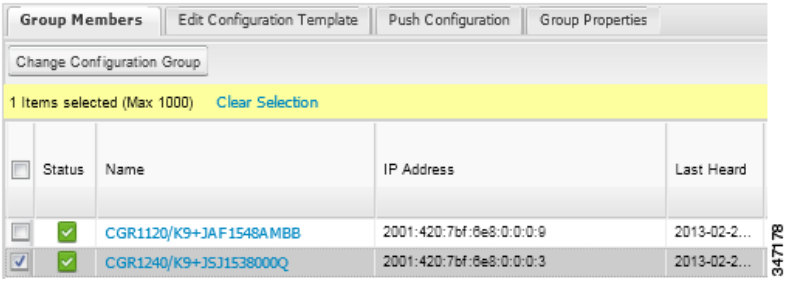
デバイスをグループ間で移動するには、次の 2 つの方法があります.

- 別の設定グループへのデバイスの手動による移動
- 他の設定グループへのデバイスの一括移動

別の設定グループへのデバイスの手動による移動

デバイスを別の設定グループに移動するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. 設定グループ(左ペイン)のリストからグループを選択します。
3. 移動するデバイスのチェックボックスを選択します。
4. [Change Configuration Group] をクリックします。



5. ダイアログボックスのドロップダウン メニューから、デバイスの移動先グループを選択します。
6. [Change Config Group] をクリックします。
7. [OK] をクリックします。

他の設定グループへのデバイスの一括移動

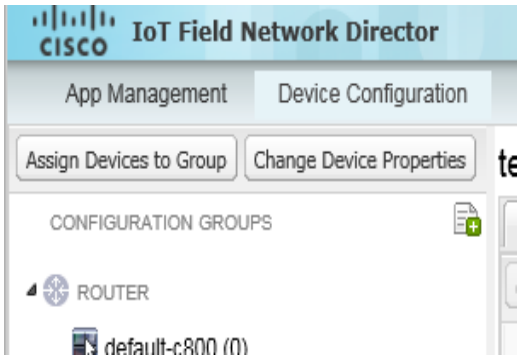
多数のデバイスをグループ間で移動する場合は、移動するデバイスのリストを含む CSV ファイルをインポートします。

たとえば、次の CSV ファイルは、3 つの CGR の EID の移動を指定しています。

```
eid
CGR1120/k9+JS1
CGR1120/k9+JS2
CGR1120/k9+JS3
```

デバイスを一括して他の設定グループに移動するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. [Assign Devices to Group] をクリックします。



3. [Browse] をクリックし、移動するデバイスのリストを含む CSV ファイルを検索し、[Open] をクリックします。

4. [Group] ドロップダウン メニューから、デバイスのターゲット グループを選択します。
5. [Change Group] をクリックします。
6. [OK] をクリックします。

設定グループ内のデバイスのリスト表示

設定グループ内のデバイスをリスト表示するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. 設定グループ（左ペイン）のリストからグループを選択します。
3. リスト内のデバイスについてさらに情報を取得するには、EID をクリックします。

定期的なインベントリ通知とマーク ダウン タイマーの設定

FAR の設定グループに対する定期的なインベントリ通知の間隔を、IoT FND がそれらの FAR を [Down] としてマーキングをするのに使用するロジックに影響を及ぼさずに変更することができます。ただし、これを実現するには、FAR グループに対する定期的な設定通知の頻度を、マーク ダウン タイマーよりも少なくなるように有効化する必要があります。

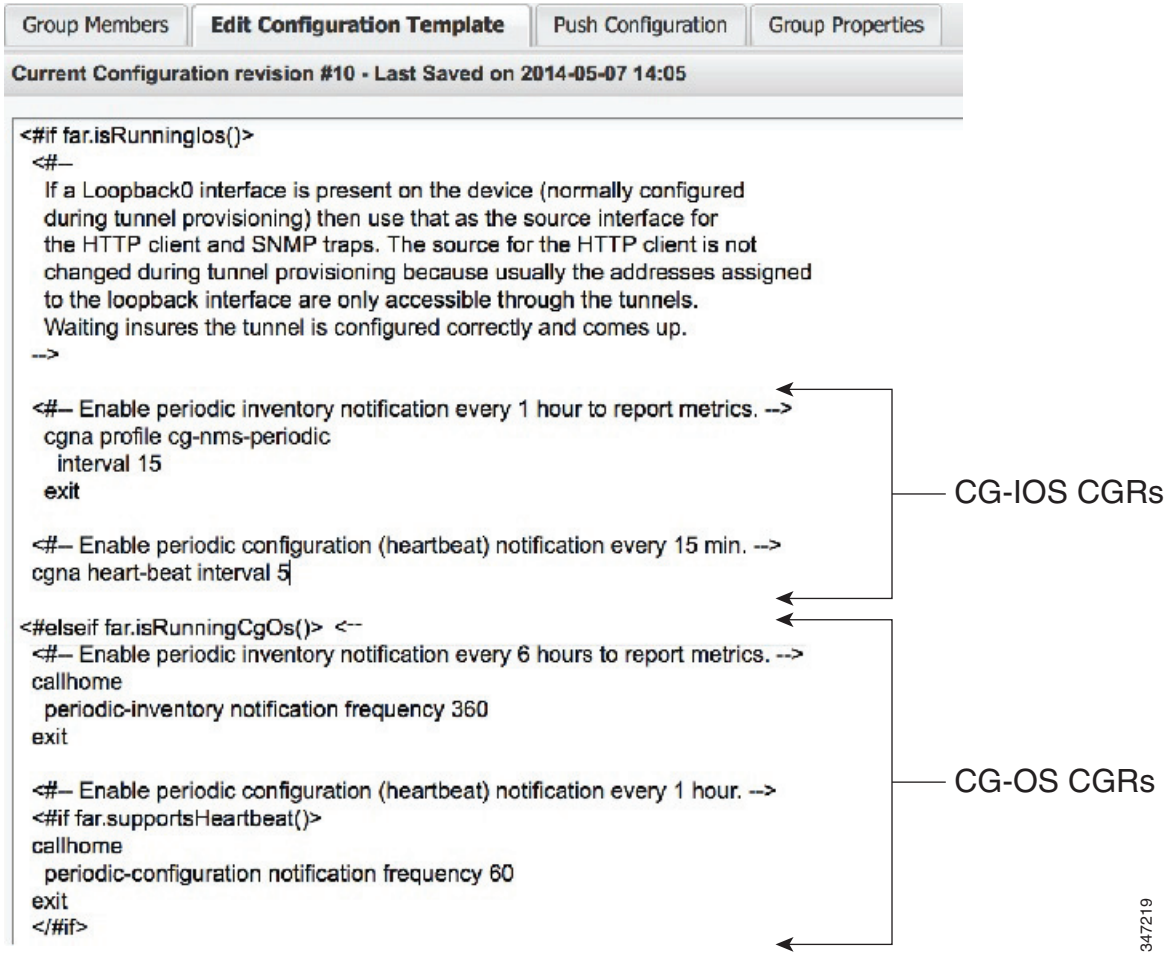
グループの [Group Properties] タブをクリックし、[Mark Routers Down After] フィールドの値を変更することにより、マーク ダウン タイマーを設定できます。

- 定期的なインベントリ通知の設定
- マーク ダウン タイマーの設定

定期的なインベントリ通知の設定

ROUTER 設定グループの定期的インベントリ通知間隔を設定するには、次の手順を実行します。

1. [Config] > [Device Configuration] をクリックします。
2. ROUTER 設定グループを選択します。
3. [Edit Configuration Template] をクリックします。



4. この手順は OS に固有のものです。

   - Cisco IOS CGR の場合は、**cgna heart-beat interval** のパラメータ値を変更します。時間の値は分単位です。

     たとえば、IOS CGR で定期的インベントリ通知が 20 分ごとにメトリックをレポートするようにするには、テンプレートに次の行を追加します。

     ```
     <#-- Enable periodic configuration (heartbeat) notification every 20 min. -->
     cgna heart-beat interval 20
     exit
     ```

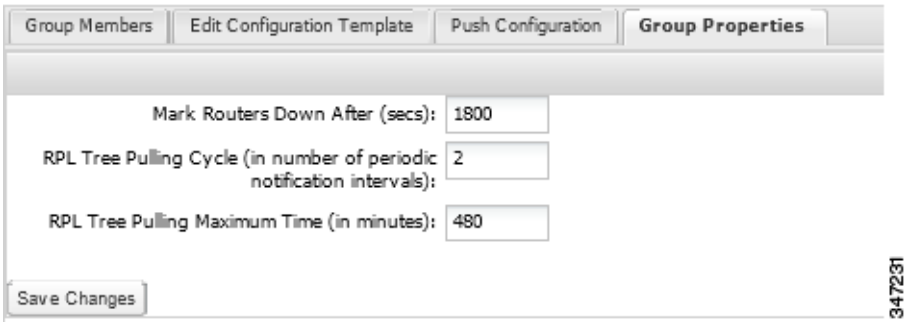
   - CG-OS CGR の場合は、**periodic-inventory notification frequency** のパラメータ値を新しい値に変更します。時間の値は分単位です。

5. [Save Changes] をクリックします。

マーク ダウン タイマーの設定

ROUTER 設定グループのマークダウン タイマーを設定するには、次の手順を実行します。

1. [Config] > [Device Configuration] をクリックします。
2. ROUTER 設定グループを選択します。
3. [Group Properties] をクリックします。



4. [Mark Routers Down After] フィールドに、定期的設定通知（ハートビート）が期間中に IoT FND に送信されなくなってから何秒後に IoT FND により FAR をダウンとしてマーキングするかを入力します。

   (注) ハートビート間隔対マーク ダウン タイマーは、1:3 の割合にすることをお勧めします。

5. [Save Changes] をクリックします。

6. 設定テンプレート内の定期的設定通知頻度が、[Mark Routers Down After] フィールドに入力した値よりも低く設定されていることを確認します。

   a. [Edit Configuration Template] をクリックします。

   b. 定期的設定通知頻度のパラメータ値が、[Mark Routers Down After] の値よりも低く設定されていることを確認します。

   通知の値には、最大でマークダウンの値の 3 分の 1 の値を使用します。たとえば、マークダウンの値として 3600 秒（60 分）を選択した場合、定期的設定通知頻度のパラメータは 20 分に設定します。

```
<#-- Enable periodic configuration (heartbeat) notification every 20 minutes.-->
<#if far.supportsHeartbeat()>
callhome
  periodic-configuration notification frequency 20
exit
</#if>
```

   (注) 定期的インベントリ通知間隔および定期的設定通知頻度を制御する機能は、CGR イメージ バージョン 3.2 に適用されます。

デバイス設定グループの名前変更

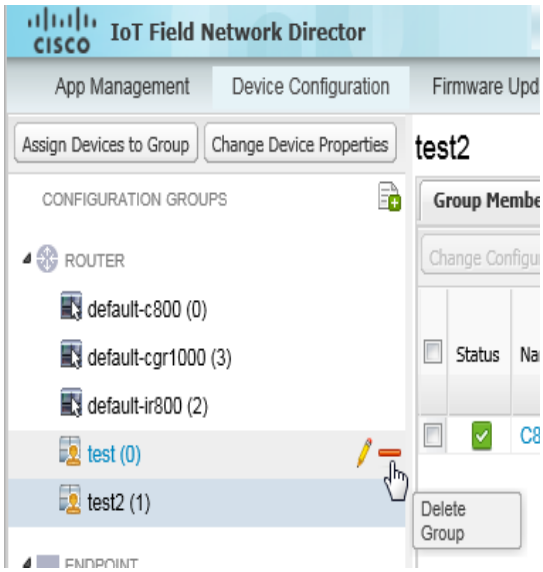
デバイス設定グループの名前を変更するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。

2. 設定グループ（左ペイン）のリストからグループを選択します。

3. [Edit Group] アイコンをクリックします。

   リスト内のグループ名の上にマウスポインタを置くと、[Edit Group] ボタンは鉛筆アイコンとして表示されます。



4. [Rename Group] ダイアログボックスに新しい名前を入力し、[OK] をクリックします。

(注) 無効な文字(「=」、「+」、「~」など)を入力すると、IoT FND は赤色のアラート アイコンを表示し、該当するフィールドを赤色で強調表示し、さらに [OK] ボタンを無効にします。

デバイス グループの削除

(注) グループを削除する前に、そのグループ内のすべてのデバイスを他のグループに移動してください。空でないグループは削除できません。

設定グループを削除するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. 設定グループ(左ペイン)のリストからグループを選択します。
3. グループが空であることを確認します。
4. [Delete Group](Ell)をクリックします。

   リスト内のグループ名の上にマウスポインタを置くと、[Delete] アイコンは赤色のマイナス記号として表示されます。
5. [Yes] をクリックして確定し、[OK] をクリックします。

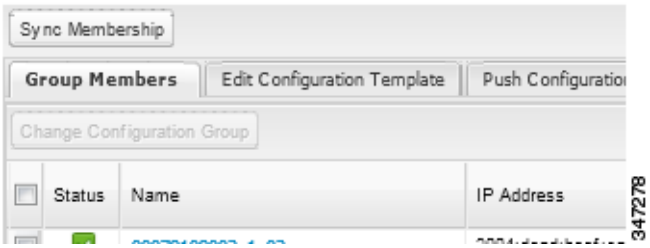
エンドポイント メンバーシップの同期

ME は、それが属する IoT FND グループに関する情報を維持します。グループ情報が変更されると、ME は非同期の状態になります。たとえば、ME グループの名前を変更しても、グループのメンバーは(たとえば、パケット損失が原因で)すぐには変更されない場合があります。デバイスが同期されていないと、IoT FND によりグループに対して実行した操作がデバイスに到達しません。ME を同期の状態に維持するには、[Sync Membership] ボタンを使用して、グループ情報をグループ メンバーにプッシュします。

グループ情報を ME に送信するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. ENDPOINT グループ(左ペイン)を選択します。
3. 同期するグループ内のメンバーのチェックボックスを選択します。

4. [Sync Membership] をクリックします。



5. グループのメンバーシップを同期するよう求められたら、[Yes] をクリックします。
6. [OK] をクリックします。

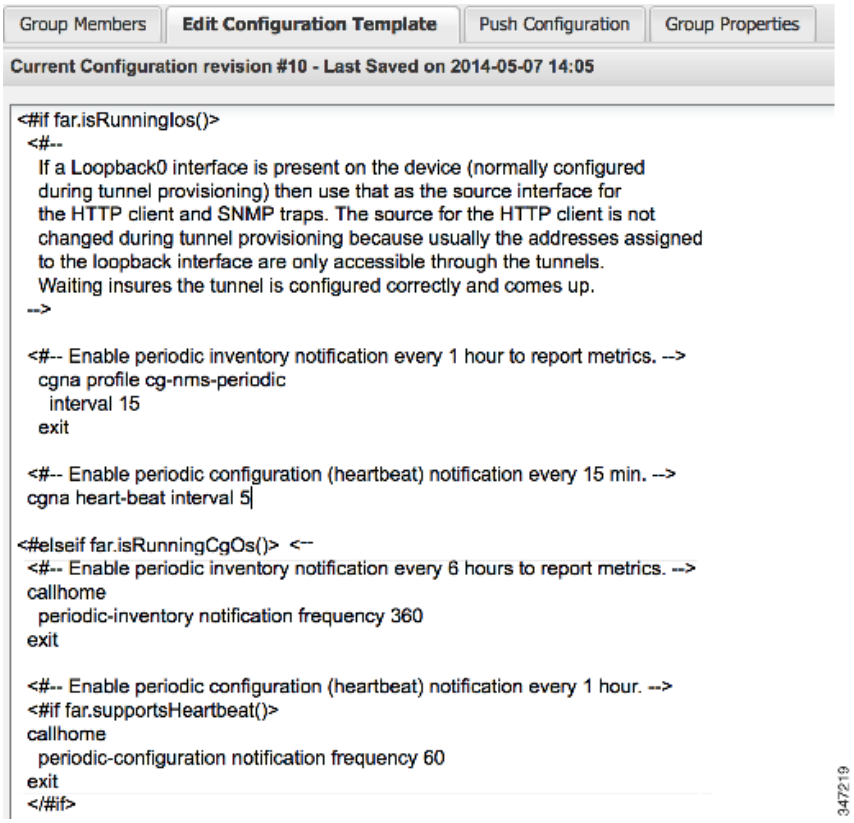
デバイスが最初に同期されるのは、IoT FND に登録した後です。

ROUTER 設定テンプレートの編集

IoT FND では、設定テンプレートを使用して、FAR を一括して設定することができます。FAR を IoT FND に登録すると、IoT Field Network Director はデフォルト テンプレートで定義されている設定をデバイスにプッシュし、変更内容をルータのスタートアップ設定にコミットします。次に、IoT FND はルータから実行中の設定を取得し、その後デバイスのステータスを [Up] に変更します。

ROUTER グループの設定テンプレートを編集するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. [CONFIGURATION GROUPS]（左ペイン）で、編集するテンプレートを含むグループを選択します。
3. [Edit Configuration Template] をクリックします。



4. テンプレートを編集します。

   テンプレートは FreeMarker 構文で表示されます。FreeMarker の詳細については、「トンネル プロビジョニング テンプレートのシンタックス」を参照してください。

   (注) ルータの設定テンプレートは、入力した設定データを確認しません。保存する前に設定を確認してください。

5. [Save Changes] をクリックします。

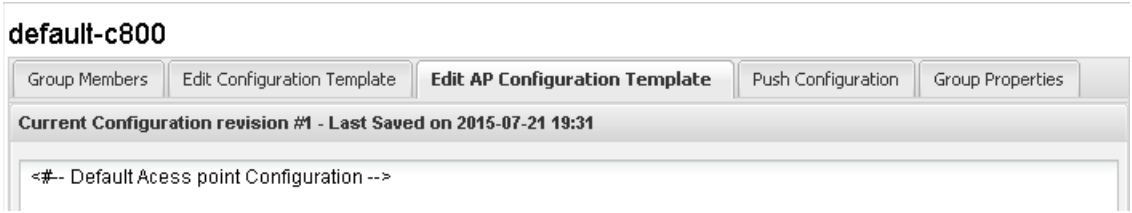
IoT FND は変更内容をデータベースにコミットし、テンプレートのバージョン番号を増やします。

AP 設定テンプレートの編集

IoT FND では、設定テンプレートを使用して、AP を一括して設定することができます。AP を IoT FND に登録すると、デフォルト テンプレートで定義されている設定がデバイスに適用され、変更内容がスタートアップ設定にコミットされます。次に、IoT FND は AP から実行中の設定を取得し、その後デバイスのステータスを [Up] に変更します。

AP グループの設定テンプレートを編集するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. [CONFIGURATION GROUPS] (左ペイン) で、編集するテンプレートを含む組み込み AP デバイスを含む C800 デバイス グループを選択します。
3. [Edit AP Configuration Template] をクリックします。



4. テンプレートを編集します。

   テンプレートは FreeMarker 構文で表示されます。FreeMarker の詳細については、「トンネル プロビジョニング テンプレートのシンタックス」を参照してください。

   AP テンプレートの例

```
ip dhcp pool TEST_POOL
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 lease infinite
!
dot11 ssid GUEST_SSID
authentication open
authentication key-management wpa
wpa-psk ascii 0 12345678
guest-mode
!
interface Dot11Radio0
no ip address
encryption mode ciphers aes-ccm
ssid GUEST_SSID
!
interface Dot11Radio0
no ip address
encryption mode ciphers aes-ccm
```

```
ssid GUEST_SSID
```

(注) AP の設定テンプレートは、入力した設定データを確認しません。保存する前に設定を確認してください。

5. [Save Changes] をクリックします。

IoT FND はデータベースに変更内容をコミットし、テンプレートのリビジョン番号を増やします。

デュアル PHY サポートの有効化

CGR マスターおよびスレーブ インターフェイスを設定することができます。デュアル PHY WPAN インターフェイスの設定の詳細については、『Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide (Cisco IOS)』を参照してください。

ルータ GPS トラッキングの有効化

GPS トラップを有効化することにより、ルータが距離のしきい値、時間のしきい値、またはその両方を移動した場合に、イベントをトリガーできます。たとえば、距離のしきい値をモニタする固定のポール トップ CGR を設定して、盗難またはポール インシデントによる動きを検出するか、またはモバイル ルータの場合は、両方のしきい値を設定して継時的な距離を判定します。推奨される距離のしきい値は 100 フィート(30 m)です。

GPS トラップを有効にするには、デフォルト設定テンプレートの次の行をアンコメントします。

```
<#--
Enable the following configurations to generate events that track if the router
moves by a certain distance (unit configurable) or within a certain time (in minutes)
-->
<#-- cgna geo-fence interval 10 -->
<#-- cgna geo-fence distance-threshold 100 -->
<#-- cgna geo-fence threshold-unit foot -->
<#-- cgna geo-fence active -->
```

ヒント:GPS トラップは情報ログだけを生成するため、高い重大度([CRITICAL] など)のルール ベースのイベントを作成して、ルータの動きを管理者に知らせることを推奨します。このタイプのルールはたとえば次のように定義されます:configGroup:name eventName:deviceLocChanged(「ルールの追加」を参照)。

SNMP v3 情報イベントの設定

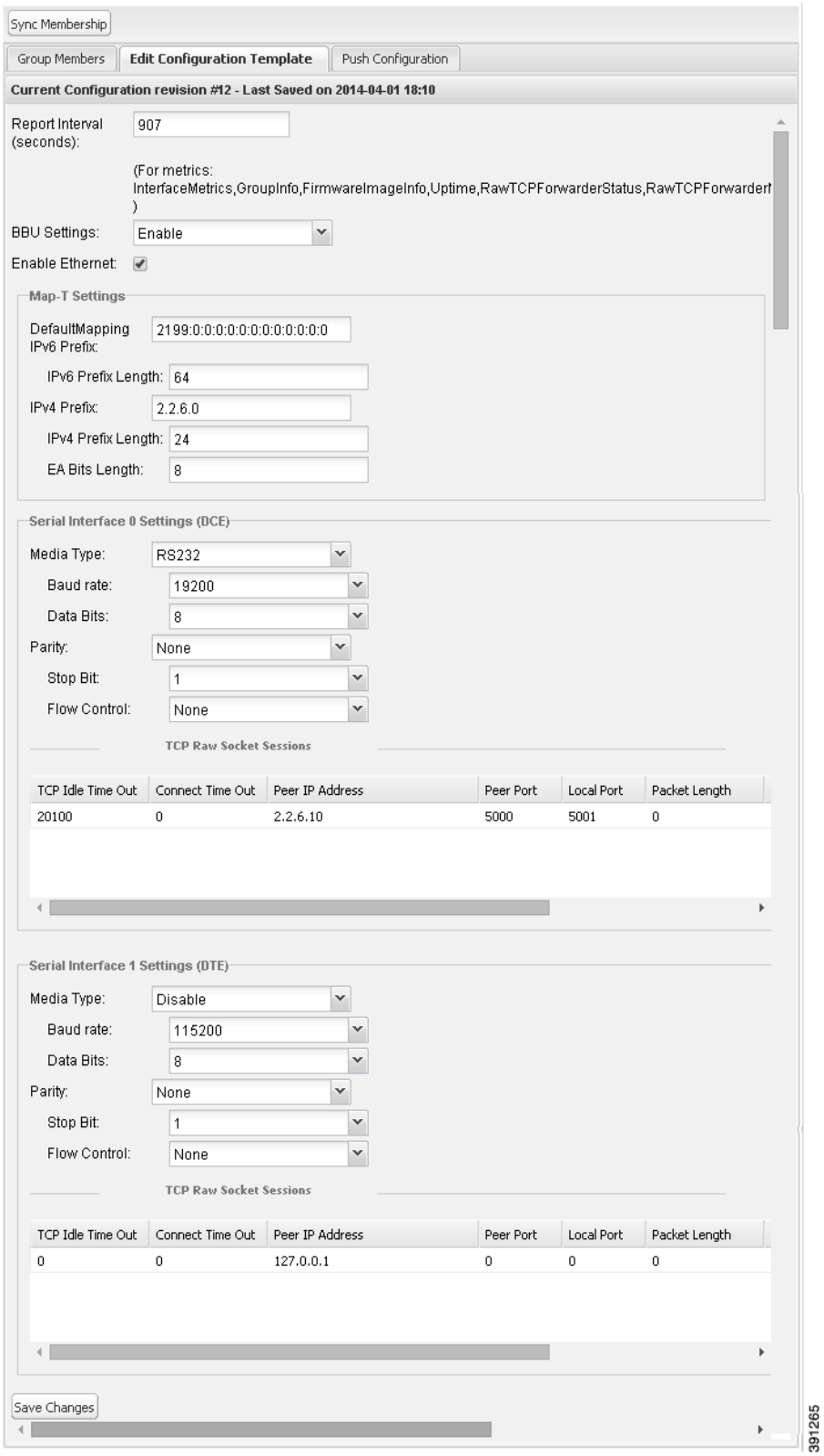
Cisco IOS ルータで、SNMP v3 情報イベントを設定して、デフォルトの SNMP v3 トラップを置き換えます。CG-OS ではデフォルトで、ルータ上にトラップを生成する IoT FND イベント関連の変更に対して SNMP v3 トラップが設定されます。IoT FND は、これらのトラップを対応するイベントにマッピングします。Cisco IOS ルータでは、これらの SNMP v3 トラップを SNMP v3 情報イベントに変換することにより、ルータからイベントを受信するたびにルータに確認が送信されます。これにより、ルータはトラップが IoT FND により受信されたことを確認します。SNMP v3 情報イベントを有効にするには、デフォルトの設定ファイルで次の行をアンコメントして、新しい設定ファイルをグループ内のすべてのルータにプッシュします。

```
<#-- Enable the following configurations for the nms host to receive informs instead of traps -->
<#-- no snmp-server host ${nms.host} traps version 3 priv ${far.adminUsername} -->
<#-- snmp-server engineID remote ${nms.host} ${nms.localEngineID} -->
<#-- snmp-server user ${far.adminUsername} cgnms remote ${nms.host} v3 auth sha ${far.adminPassword} priv aes
256 ${far.adminPassword} -->
<#-- snmp-server host ${nms.host} informs version 3 priv ${far.adminUsername} -->
```

ENDPOINT 設定テンプレートの編集

ENDPOINT 設定テンプレートを編集するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. [CONFIGURATION GROUPS](左ペイン)で、編集するテンプレートを含む ENDPOINT グループを選択します。
3. [Edit Configuration Template] をクリックします。


Sync Membership
Group Members
Edit Configuration Template
Push Configuration
Current Configuration revision #12 - Last Saved on 2014-04-01 18:10
Report Interval (seconds):
907
(For metrics: InterfaceMetrics,GroupInfo,FirmwareImageInfo,Uptime,RawTCPForwarderStatus,RawTCPForwarderI)
BBU Settings:
Enable
Enable Ethernet:
Map-T Settings
DefaultMapping IPv6 Prefix:
2199:0:0:0:0:0:0:0:0:0:0:0
IPv6 Prefix Length:
64
IPv4 Prefix:
2.2.6.0
IPv4 Prefix Length:
24
EA Bits Length:
8
Serial Interface 0 Settings (DCE)
Media Type:
RS232
Baud rate:
19200
Data Bits:
8
Parity:
None
Stop Bit:
1
Flow Control:
None
TCP Raw Socket Sessions
TCP Idle Time Out
Connect Time Out
Peer IP Address
Peer Port
Local Port
Packet Length
20100
0
2.2.6.10
5000
5001
0
Serial Interface 1 Settings (DTE)
Media Type:
Disable
Baud rate:
115200
Data Bits:
8
Parity:
None
Stop Bit:
1
Flow Control:
None
TCP Raw Socket Sessions
TCP Idle Time Out
Connect Time Out
Peer IP Address
Peer Port
Local Port
Packet Length
0
0
127.0.0.1
0
0
0
Save Changes
391265

4. テンプレートを編集します。

   たとえば、[Report Interval] フィールドに、データの更新間隔を秒数で入力できます。デフォルトで、ME は 28,800 秒（8 時間）ごとに新しいメトリック セットを送信します。

   [Edit Configuration Templates] タブでは、次の値を変更できます。

   - Report Interval：データの更新間隔の秒数。
   - BBU Settings：このオプションを有効にすると、バッテリ バックアップ ユニットによる Range Extender の BBU 設定を設定できます。
   - Enable Ethernet：選択したデバイスのイーサネットを有効にするか、または選択した DA ゲートウェイ デバイスで NAT 44 設定を設定するには、このチェックボックスをオンにします。

     （注）NAT 44 設定では、CSV ファイル内のすべての 3 つのフィールドに値を指定する必要があります。デフォルト値はそれぞれ、127.0.0.1、0、0 です。特定のマップ インデックスでは他の設定は必要ありません。これらの設定は、マップ インデックスで無効な場合、設定のプッシュ時に無視されます。
   - MAP-T Settings：デバイスの iPv6 および iPv4 設定。

     （注）Cisco IOS CGR では、MAP-T ルールは、MAP-T IPv6 の基本マッピング ルール（BMR）、IPv4 の BMR、および IPv6 のデフォルト マッピング ルール（DMR）を指定することによって設定されます。Cisco IR509 デバイスでは、MAP-T IPv6 は、MAP-T BMR IPv6 ルール、IPv4 サフィックス値、および BMR EA 長さ値に基づく長さを統合する IPv6 プレフィックスです。
   - Serial Interface 0 (DCE) Settings：選択したデバイスのデータ通信装置（DCE）通信の設定。

     （注）1 つのシリアル インターフェイスは 1 つのセッションでのみ使用できます。選択した DA ゲートウェイ デバイスの（各仮想回線とシリアル ポートの）すべての TCP raw ソケット セッションに対し、次のパラメータを設定する必要があります。
   - イニシエータ：デバイスをクライアント/サーバとして指定します。
   - TCP アイドル タイムアウト（分）：アイドル接続を維持するよう時間を設定します。
   - ローカル ポート：デバイスのポート番号を設定します。
   - ピアポート：デバイスに接続されているクライアント/サーバのポート番号を設定します。
   - ピア IP アドレス：デバイスに接続されているホストの IP アドレスを設定します。
   - 接続タイムアウト：イニシエータの DA ゲートウェイ デバイスの TCP クライアント接続タイムアウトを設定します。
   - パケット長：TCP パケットに変換するシリアル データの最大長を設定します。
   - パケット タイマー（ms）：TCP パケットの各作成間の時間間隔を設定します。
   - 特殊文字：TCP パケット作成のデリミタを設定します。
   - Serial Interface 1 (DTE) Settings：選択したデバイスのデータ端末装置（DTE）通信の設定。

     （注）IPv6 プレフィックスは有効である必要があります。最大プレフィックス長は次のとおりです。
     - IPv6: 0–128
     - IPv4: 0–32

5. [Save Changes] をクリックします。

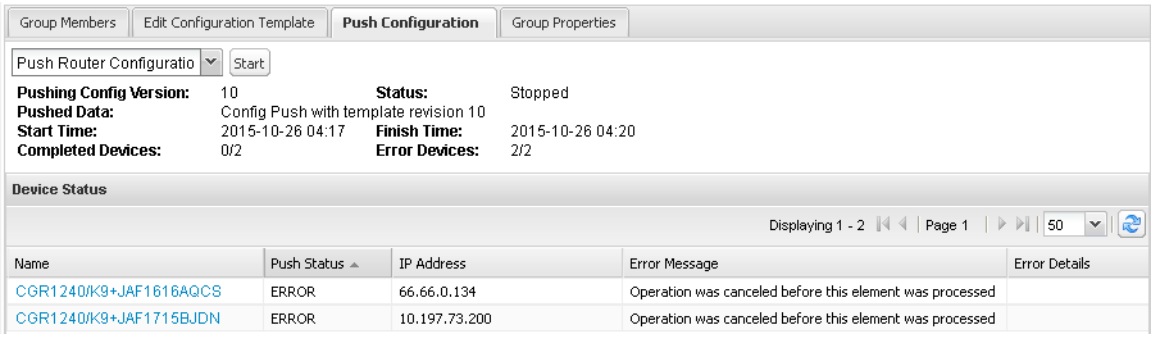
IoT FND は変更内容をデータベースにコミットし、バージョン番号を増やします。

FAR への設定のプッシュ

（注）CGR、C800、IR800、および ISR 800 をネットワーク上に共存させることができます。ただし、両方のルータ タイプを含むカスタム設定テンプレートを作成する必要があります。

FAR に設定をプッシュするには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. グループまたはグループのサブセットを選択し、設定を [CONFIGURATION GROUPS] ペインにプッシュします。
3. [Push Configuration] タブをクリックします。



4. [Select Operation] ドロップダウン メニューで、[Push Router Configuration] を選択します。

   組み込み AP デバイスを含む C800 および IR800 グループの場合は、[Push AP Configuration] を選択して、AP 設定テンプレートをプッシュします。

5. [Start] をクリックします。

   [Push Configuration] ページに、グループ内のすべてのデバイスのプッシュ操作のステータスが表示されます。デバイスに設定をプッシュしているときにエラーが発生すると、エラーおよびその詳細が関連のカラムに表示されます。

   [Status] カラムに、次のいずれかの値が表示されます。

   - NOT_STARTED：設定のプッシュが開始されていません。
   - RUNNING：設定のプッシュが進行中です。
   - PAUSED：設定のプッシュが一時停止されています。アクティブな設定操作は完了しますが、キューに置かれた設定操作は開始されません。
   - STOPPED：設定のプッシュは停止しました。アクティブな設定操作は完了しますが、キューに置かれた設定操作は開始されません。
   - FINISHED：すべてのデバイスへの設定のプッシュが完了しました。
   - STOPPING：設定のプッシュは停止の処理中です。アクティブな設定操作は完了しますが、キューに置かれた設定操作は開始されません。
   - PAUSING：設定のプッシュは休止の処理中です。アクティブな設定操作は完了しますが、キューに置かれた設定操作は開始されません。

ヒント：ステータス情報を更新するには、[Refresh] ボタンをクリックします。

CGR SD カードのパスワード保護の有効化

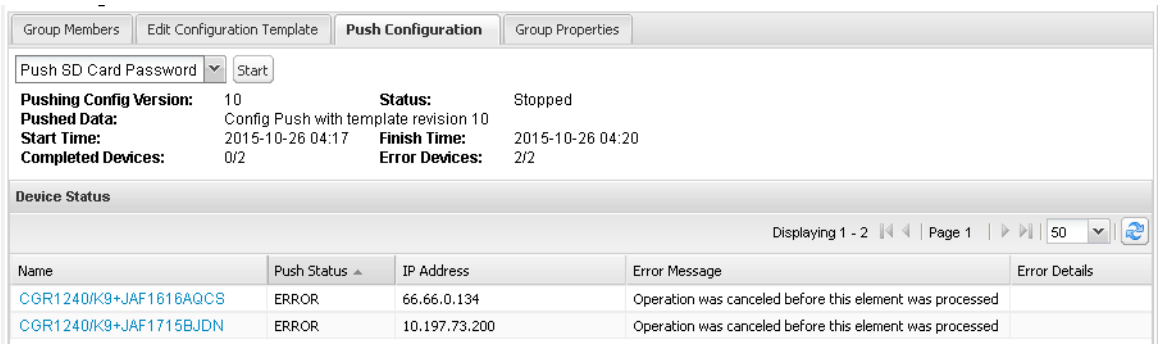
CGR SD カードのパスワード保護により、不正アクセスを防止し、CGR SD カードを他のパスワードで他のシステムに転用することを防ぐことができます。

（注）これは、C800 および IR800 には適用されません。

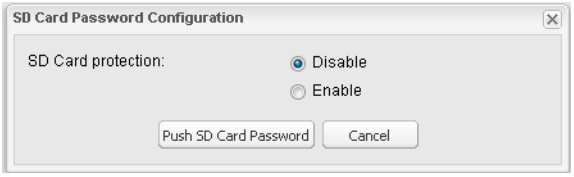
[Device Info] ペインの [Inventory] セクションに、CGR SD カードのパスワード保護のステータスが表示されます。[Config Properties] タブの [Router Credentials] セクションには、SD カードのパスワードが表示されます。

CGR SD カードのパスワード保護を有効にするには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. CGR グループまたは CGR を選択し、設定を [CONFIGURATION GROUPS] ペインにプッシュします。
3. [Push Configuration] タブを選択します。



4. [Select Operation] ドロップダウン メニューで、[Push SD Card Password] を選択します。
5. [Start] をクリックします。
6. [SD Card protection] > [Enable] を選択します。



7. 目的の保護の方法を選択します。
   - Property: このパスワードは、CSV または XML ファイル、あるいは Notification Of Shipment ファイルを使用して設定されます。
   - Randomly Generated Password: パスワード長を入力します。
   - Static Password: パスワードを入力します。
8. [Push SD Card Password] をクリックします。

メッシュ エンドポイントへの設定のプッシュ

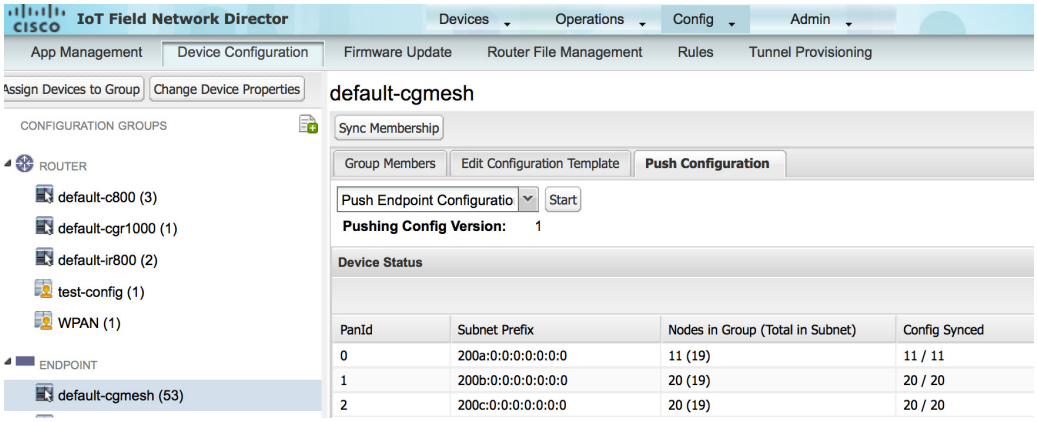
メッシュ エンドポイントに設定をプッシュするには、次の手順を実行します。

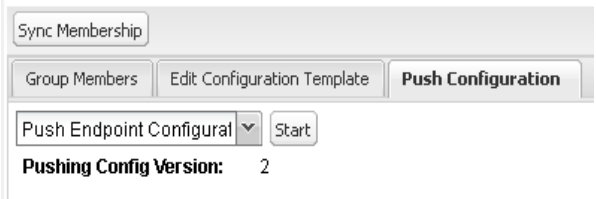
1. [Config] > [Device Configuration] を選択します。
2. グループまたはグループのサブセットを選択し、設定を [ENDPOINT] リストにプッシュします。

3. [Push Configuration] タブをクリックします。

   (注) [Push Configuration] タブは、以下に概略を示す cgmesh エンドポイントのサブネット ビューをサポートします。

Pan ID	エンドポイント(ノード)のグループのパーソナル エリア ネットワーク ID (PAN ID)を示します。
Subnet Prefix	エンドポイントの IPv6 サブネット プレフィックスを示します。
Nodes in Group	グループ内のノードの数。上の例では、グループ内には合計 51 のノードがあり、それらは 3 つの異なるサブネットに分割されています。
Total in Subnet	サブネット内のノードの数。上の例では、サブネット内には 19 のノードがあります。
Config Synced	Pan 内の全ノードのうち、設定のプッシュが処理中であるかまたは終了している Pan ID 内のノードの数を示します。





4. [Select Operation] ドロップダウン メニューで、[Push Endpoint Configuration] を選択します。

5. [Start] をクリックします。

   [Push Configuration] ページに、グループ内のすべてのデバイスのプッシュ操作のステータスが表示されます。デバイスに設定をプッシュしているときにエラーが発生すると、エラーおよびその詳細が関連のカラムに表示されます。

   [Status] カラムに、次のいずれかの値が表示されます。

   - NOT_STARTED:設定のプッシュが開始されていません。
   - RUNNING:設定のプッシュが進行中です。
   - PAUSED:設定のプッシュが一時停止されています。アクティブな設定操作は完了しますが、キューに置かれた設定操作は開始されません。

- STOPPED：設定のプッシュは停止しました。アクティブな設定操作は完了しますが、キューに置かれた設定操作は開始されません。
- FINISHED：すべてのデバイスへの設定のプッシュが完了しました。
- STOPPING：設定のプッシュは停止の処理中です。アクティブな設定操作は完了しますが、キューに置かれた設定操作は開始されません。
- PAUSING：設定のプッシュは休止の処理中です。アクティブな設定操作は完了しますが、キューに置かれた設定操作は開始されません。

ステータス情報を更新するには、[Refresh] ボタンをクリックします。

ゲスト OS の管理

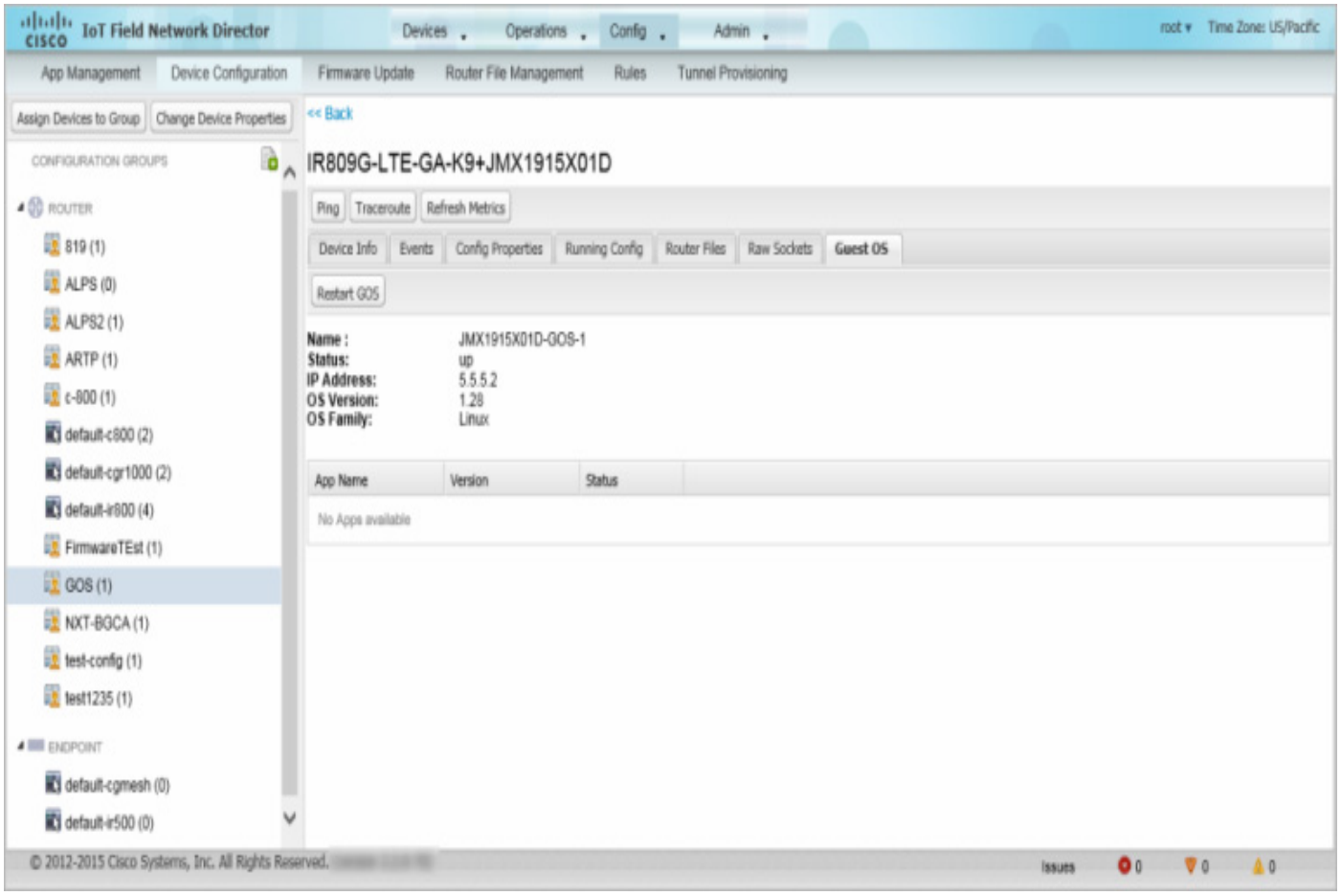
Cisco IOS CGR は仮想マシンをサポートし、Cisco IOS 仮想マシンの横で実行中のゲスト OS（GOS）インスタンスでアプリケーションを実行します。GOS は、Linux です。GOS 上で動作するアプリケーションは通常、モニタリングおよびアカウンティング目的で、フィールドから統計情報を収集します。Cisco IOS ファームウェア バンドルでは、CGR 上の VM インスタンスに参照 GOS がインストールされます。IoT FND は、GOS で、次のロールベースの機能をサポートします。

- GOS ステータスのモニタリング
- GOS アプリケーションの管理
- Cisco IOS ファームウェア バンドル内の参照 GOS のアップグレード

  （注）IoT FND は、シスコが提供している参照 GOS のみをサポートします。

GOS は、[Guest OS] タブの [Config] > [Device Configuration] ページで管理およびモニタします。

図 6　[Config] > [Device Configuration] ページ、[Guest OS] タブの [Restart GOS] ボタン



この項では、次のトピックについて取り上げます。

- GOS のインストール
- GOS アプリケーションの管理
- ゲスト OS の再起動

GOS のインストール

CGR の工場出荷時の設定によっては、GOS は VM インスタンス内に存在します。GOS は、Cisco IOS ファームウェア バンドルとともにインストールされます（「FAR ファームウェアのアップデート」セクション（-259ページ）を参照）。Cisco IOS イメージ バンドルのインストールまたはアップグレードを実行すると、GOS、ハイパーバイザ、Cisco IOS イメージがすべてアップグレードされます。

IoT FND は、Cisco IOS のインストールまたはアップデート後に GOS を検出すると、必要な設定を行う前に通信の初期設定が完了しているかどうかをチェックします。CGR は、DHCP プール、および IP アドレスを提供しゲスト OS のゲートウェイとして機能するように設定されているギガビット イーサネット 0/1 インターフェイスを備えている必要があります。CGR の設定の詳細については、*Cisco 1000 Series Connected Grid Routers Configuration Guides* Web ポータルを参照してください。

(注) VM インストールに Cisco OS 以外 がインストールされていることを IoT FND が検出すると、ファームウェア バンドルのアップロードおよび Cisco の参照 GOS のインストールは実行されません。

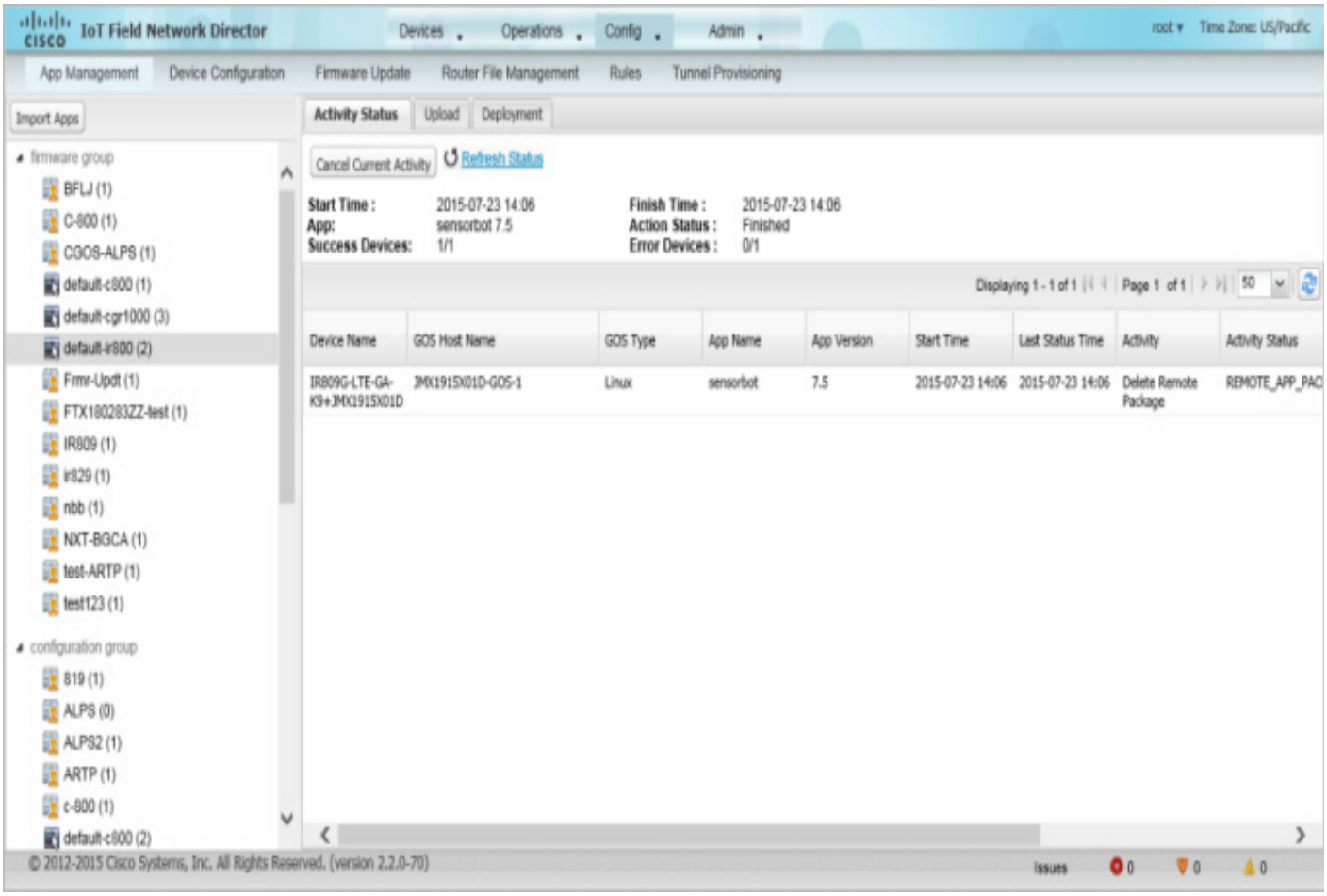
GOS アプリケーションの管理

アプリケーションは VM インスタンス上で実行されますが、Cisco IOS ファームウェア バンドルには組み込まれません。GOS アプリケーションは、標準の *app-<appname>-ver-<version>*.zip ファイルとして配布し、[Config] > [App Management] ページの使用により、アップロード、インストール、開始/停止、およびアンインストールします。IoT FND の内部バックアップおよび復元メカニズムにより、アップグレード中、既存のアプリケーションは保持されます。

(注) IoT FND の GOS 通信（SSH を使用した GOS へのアプリケーションのアップロードなど）では、gosPassword を CGR プロパティ ファイルにする必要があります。プロパティ ファイルを CSV/XML アップロード内にアップロードします。gosPassword プロパティがないと、IoT FND は GOS にアプリケーションをアップロードできません。

[GOS Application Management] ロールが有効になっているユーザは、ネットワーク内の Cisco IOS CGR で、アプリケーションをアップロード、インストール、および導入することができます。

図 7　　[Config] > [Apps Management] ページの最後のジョブのステータス



GOS アプリケーション アクティビティの管理

[Config] > [App Management Activity Status] タブで、アプリのアクティビティ（ジョブ）を管理できます。一番上のペイン（デバイス リストの上）に、最後のアクティビティのジョブに関する次のような情報が表示されます。

- 最後のアクティビティの開始時間と停止時間。
- アプリケーション名。
- アクティビティのステータス。
- 成功したデバイスの数と失敗したデバイスの数。

表 8 に、[Activity Status] タブにあるデバイス リストに表示されるフィールドを示します。

表 8　　[Activity Status] タブ

フィールド	説明
デバイス名（Device Name）	選択したデバイスの名前。
GOS Host Name	GOS ホストの名前。
App Name	アプリケーションの名前。
App Version	アプリケーションに割り当てられているバージョン。
Start Time	選択したアクティビティの開始。
Last Status Time	最後のステータスの更新時刻。
アクティブな状態	選択したアクティビティ。Upload、Set to Run、Install、Start、Stop、Uninstall、および Delete Remote Package。
Activity Status	選択したアクティビティのステータス。
Progress	完了したかアクティビティの数。
メッセージ	アクティビティによって生成されたメモ。
Error Details	アクティビティの途中で発生したエラーの詳細。

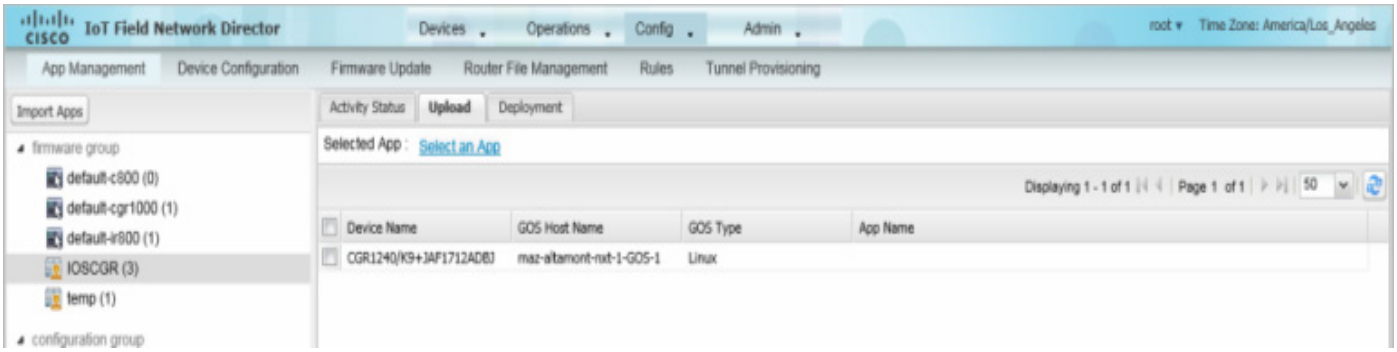
[Activity Status] タブでは、次の操作も行うことができます。

- [Cancel Current Activity] ボタンをクリックして、任意のアクティビティをキャンセルする。進行中の任意のアクティビティをキャンセルできます。
- [Refresh Status] ボタンをクリックして、アクティビティ ステータスを更新します。

GOS アプリケーションのアップロード

GOS アプリケーションを IoT FND にインポートした後は、Cisco IOS CGR および IR800 に導入するために、[Config] > [Apps Management] ページの [Upload] タブを使用して GOS アプリケーションをアップロードすることができます（図 8）。アプリケーションは OS に固有のものです。GOS が Linux の場合、アップロードしたすべてのアプリケーションが Linux 上でで実行される必要があります。

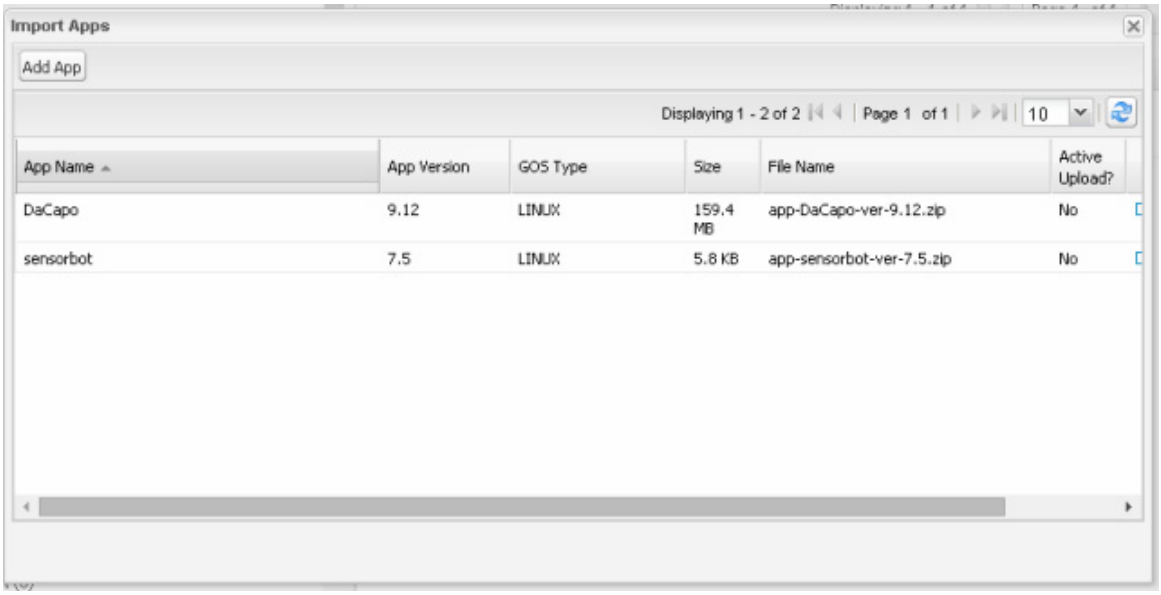
図 8　[Upload] タブ



アプリケーションを IoT FND にアップロードして Cisco IOS CGR および IR800 に導入するには、[Config] > [Apps Management] ページで次の手順を実行します。

1. 左ペインで、ファームウェアまたは設定グループを選択します。
2. [Upload] タブをクリックします。
3. [Select an App] をクリックするか、または左ペインの [Import Apps] ボタンをクリックします。

   [Import Apps] ダイアログボックスに、すでに NMS サーバにアップロードされているアプリケーションが表示されます。



4. [Import Apps] ダイアログボックスで、[Add App] をクリックします。
5. [Add App] ダイアログボックスで、[Browse] をクリックし、目的のアプリケーションを含むディレクトリに移動します。

   (注) アプリケーションは標準の *<appname>-<version>*.zip ファイル形式である必要があります。
6. [Open] ダイアログ ボックスで、アプリケーション ファイルを選択し、[Open] をクリックします。
7. [Add File] をクリックします。

   (注) 一度に追加できるアプリケーションは 1 つのみです。

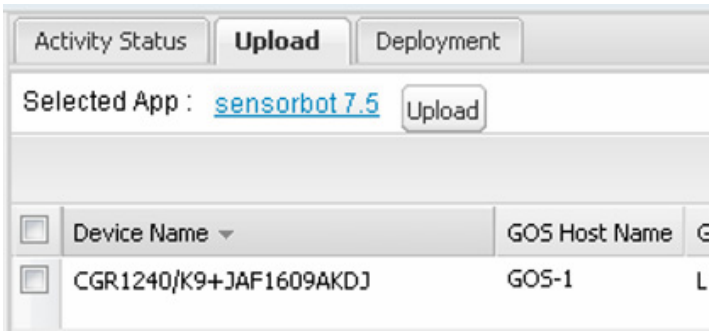
   アプリケーション ファイルは NMS サーバにアップロードされ、[App Name] リストに表示されます。

8. [Add App] ダイアログボックスで CGR にアップロードするアプリケーションをクリックし、[Add to Upload] をクリックしてから [OK] をクリックします。

   [App Name] リストにアプリケーションのファイル名が表示されます。

9. [App Name] リストで、アップロードするアプリケーションを選択します。

   [Upload] の [Selected App] フィールドに、アプリケーションのファイル名（次の例では、sensorbot 7.5）がリンク付きで表示されます。



10. [Upload] ボタンをクリックし、そのファイルを IoT FND にアップロードします。

アクティビティ ステータス（UPLOAD_OP_COMPLETE または UPLOAD_OP_WAITING）が [Upload] タブに表示されます。

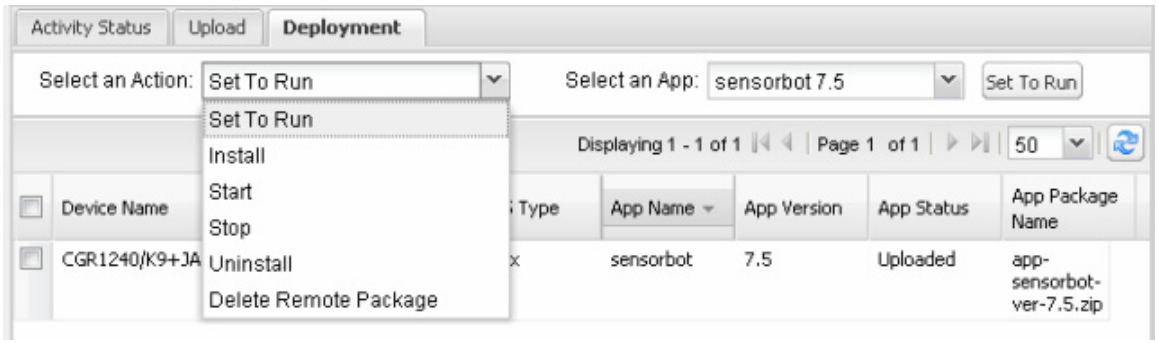
GOS アプリケーションの導入

[Config] > [App Management Deployment] タブを使用して、選択した CGR および IR800 で次のアクティビティを実行することができます。

- Set to Run：インストール操作と開始操作の組み合わせです。
- Install：リモート パッケージをインストールしてアプリケーションを解凍します。
- Start and Stop：アプリケーションを開始または停止します。
- Uninstall：アプリケーションをアンインストールします。
- Delete Remote Package：リポジトリから以前のアップロード パッケージを削除します。

選択した CGR に GOS アプリケーションを導入するには、次の手順を実行します。

1. [Config] > [Apps Management] ページの左ペインで、ファームウェアまたは設定グループを選択します。
2. [Deployment] タブをクリックします。
3. [Select an Action] ドロップダウン メニューから、選択したグループで実行するアクションを選択します。



選択したアクションが右側のアクション ボタンに反映されます(つまり、[Install] のアクションを選択すると、アクション ボタンのラベルは「Install」になります)。

4. [Select an App] ドロップダウン メニューで、1 つのアプリケーション、またはすべてのアプリケーションを選択します。
5. アクション ボタンをクリックします。

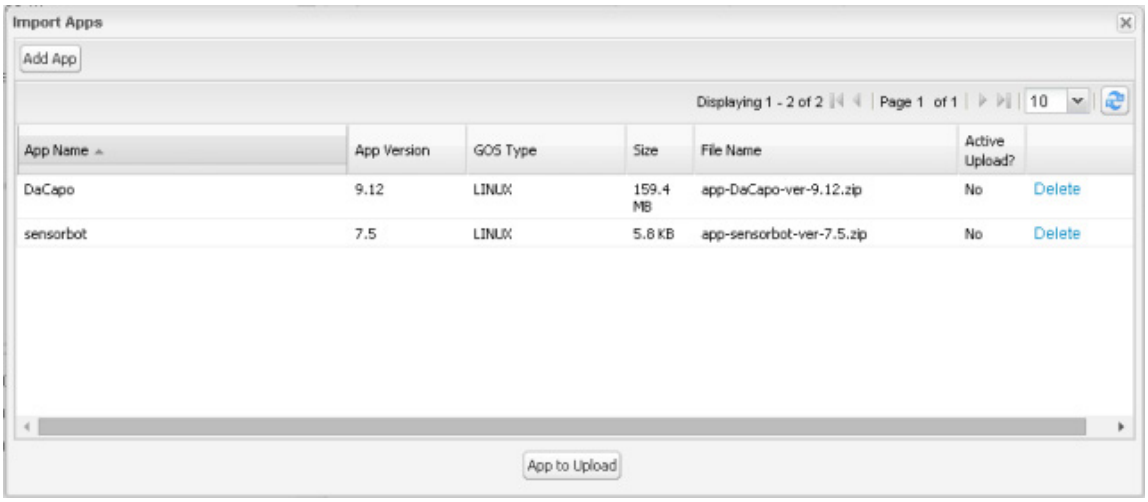
アクティビティが開始します。[Activity Status] タブでアクティビティの進行状況をモニタできます。

GOS アプリケーションの削除

NMS サーバからアプリケーションを削除するには、[Config] > [Apps Management] ページで次の手順を実行します。

1. 左ペインで、ファームウェアまたは設定グループを選択します。
2. [Upload] タブをクリックします。
3. [Select an App] をクリックするか、または左ペインの [Import Apps] ボタンをクリックします。

   [Import Apps] ダイアログボックスに、すでに NMS サーバにアップロードされているアプリケーションが表示されます。
4. [App Name] リストで右にスクロールし、該当のアプリケーションを含む行の [Delete] リンクをクリックして NMS サーバから削除します。



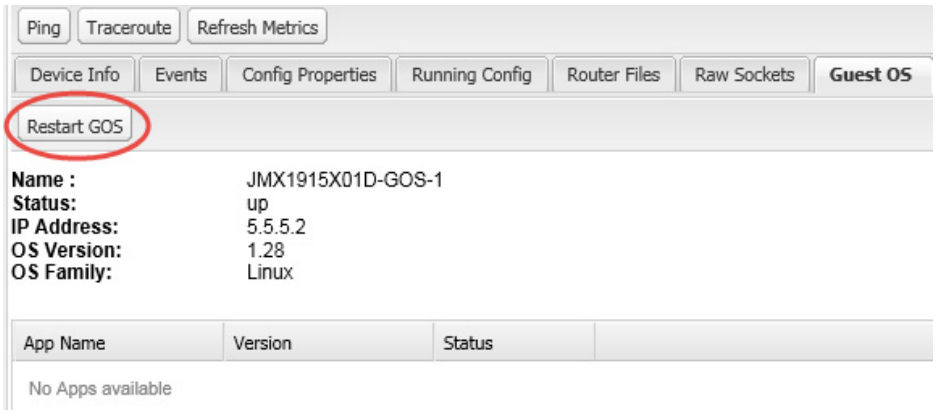
5. 確認ダイアログボックスで [OK] をクリックします。

ゲスト OS の再起動

GOS を再起動するには、[Config] > [Device Configuration] ページで次の手順を実行します。

1. [CONFIGURATION GROUPS] ペインで、再起動する GOS が置かれたデバイスを選択します。
2. [Guest OS] タブをクリックします。
3. [Restart] ボタンをクリックします（図 9）。

図 9　　[Config] > [Device Configuration] ページ：[Guest OS] タブの [Restart] ボタン



GOS 設定のプッシュ

IoT FND 設定テンプレートを使用して、CGR に GOS 設定をプッシュすることができます。これは、DHCP プールを設定する唯一の方法です。

ファイルの管理

[Config] > [Router File Management] ページを使用して、FAR 上で、デュアル バックホールおよび組み込み型イベント マネージャ（EEM）スクリプトを転送および実行しますTemplate モジュールでは、ファイルの検証を実行します。この項では、次のトピックについて取り上げます。

- ファイルのタイプと属性
- IoT FND へのファイルの追加
- ファイル転送
- ファイルの表示
- ファイルのモニタリング
- アクションのモニタリング
- ファイルの削除

（注）ファイル マネージャはロールに依存し、すべてのユーザが使用できるわけではありません。ロールの管理を参照してください。

ファイルのタイプと属性

FAR では、組み込みアプレットと個々に FAR で実行される Tool Command Language（TCL）スクリプトの 2 つのタイプの EEM スクリプトが使用されます。ファームウェアのアップグレードをしなくても、FAR 上で新しい EEM TCL スクリプトをアップロードして実行できます。EEM ファイルは、*eem* ディレクトリに FAR フラッシュ メモリをアップロードします。これらのスクリプトは、[Import File] ページの [File Type] カラムに *eem script* として表示されます。EEM TCL スクリプトを有効にするには、設定テンプレート ファイルを編集する必要があります（ROUTER 設定テンプレートの編集を参照）。この機能は現在、IoT FND でサポートされるすべての FAR OS バージョンで使用できます。

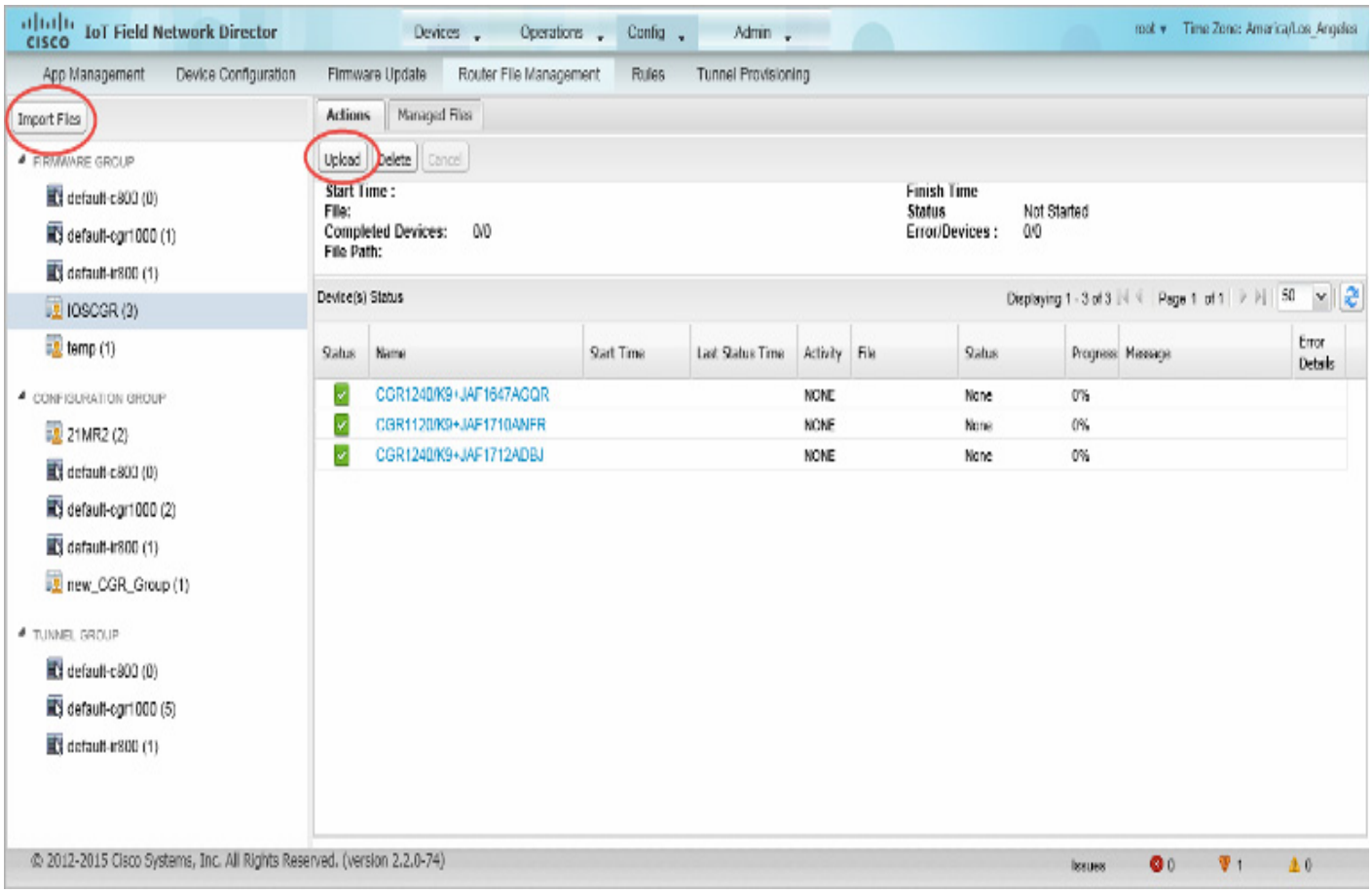
また、ファイル管理機能の向上のために、他のファイル タイプを FAR に転送することもできます。FAR にファイルをアップロードするには、最初にファイルを IoT FND にインポートする必要があります。IoT FND はファイルを処理し、次の属性を使用して IoT FND に保存します。

- ファイル名
- 説明
- Import Date/Time
- サイズ
- Sha1 Checksum
- MD5 Checksum
- File Content

IoT FND へのファイルの追加

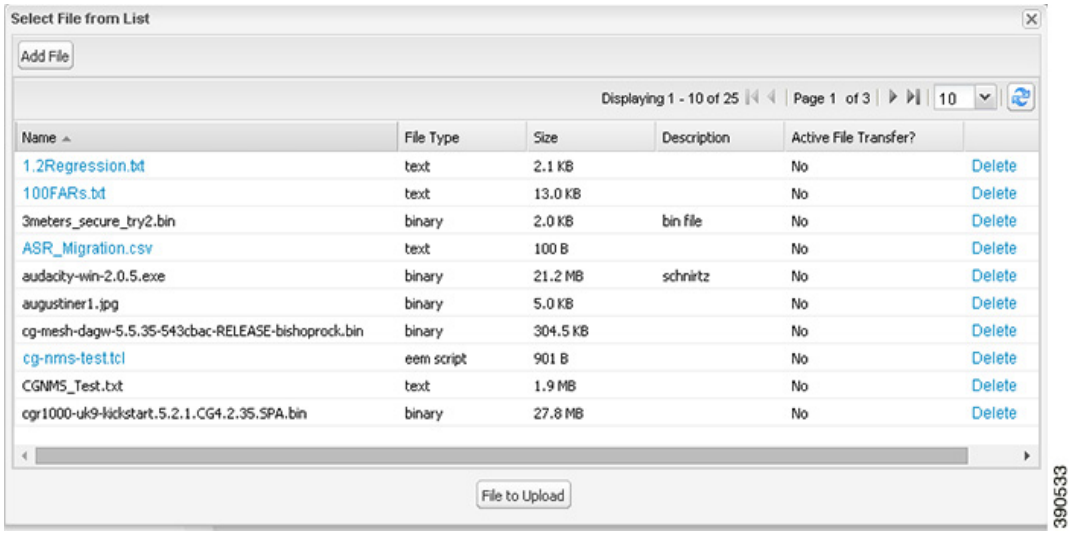
IoT FND にファイルを追加するには、次の手順を実行します。

1. [Config] > [Router File Management] ページで、[Import Files] または [Upload] をクリックし、選択したファイルを開きます。



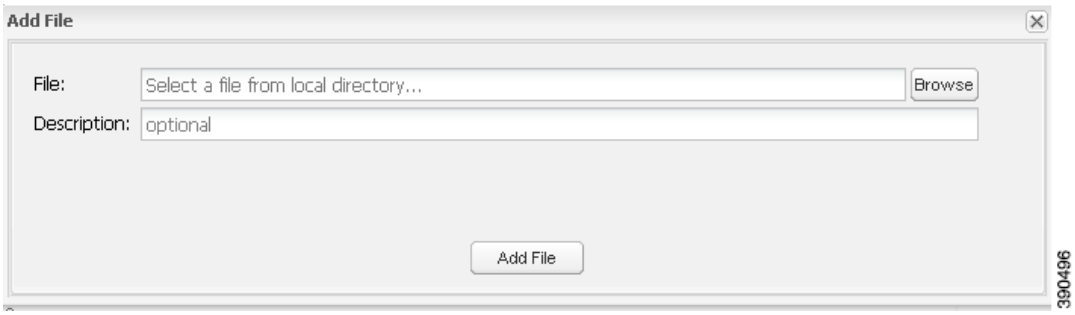
2. [Add File] をクリックし、ファイルの場所を検索します

(注)インポート ファイル の最大サイズは 200 MB です。



(注) [Select File from List] ダイアログ ボックスでは、ファイルがアクティブなファイル転送中でない場合は、IoT FND データベースからインポート済みのファイルを削除することもできます。これによりファイルは IoT FND データベースから削除されますが、ファイルを含む FAR からは削除されません。アップロードされたテキスト ファイルを表示するには、名前のハイパーリンクをクリックします(ファイル サイズは 100 KB 未満である必要があります)。

3. (任意)ファイルの説明を入力します。



4. [Add File] をクリックします。

   アップロードが完了すると、[Select File From List] ダイアログボックスにファイル名が表示されます。

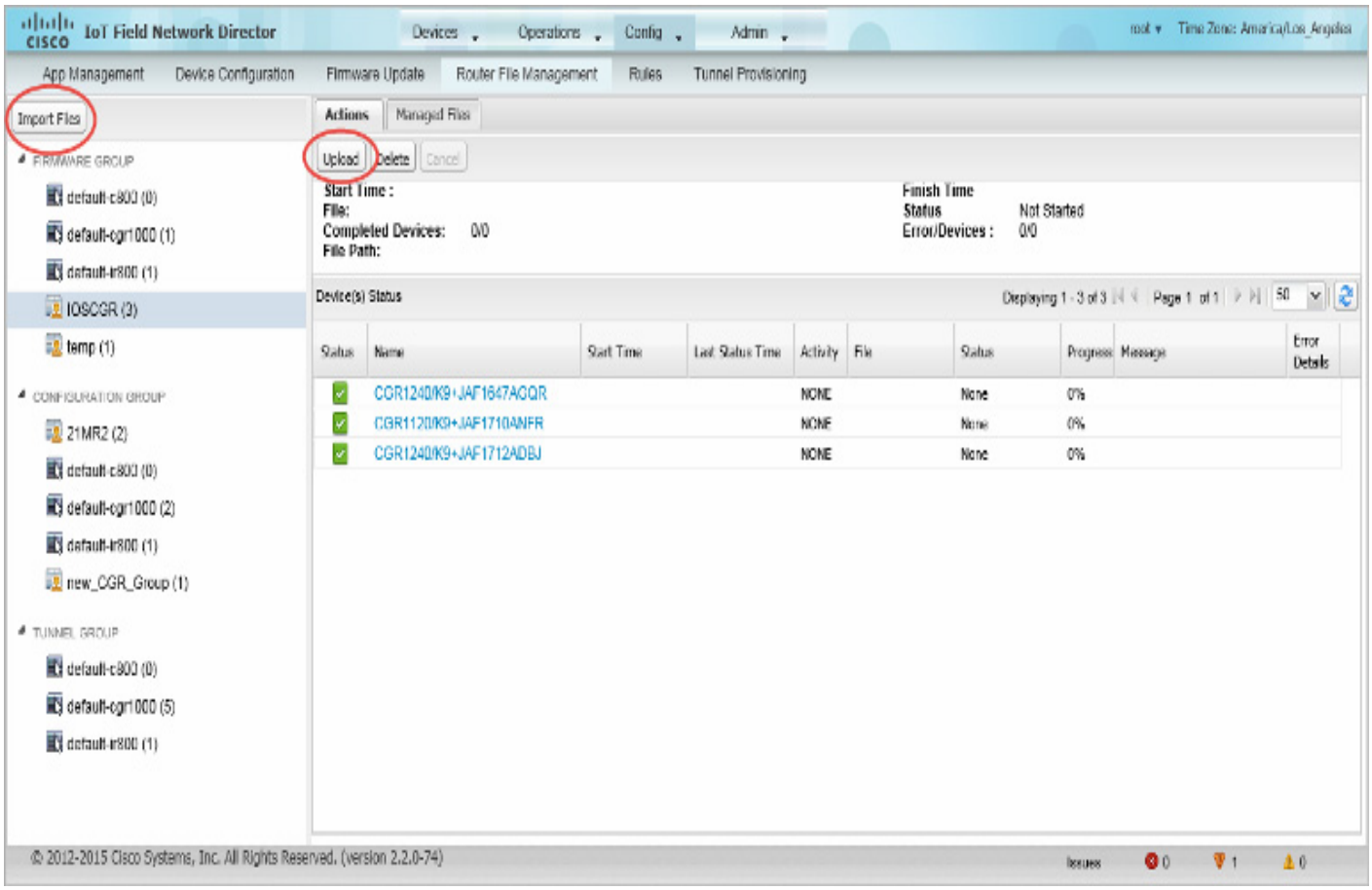
5. ステップ 2 から 4 を繰り返して他のファイルを追加するか、ファイル転送 を参照して選択したデバイスまたはグループにファイルをアップロードするか、または [Select File From List] ダイアログボックスを閉じます。

ファイル転送

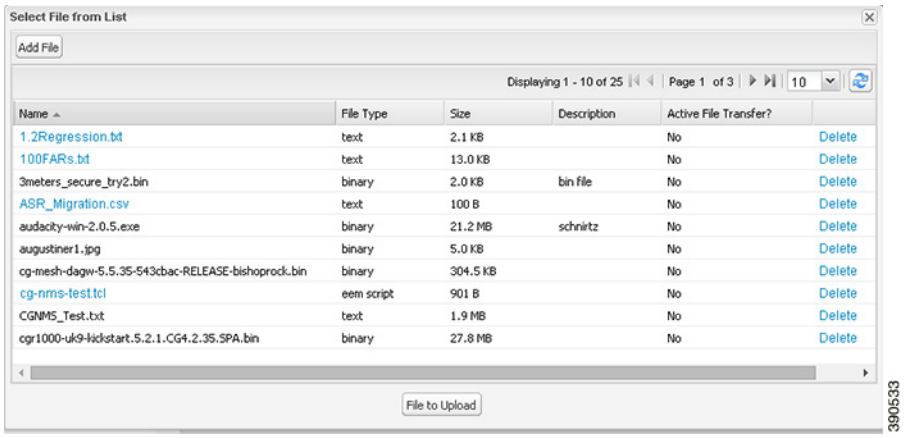
NMS データベースからファームウェア グループ、設定グループ、トンネル プロビジョニング グループ、または個々の FAR にファイルを転送できます。インポート ファイルの最大サイズは 200 MB です。

ファイル転送を実行するには、次の手順を実行します。

1. [Config] > [Router File Management] ページの [Browse Devices] ペインで、ファイルの転送先のグループを選択します。
2. [Import Files] または [Actions] タブの [Upload] をクリックします。

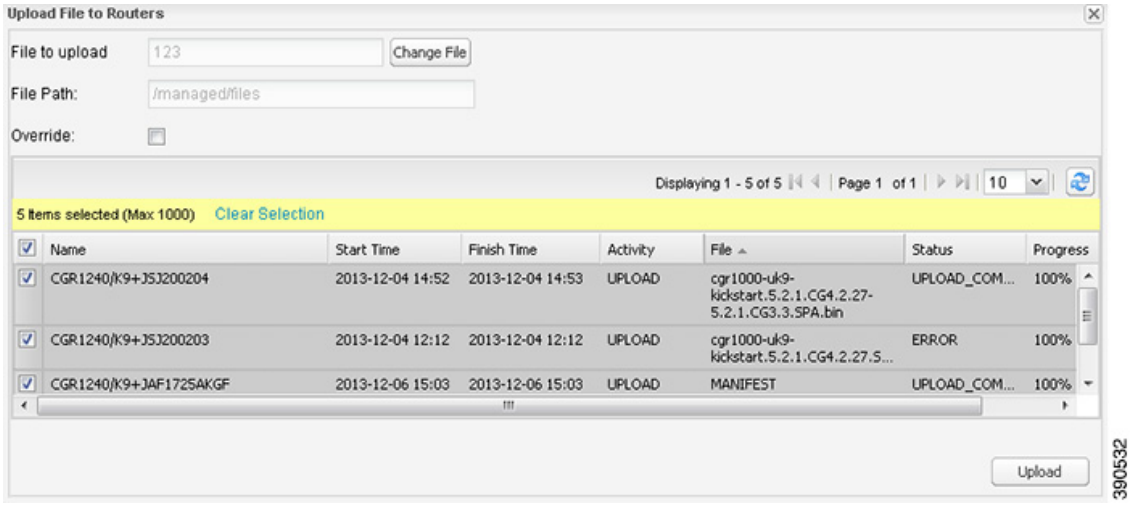


[Select File from List] ダイアログボックスが表示されます。



3. 選択しているグループで、FAR に転送するファイルを選択します。
4. [File to Upload] をクリックします。

   [Upload File to Routers] ダイアログボックスが表示されます。



5. ファイルの転送先となる FAR のチェックボックスをオンにします。
6. [Upload] をクリックします。

グループに対して進行中のファイル転送またはファイル削除、設定のプッシュ、ファームウェアのアップロード、またはインストールまたはリプロビジョニング操作がなければ、アップロードが開始します。

選択したグループ内のすべてのファイルを転送することを選択するか、またはグループ内の FAR のサブセットだけを選択することができます。また、他のグループとファイルを選択して、別のファイル転送またはファイル削除を同時に実行することもできます。

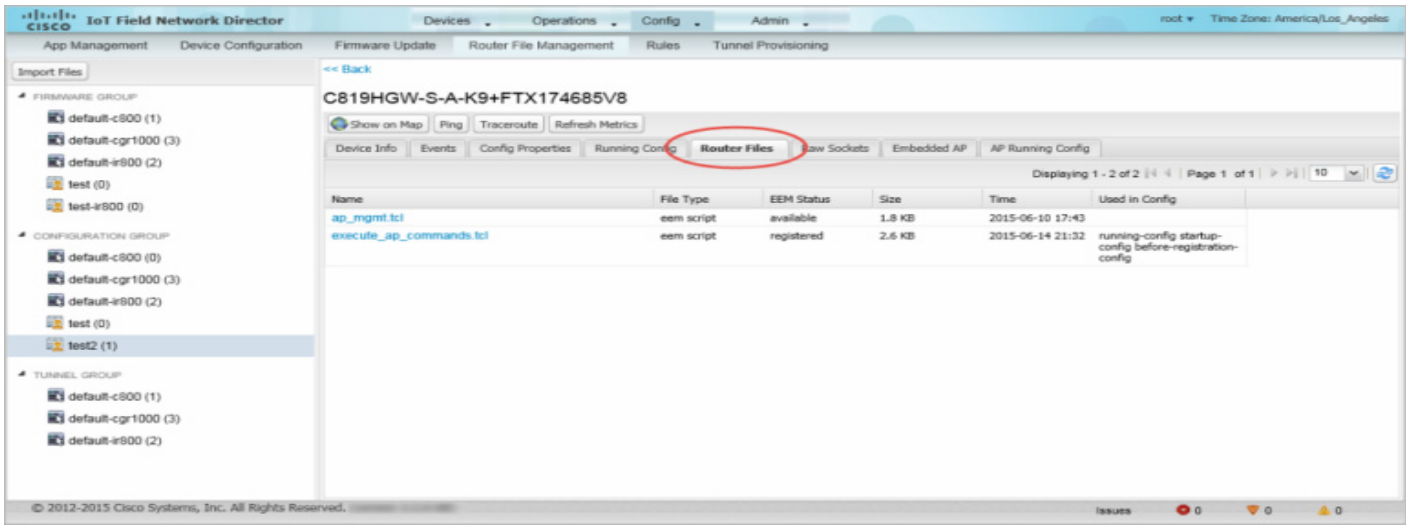
IoT FND から転送されるすべてのファイルは、Cisco IOS CGR では flash:/managed/files/、CG-OS CGR では bootflash:/managed/files/ 内の FAR に置かれます。

最後のファイル転送のステータスは、操作(ファームウェア アップデート、設定のプッシュなど)およびグループのステータスとともに、グループに付属して保存されます。

ファイルの表示

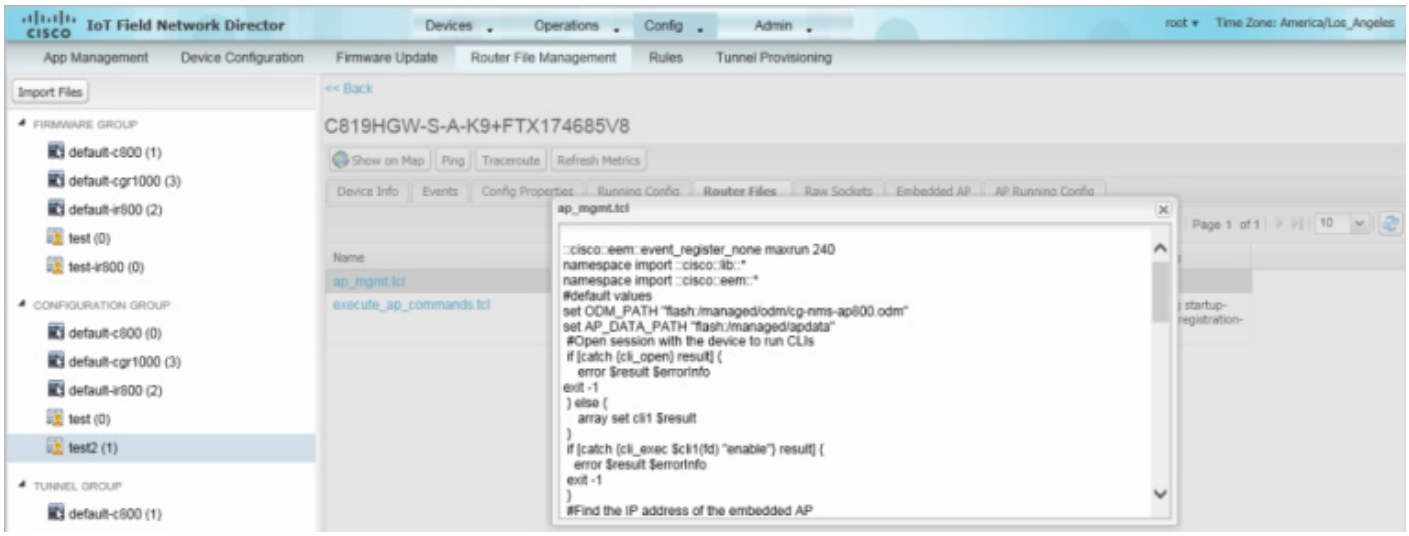
インポートされたテキスト ファイルの内容を表示するには、次の手順を実行します。

1. EID リンクをクリックして [Device Info] ペインを表示します。
2. [Router Files] タブをクリックします。



3. ファイル名のリンクをクリックし、新しいウィンドウの内容を表示します。

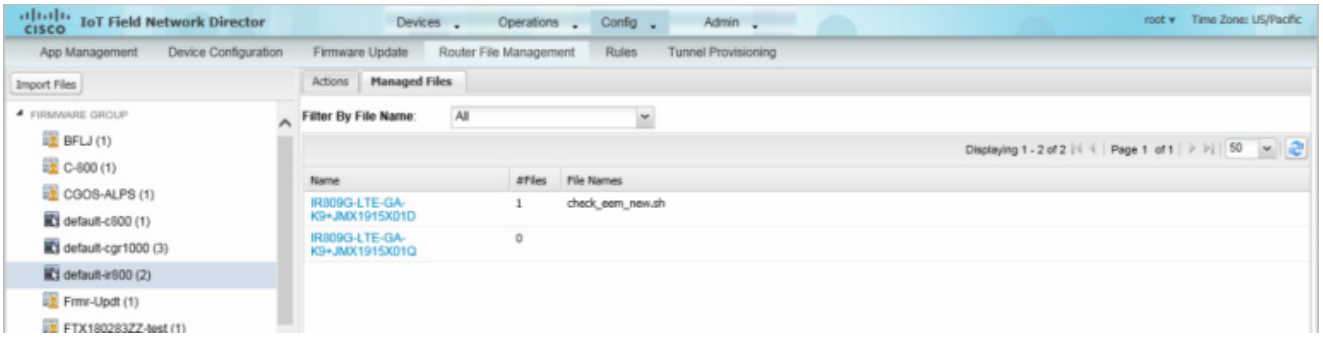
   (注) IoT FND は、100 KB 未満のプレーン テキストとして保存されているファイルのみを表示します。これより大きいテキスト ファイル、およびサイズに関係なくバイナリ ファイルは表示できません。それらのファイル タイプはハイパーリンクになりません。



ファイルのモニタリング

[Config] > [Router File Management] ページで [Managed Files] タブをクリックして、FAR のリストおよび .../managed/files/ ディレクトリにアップロードしたファイルを表示します。メイン ペインにリスト表示されるデバイスは、選択したグループのメンバーです。

図 10　[Managed Files] タブ



このリストには次の情報が含まれます。

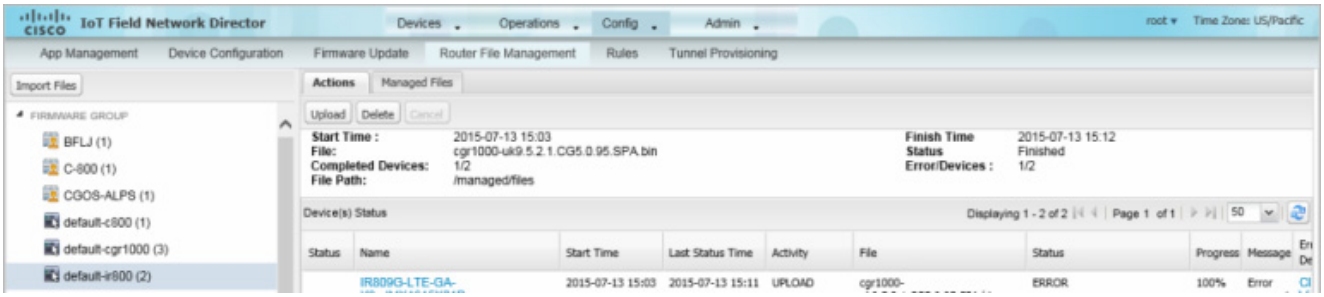
- [Device Info] ページへの EID リンク
- デバイスに保存されているファイルの数
- アップロードされているファイルの名前

特定のファイルを含むデバイスのみを表示する場合は、[Filter By File Name] ドロップダウン メニューを使用します。グループ内のすべてのデバイスを含める場合は、[All] を選択します。ファイル転送、または削除中にリストを更新するには、更新ボタンをクリックします。

アクションのモニタリング

[Config] > [Router File Management] ページで、[Actions] タブをクリックして、選択したグループの FAR での最後のファイル転送または最後に削除したファイルを表示します。[Cancel] ボタンをクリックすると、任意のアクティブなファイル操作を終了できます。

図 11　[Actions] タブ



[Actions] タブには次の属性がリスト表示されます。

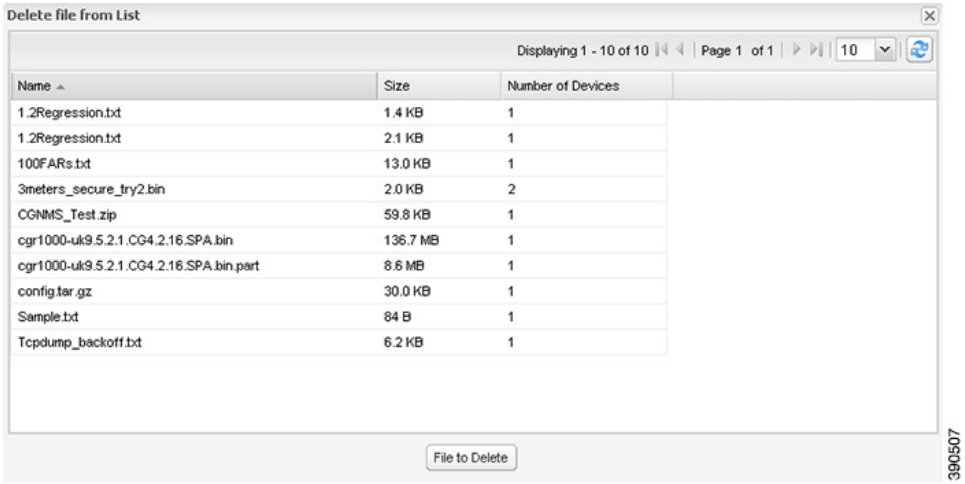
- 最後の転送の開始日時
- 最後の転送の終了日時
- ファイル名
- プロセスのステータス：UNKNOWN、AWAITING_DELETE、DELETE_IN_PROGRESS、DELETE_COMPLETE、CANCELLED、NOTSTARTED、UPLOAD_IN_PROGRESS、UPLOAD_COMPLETE、STOPPING、STOPPED
- アップロードが完了したデバイスの数とターゲット デバイスの合計数
- エラーの数とエラーが発生したデバイスの数
- ファイル パス

- [Device Info] ページへの EID リンク
- 実行されたアクティビティ：UPLOAD、DELETE、NONE
- 進捗率
- プロセス中に検出された問題に関するメッセージ
- エラーの詳細

ファイルの削除

ファイルを FAR から削除するには、次の手順を実行します。

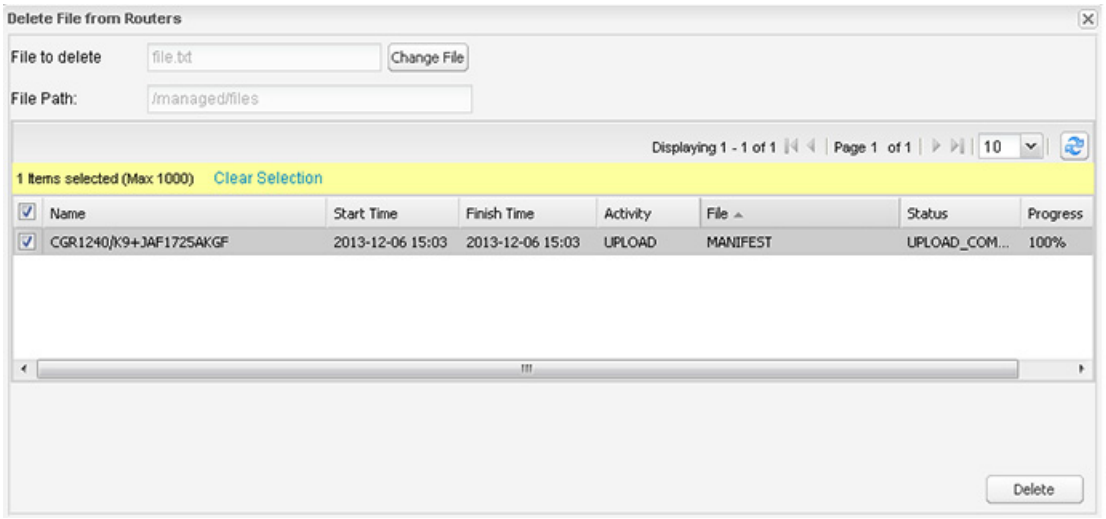
1. [Config] > [Router File Management] ページの [Browse Devices] ペインで、ファイルの転送先のグループを選択します。
2. [Actions] タブで [Delete] を選択します。
3. [Delete file from List] ダイアログで、削除するファイルを選択します。



選択したグループのすべての FAR、またはグループ内の FAR のサブセットからファイルを削除できます。

4. [File to Delete] をクリックします。

[Delete File from Routers] ダイアログボックスが表示されます。



5. ファイルを削除する FAR のチェックボックスをオンにします。

   - [Change File] をクリックして、選択した FAR から別のファイルを削除することができます。
   - 複数の FAR を選択できます。
   - 一度に削除できるのは 1 個のファイルだけです。

6. [Delete] をクリックします。

   グループで進行中のファイル転送またはファイル削除、設定のプッシュ、ファームウェアのアップロード、またはインストールまたはリプロビジョニング操作がなければ、削除操作が開始します。IoT FND は、デバイスの .../managed/files/ ディレクトリで、指定したファイル名を検索します。

   (注) 削除では、IoT FND データベースからではなく、選択したデバイスからすべてのファイル コンテンツが消去されます。選択したグループのクリーンアップ ファイルのステータスが表示されます。

   このグループでファイル転送またはファイル削除が処理されている間に、別のグループとファイルを選択して、別のファイル削除を実行することができます。ファイル削除が完了する前に削除処理をキャンセルすると、現在実行中のファイル削除処理は完了し、すべての待機中のファイル削除がキャンセルされます。

ワーク オーダーの管理

- ワーク オーダーの表示
- Device Manager (IoT-DM) ユーザのユーザ アカウントの作成
- ワーク オーダーの作成
- ワーク オーダーの編集
- ワーク オーダーの削除

(注) ワーク オーダー機能は、リリース 3.0 以降の IoT-DM で動作します。統合の手順については、『*Cisco Connected Grid Device Manager Installation and User Guide, Release 3.1*』の「*Accessing Work Authorizations*」、または『*Cisco Connected Grid Device Manager Installation and User Guide (Cisco IOS), Release 4.0 and 4.1*』の「*Managing Work Orders*」、あるいは『*Cisco IoT Device Manager Installation and User Guide (Cisco IOS), Release 5.0*』を参照してください。

(注)CGDM リリース 3.1 以降を使用している場合は、IoT-DM と IoT FND との接続認証のために、次の手順により SSLv3 を有効にする必要があります。

1. IoT FND を停止します。

```
service cgms stop
```

2. IoT-DM リリース 3.x 以降では、次のファイルで **protocol="TLSv1"** 属性を置き換えます。

   - /opt/cgms/standalone/configuration/standalone.xml
   - /opt/cgms/standalone/configuration/standalone-cluster.xml

   CGDM 3.x の場合

   - 属性を **protocol="TLSv1,SSLv3"** に置き換えます。

   CGDM 4.x および IoT-DM 5.x の場合

   - 属性を **protocol="TLSv1.x,SSLv3"** に置き換えます。

3. IoT FND を起動します。

```
service cgms start
```

ワーク オーダーの表示

IoT FND でワーク オーダーを表示するには、[Operations] > [Work Orders] を選択します。

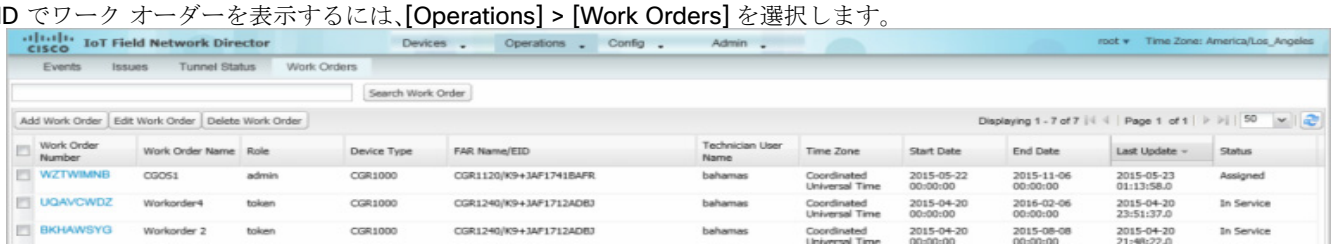


表 9 に、[Work Orders] ページに表示するフィールドを示します。

表 9　[Work Orders] ページのフィールド

フィールド	説明
Work Order Number	ワーク オーダーの一意の識別子。
Work Order Name	ワーク オーダーの名前。
ロール	(CG-OS のみ) ワーク オーダーに割り当てられたユーザのロール。tech、admin、または viewer。
FAR Name	ワーク オーダーに関連付けられた FAR の EID。
Technician User Name	割り当てられた技術者のユーザ名。
Time Zone	FAR が置かれているタイムゾーン。ユーザのタイムゾーン *ではありません*。この値は導入に依存し、ユーザのタイムゾーンに一致させることができます。
Start Date	フィールド技術者に割り当てられたプロジェクトの開始日と終了日。
End Date	

表 9　[Work Orders] ページのフィールド（続き）

フィールド	説明
Last Update	ワーク オーダーの最後のステータス更新の時刻。
Status（ステータス）	ワーク オーダーのステータス。有効なステータス値は、New、Assigned、InService、Completed、Incomplete、または Expired です。

ワーク オーダーの検索

検索を改善するには、[Search Work Order] フィールドで次の構文を使用します（[Operations] > [Work Orders]）。

パラメータ	説明
workOrderNumber	ワーク オーダーの一意の識別子。
role	（CG-OS のみ）ワーク オーダーに割り当てられたユーザのロール。有効なロールは、tech、admin、または viewer です。
technicianUserName	ワーク オーダーに割り当てられた技術者のユーザ名。
workOrderStatus	ワーク オーダーのステータス。有効なステータス ラベルは、New、Assigned、InService、Completed、Incomplete、または Expired です。
eid	ワーク オーダーに関連付けられた FAR の EID。

たとえば、admin ロールを持つユーザが割り当てられている完了したワーク オーダーを検索するには、次の構文を使用します。

role:admin workOrderStatus:Completed

IoT FND でワーク オーダーを検索するには、次の手順を実行します。

1. [Operations] > [Work Orders] を選択します。
2. [Search Work Order] フィールドに検索構文を入力し、[Search Work Orders] をクリックします。

Device Manager（IoT-DM）ユーザのユーザ アカウントの作成

ワーク オーダーを作成する前に、IoT-DM を使用して IoT FND からワーク オーダーをダウンロードするフィールド技術者のユーザ アカウントを作成する必要があります。

Device Manager ユーザ アカウントを作成するには、次の手順を実行します。

1. 定義されていない場合は、次の手順により、[Device Manager User] ロールを作成します。
   a. [Admin] > [Access Management] > [Roles] を選択します。
   b. [Add] をクリックします。
   c. （CG-OS のみ）[Role Name] フィールドに、ロールの名前を入力します。
   d. [Device Manager User] チェックボックスをオンにし、[Save] をクリックします。
2. ユーザ アカウントを作成します。
   a. [Admin] > [Access Management] > [Users] を選択し、[Add] をクリックします。
   b. ユーザ名、パスワード、およびタイム ゾーン情報を設定します。
   c. [Monitor Only] およびステップ 1 で作成した [Device Manager User] ロールのチェックボックスをオンにします。
   d. [Save（保存）] をクリックします。

ワーク オーダーの作成

技術者により導入済みの FAR（CGR 1120 または CGR 1240）または DA ゲートウェイ（IR509）をフィールドで確認することが必要な場合は、ワーク オーダーを作成します。ワーク オーダーには、技術者がルータに接続するのに必要な WiFi クレデンシャルが含まれています。

はじめる前に

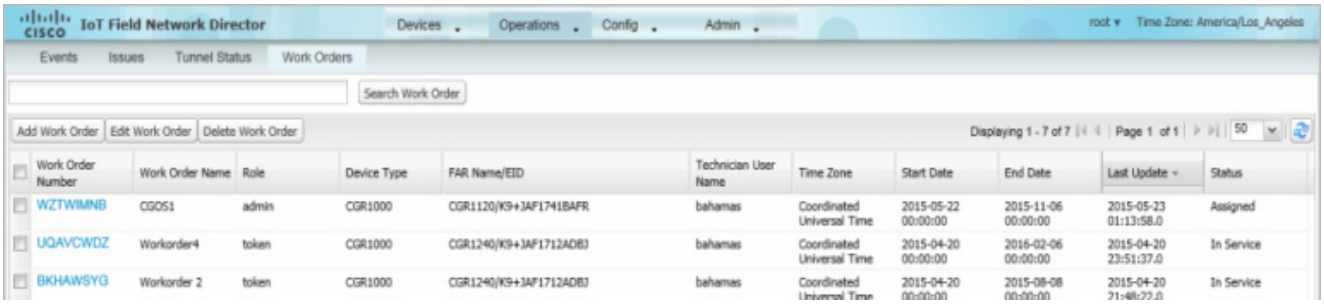
- ユーザ アカウントで、[Work Order Management] 権限が有効になっている必要があります。
- IoT DM への要求に署名済みワーク オーダーを提供するには、エイリアス cgms を使用して、cgms_keystore に IoT DM 証明書をインポートする必要があります。
- フィールド技術者のユーザ アカウントを作成します。（Device Manager（IoT-DM）ユーザのユーザ アカウントの作成を参照）。

（注）ワーク オーダーは、CGR および IR509 デバイスでのみ作成できます。

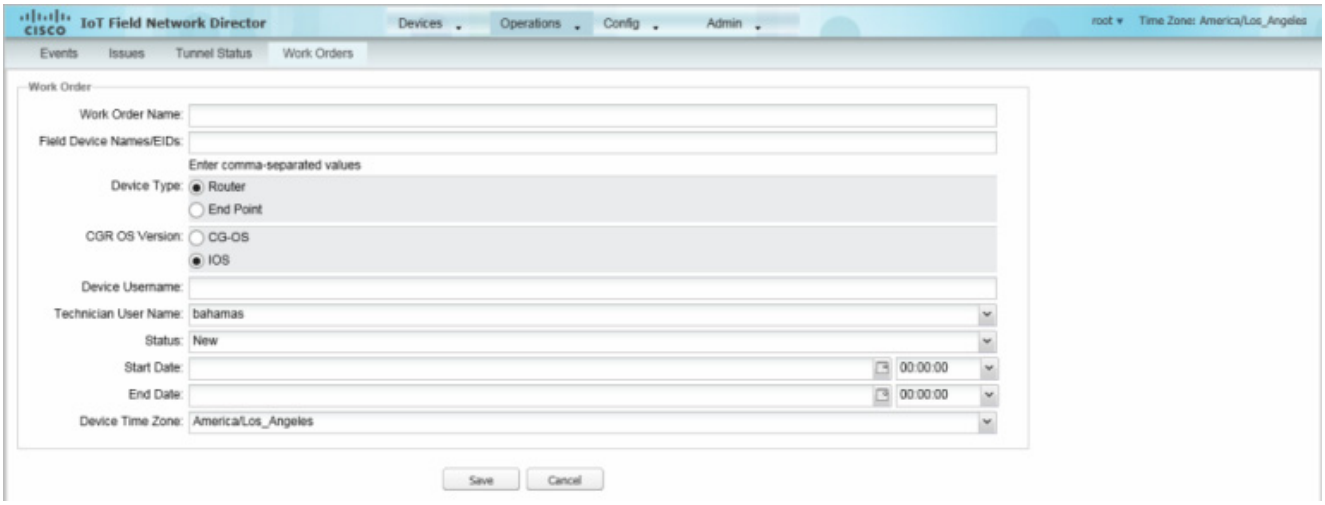
手順の詳細

ルータ（CGR1000）またはエンドポイント（IR509）のワーク オーダーを作成するには、次の手順を実行します。

1. [Operations] > [Work Orders] を選択します。



2. [Add Work Order] をクリックします。



3. [Work Order Name] フィールドに、ワーク オーダーの名前を入力します。
4. [Field Device Names/EIDs] フィールドに、FAR の名前または EID の カンマ区切りリストを入力します。

   リスト内のすべての FAR に対し、IoT FND は個別のワーク オーダーを作成します。

5. [Device Type]（[Router] または [Endpoint]）および [CGR OS Version]（[CG-OS] または [IOS]）は自動入力されます。
6. [Device Username] フィールドに IoT-DM システム名を入力します。

   ドロップダウン メニューから IoT-DM の [Technician User Name] を選択します。このメニューには、IoT-DM ユーザ権限が有効なユーザのみがリストされます。
7. [Status] ドロップダウン メニューから、ワーク オーダーのステータス（New、Assigned、In Service、Completed、または InComplete）を選択します。 [New] オプションは自動入力されます。

   (注) IoT DM ユーザがワーク オーダーを取得するには、IoT FND でワーク オーダーがそのユーザに対して [Assigned] の状態である必要があります。ワーク オーダーが他の状態の場合、IoT DM は署名済みのワーク オーダーを取得できません。

   (注) ワーク オーダーが IoT DM ユーザにより正常に要求されると、ワーク オーダーのステータスは [In Service] に変更されます。
8. [Start Date] および [End Date] フィールドで、ワーク オーダーが有効な開始日と終了日を指定します。

   ワーク フローが有効でないと、技術者がルータにアクセスできません。
9. [Device Time Zone] フィールドで、ドロップダウン メニューからデバイスのタイム ゾーンを選択します。
10. [Save（保存）] をクリックします。
11. [OK] をクリックします。

ワーク オーダーは、「ワーク オーダーの作成」で説明するように [Field Devices] ページ（[Devices] > [Field Devices]）で、および [Device Info] ページでも作成できます。

ワーク オーダーのダウンロード

IoT FND で作成されたワーク オーダーをフィールド技術者がダウンロードする際には、単一の Cisco CGR 1000 ルータを管理する場合にフィールド技術者が使用する Windows ベースのアプリケーションである Cisco IoT-DM が使用されます。技術者は、[Assigned] の状態のすべてのワーク オーダーをダウンロードできます。

フィールド技術者は、IoT-DM を使用してワーク オーダーのステータスを更新し、更新されたステータスは IoT FND に送信されます。

(注) 証明書はワーク オーダーに含まれるのでなく、IoT FND からワーク オーダーをダウンロードするより前に、IoT-DM フィールド ラップトップにプレインストールされています。

IoT-DM の詳細については、『*Cisco IoT Device Manager User Guide*』を参照してください。

ワーク オーダーの編集

ワーク オーダーの詳細を編集するには、次の手順を実行します。

1. [Operations] > [Work Orders] を選択します。
2. 編集するワーク オーダーを選択し、[Edit Work Order] をクリックします。

   または、ワーク オーダー番号をクリックして、ワーク オーダーの詳細を表示しているページを開きます。
3. [Save（保存）] をクリックします。

ワーク オーダーの削除

ワーク オーダーを削除するには、次の手順を実行します。

1. [Operations] > [Work Orders] を選択します。
2. 削除するワーク オーダーのチェックボックスを選択します。

3. [Delete Work Order] をクリックします。
4. [Yes] をクリックします。

デバイス プロパティ

この項では、IoT FND で表示できるデバイスのプロパティについて説明します。これらのプロパティには、設定可能なものとそうでないものがあります。

- デバイス プロパティのタイプ
- カテゴリ別デバイス プロパティ

デバイス プロパティのタイプ

IoT FND は、そのデータベース内に次の 2 種類のデバイス プロパティを保存します。

- 実デバイス プロパティ：IP アドレス、送信速度、SSID など、デバイスによって定義されるプロパティ。
- IoT FND デバイス プロパティ：GIS マップでのデバイスの位置を表示するために IoT FND が使用する緯度や経度プロパティなど、デバイスに関して IoT FND によって定義されるプロパティ。

  (注) [Key] カラムは、フィルタで使用できる IoT FND データベースにおけるプロパティ名のバージョンを提供します。たとえば、IP アドレスが 10.33.0.30 ののデバイスを検索するには、[Search Devices] フィールドに **ip:10.33.0.30** と入力します。

カテゴリ別デバイス プロパティ

この項では、次に示すカテゴリ別の IoT FND デバイスのプロパティを表示します。

- セルラー リンクの設定
- CGR のセルラー リンク メトリック
- DA ゲートウェイのプロパティ
- デュアル PHY WPAN のプロパティ
- 組み込みアクセスポイント クレデンシャル
- 組み込み AP のプロパティ
- イーサネット リンク メトリック
- ゲスト OS のプロパティ
- [Head-End Routers] > [Netconf Config]
- [Head-End Routers] > [Tunnel 1 Config]
- [Head-End Routers] > [Tunnel 2 Config]
- Inventory
- メッシュ リンクの設定
- メッシュ デバイスの状態
- メッシュ リンク キー

- メッシュ リンクの設定
- メッシュ リンク メトリック
- NAT44 メトリック
- PLC メッシュ情報
- raw ソケット メトリックおよびセッション
- ルータ バッテリ
- ルータの設定
- ルータ クレデンシャル
- ルータの DHCP プロキシの設定
- Router Health
- ルータ トンネルの設定
- ルータ トンネル 1 の設定
- ルータ トンネル 2 の設定
- SCADA メトリック
- ユーザ定義のプロパティ
- WiFi インターフェイスの設定
- WiMAX の設定
- WiMAX リンク メトリック
- WiMAX リンクの設定

IoT FND のすべてのデバイスには、デバイスの検索に使用されるフィールドのリストが提供されています。デバイスで使用可能なフィールドは、[Device Type] フィールドで定義されます。フィールドは、設定可能であるか、または情報用です。設定可能なフィールドは、XML および CSV ファイルを使用して設定され、デバイス EID が検索キーになります。情報用フィールドは、デバイスにより提供されます。フィールドには、FAR のデバイス設定テンプレートからもアクセスできます。

セルラー リンクの設定

表 10 に、すべてのセルラー インターフェイスの [Device Detail] ページの [Cellular Link] エリアのフィールドを示します。

(注) IoT FND 3.2、シスコ ルータ IR829、CGR1240、CGR1120、および Cisco 819 4G LTE ISR（C819）以降では、デュアル モデムとモデムごとに 2 つの物理インターフェイス（インターフェイス 0 と 1、インターフェイス 2 と 3）をサポートする新しいデュアルアクティブ無線モジュールをサポートします。次の SKU を参照してください。

- IR829GW-2LTE-K9
- CGR 1000 ルータの CGM-LTE-LA
- C819HG-LTE-MNA-K9

デュアル モデムとそれらの 2 つの物理インターフェイス（および 4 つの論理インターフェイス 0、1、2、3）でサポートされるセルラー プロパティは次のように表示されます。

Cellular Link Metrics

セルラー リンクの設定	インターフェイス 0 とインターフェイス 1	インターフェイス 2 とインターフェイス 3

また、4G LTE デュアルアクティブ無線モジュールは、表 10 にまとめられているすべてのフィールドをサポートせず、表示しません

表 10　[Cellular Link Settings] のフィールド

フィールド	Key	設定可能かどうか	説明
Cellular Network Type	該当なし	Yes	GSM または CDMA など、セルラー ネットワークのタイプを定義します。
Module Status	cellularStatus	不可	セルラー インターフェイス モジュールがネットワークでアクティブであるかどうかを示します。モジュールによっては状態が不明な場合もあります。
Network Name	_	Yes	AT&T や Verizon など、サービス プロバイダーの名前を定義します。
APN	cellularAPN	不可	セルラー インターフェイスが接続する AP のアクセスポイント名（APN）を表示します。
Cell ID	cellularID	不可	セルラー インターフェイスの セル ID を表示します。インターフェイスをアクティブにするには、この値が必要です。
Cellular SID	cellularSID	不可	CDMA セルラー エリアのシステム識別番号を表示します。
Cellular NID	cellularNID	不可	CDMA セルラー エリアのネットワーク識別番号を表示します。
Cellular Roaming Status	cellularRoamingStatus	不可	モデムがホーム ネットワークに接続しているか、ローミングしているかを表示します。
Cellular Modem Serial Number	該当なし	非対応	接続されているモデムのシリアル番号を表示します。
Cellular Modem Firmware Version	cellularModemFirmwareVersion	不可	CGR にインストールされているモジュール上のモデム ファームウェアのバージョンを表示します。
Connection Type	connectionType	不可	接続タイプは次のように表示されます。 ■ Packet switched ■ Circuit switched ■ LTE
Location Area Code	locationAreaCode	不可	ベース ステーションによって提供されるロケーション エリア コード（LAC）を表示します。
Routing Area Code	routingAreaCode	不可	ベース ステーションによって提供されるルーティング エリア コードを表示します。

表 10　[Cellular Link Settings] のフィールド（続き）

フィールド	Key	設定可能かどうか	説明
IMEI	cellularIMEI	不可	GSM ネットワーク内だけのセルラー インターフェイスの国際移動体装置識別番号（IMEI）を表示します。IMEI 値はセルラー インターフェイスで一意の番号になります。
APN	cellularAPN	不可	セルラー インターフェイスが接続する AP のアクセスポイント名（APN）を表示します。
Cellular Modem Firmware Version	cellularModemFirmwareVersion	不可	CGR にインストールされているセルラー モジュール上のモデム ファームウェアのバージョンを表示します。
Connection Type	connectionType	不可	接続タイプは次のように表示されます。 ■ Packet switched ■ Circuit switched
IMSI	cellularIMSI	不可	国際移動体加入者識別番号（IMSI）は、GSM および CDMA ネットワーク内の個々のネットワーク ユーザを 10 桁の数値として識別します。 値は次のとおりです。 ■ 10 桁の数値 ■ 不明（Unknown）
IMEI	cellularIMEI	不可	GSM ネットワーク内だけのセルラー インターフェイスの国際移動体装置識別番号（IMEI）を表示します。IMEI 値はセルラー インターフェイスで一意の番号になります。

CGR のセルラー リンク メトリック

表 11 に、[Device Info] ビューの [Cellular Link Metrics] エリア内のフィールドを示します。

表 11　[Cellular Link Metrics] エリアのフィールド

フィールド	Key	説明
Transmit Speed	cellularTxSpeed	定義した期間（たとえば 1 時間）に、セルラー アップリンク上をセルラー インターフェイスによって送信されたデータの現在の速度（ビット/秒）を表示します。
Receive Speed	cellularRxSpeed	定義した期間（たとえば 1 時間）に、セルラー アップリンク ネットワーク インターフェイスによって受信されたデータの平均速度（ビット/秒）を表示します。

表 11　[Cellular Link Metrics] エリアのフィールド（続き）

フィールド	Key	説明
RSSI	cellularRssi	セルラー アップリンクの無線周波数（RF）の信号強度を示します。有効値の範囲は 0 ～ -100 です。 セルラー インターフェイスの LED の状態と対応する RSSI 値は次のように表示されます。 ■ オフ：RSSI < = -110 ■ オレンジ色の点灯：-100 < RSSI <= -90 ■ 緑色の高速点滅：-90 < RSSI <= -75 ■ 緑色の低速点滅：-75 < RSSI <= -60 ■ 緑色の点灯：RSSI > -60
Bandwidth Usage (Current Billing Cycle)	CellBwPerCycle (bytes)	現在の課金サイクルでの特定のルートの現在の帯域幅使用（バイト単位）を表示します。
Cell Module Temperature	cellModuleTemp	3G モジュールの内部温度。
Cell ECIO	cellularEcio	個々のセクター レベルでの CDMA の信号強度。
Cell Connect Time	cellConnectTime	現在のコールが続いた時間の長さ。このフィールドは、CDMA にのみ適用されます。

DA ゲートウェイのプロパティ

「[DA Gateway Metrics] エリアのフィールド」に、[Device Info] ビューの [DA Gateway] エリア内のフィールドを示します。

表 12　[DA Gateway Metrics] エリアのフィールド

フィールド	Key	説明
SSID	-	メッシュの SSID。
PANID	-	サブネットの PAN ID。
送信電力	-	メッシュの送信電力。
Security Mode	-	メッシュのセキュリティ モードは次のとおりです。 ■ 0 は、セキュリティ モードが設定されていないことを示します。 ■ 1 は、802.11i キー管理を含む 802.1x を示します。
Meter Certificate	meterCert	メータ証明書のサブジェクト名。
Mesh Tone Map Forward Modulation	toneMapForwardModulation	メッシュ トーン マップのフォワード変調は次のとおりです。 ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK

表 12　[DA Gateway Metrics] エリアのフィールド(続き)

フィールド	Key	説明
Mesh Tone Map Reverse Modulation	-	メッシュ トーン マップのリバース変調は次のとおりです。 ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Device Type	-	メッシュ デバイスの主な機能(たとえば、メータ、Range Extender、または DA ゲートウェイ)。
Manufacturer of the Mesh Devices	-	デバイスによりレポートされるメッシュ デバイスの製造元。
Basic Mapping Rule End User IPv6 Prefix	-	基本的なルールのデバイスへのマッピング用のエンドユーザ IPv6 アドレス。
Basic Mapping Rule End User IPv6 Prefix Length	-	エンドユーザ IPv6 アドレスの指定のプレフィックス長。
Map-T IPv6 Address	-	Map-T 設定用の IPv6 アドレス。
Map-T IPv4 Address	-	Map-T 設定用の IPv4 アドレス。
Map-T PSID	-	Map-T の PSID。
Active Link Type	-	デバイスが IoT FND を含む他のデバイスと通信するのに経由する物理リンクのリンク タイプ。

デュアル PHY WPAN のプロパティ

表 13 に、[Device Info] ビューの [Dual PHY] エリア内のフィールドを示します。

表 13　[Dual PHY Metrics] エリアのフィールド

フィールド	Key	説明
SSID	ssid	メッシュの SSID。
PANID	panid	サブネットの PAN ID。
送信電力	txpower	メッシュの送信電力。
Security Mode	-	メッシュのセキュリティ モードは次のとおりです。 ■ 0 は、セキュリティ モードが設定されていないことを示します。 ■ 1 は、802.11i キー管理を含む 802.1x を示します。
Meter Certificate	meterCert	メータ証明書のサブジェクト名。
Mesh Tone Map Forward Modulation	toneMapForwardModulation	メッシュ トーン マップのフォワード変調は次のとおりです。 ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK

表 13　[Dual PHY Metrics] エリアのフィールド（続き）

フィールド	Key	説明
Mesh Tone Map Reverse Modulation	-	メッシュ トーン マップのリバース変調は次のとおりです。 ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Device Type	-	メッシュ デバイスの主な機能（たとえば、メータ、Range Extender、または DA ゲートウェイ）。
Manufacturer of the Mesh Devices	-	デバイスによりレポートされるメッシュ デバイスの製造元。
Basic Mapping Rule End User IPv6 Prefix	-	基本的なルールのデバイスへのマッピング用のエンドユーザ IPv6 アドレス。
Basic Mapping Rule End User IPv6 Prefix Length	-	エンドユーザ IPv6 アドレスの指定のプレフィックス長。
Map-T IPv6 Address	-	Map-T 設定用の IPv6 アドレス。
Map-T IPv4 Address	-	Map-T 設定用の IPv4 アドレス。
Map-T PSID	-	Map-T の PSID。
Active Link Type	-	デバイスが IoT FND を含む他のデバイスと通信するのに経由する物理リンクのリンク タイプ。

組み込みアクセスポイント クレデンシャル

表 14 に、[Device Info] ビューの [Embedded Access Point Credentials] エリア内のフィールドを示します。

表 14　組み込みアクセスポイント クレデンシャルのフィールド

フィールド	Key	設定可能かどうか	説明
AP Admin Username	-	Yes	アクセス ポイントの認証に使用するユーザ名。
AP Admin Password	-	Yes	アクセス ポイントの認証に使用するパスワード。

組み込み AP のプロパティ

表 15 に、C800 または IR800 の [Device Info] ビューの [Embedded AP] タブにあるフィールドを示します。

表 15　組み込み AP のプロパティ

フィールド	Key	説明
インベントリ	-	名前、EID、ドメイン、状態、IP アドレス、ホスト名、ドメイン名、First Heard、Last Heard、Last Property Heard、Last Metric Heard、モデル番号、シリアル番号、ファームウェアのバージョン、および稼働時間の詳細の要約。
Wi-Fi クライアント	-	クライアント MAC アドレス、SSID、IPv4 アドレス、IPv6 アドレス、デバイス タイプ、状態、名前、および親を指定します
Dot11Radio 0 Traffic	-	管理ステータス（アップ/ダウン）、動作ステータス（アップ/ダウン）、物理アドレス、Tx 速度（bps）、Tx 廃棄（bps）、および Rx 速度（bps）を指定します。

表 15　組み込み AP のプロパティ（続き）

フィールド	Key	説明
Dot11Radio 1 Traffic	-	管理ステータス（アップ/ダウン）、動作ステータス（アップ/ダウン）、物理アドレス、Tx 速度（bps）、Tx 廃棄（bps）、および Rx 速度（bps）を指定します。
Tunnel3	-	管理ステータス（アップ/ダウン）、動作ステータス（アップ/ダウン）、Tx 速度（bps）、Tx 廃棄（bps）、および Rx 速度（bps）を指定します。
BVI1	-	管理ステータス（アップ/ダウン）、動作ステータス（アップ/ダウン）、IP アドレス、物理アドレス、Tx 速度（bps）、Tx 廃棄（bps）、および Rx 速度（bps）を指定します。
GigabitEthernet0	-	管理ステータス（アップ/ダウン）、動作ステータス（アップ/ダウン）、物理アドレス、Tx 速度（bps）、Tx 廃棄（bps）、および Rx 速度（bps）を指定します。

イーサネット リンク メトリック

表 16 に、[Device Info] ビューの [Ethernet link traffic] エリア内のフィールドを示します。

表 16　[Ethernet Link Metrics] エリアのフィールド

フィールド	Key	説明
Transmit Speed	ethernetTxSpeed	定義した期間に、イーサネット インターフェイスで送信されたトラフィックの平均速度（ビット/秒）を表示します。
Receive Speed	ethernetRxSpeed	定義した期間に、イーサネット インターフェイスで受信されたトラフィックの平均速度（ビット/秒）を表示します。
Transmit Packet Drops	ethernetTxDrops	送信キューが満杯のときにドロップされたパケットの数（ドロップ/秒）を示します。

ゲスト OS のプロパティ

表 17 に、[Config Properties] ページの [Guest OS Properties] エリア内のフィールドを示します。

表 17　[Guest OS Properties] のフィールド

フィールド	Key	説明
GOS Password	-	GOS にアクセスするためのパスワード。
DHCPv4 Link for Guest OS Gateway	-	DHCPc4 ゲートウェイ アドレス。
Guest OS IPv4 Subnet mask	-	IPv4 サブネット マスク アドレス
Guest OS Gateway IPv6 Address	-	IPv6 ゲートウェイ アドレスです。
Guest OS IPv6 Subnet Prefix Length	-	IPv6 サブネットのプレフィックス長。

[Head-End Routers] > [Netconf Config]

表 18 に、[Head-End Routers] > [Config Properties] ページの [Netconf Client] エリア内のフィールドを示します。

表 18　[Head-End Routers] > [Netconf Config Client] のフィールド

フィールド	Key	設定可能かどうか	説明
Netconf Username	netconfUsername	Yes	HER で Netconf SSH セッションを確立するときに入力するユーザ名を指定します。
Netconf Password	netconfPassword	Yes	HER で Netconf SSH セッションを確立するときに入力するパスワードを指定します。

[Head-End Routers] > [Tunnel 1 Config]

表 19 に、[Head-End Routers] > [Config Properties] ページの [Tunnel 1 Config] エリア内のフィールドを示します。

表 19　[Head-End Routers] > [Tunnel 1 Config] のフィールド

フィールド	Key	設定可能かどうか	説明
IPsec Tunnel Source 1	ipsecTunnelSrc1	Yes	IPsec トンネル 1 の送信元インターフェイスまたは IP アドレスを指定します。
IPsec Tunnel Dest Addr 1	ipsecTunnelDestAddr1	Yes	IPsec トンネル 1 の宛先インターフェイスまたは IP アドレスを指定します。
GRE Tunnel Source 1	greTunnelSrc1	Yes	GRE トンネル 1 の送信元インターフェイスまたは IP アドレスを指定します。
GRE Tunnel Dest Addr 1	greTunnelDestAddr1	Yes	GRE トンネル 1 の宛先インターフェイスまたは IP アドレスを指定します。

[Head-End Routers] > [Tunnel 2 Config]

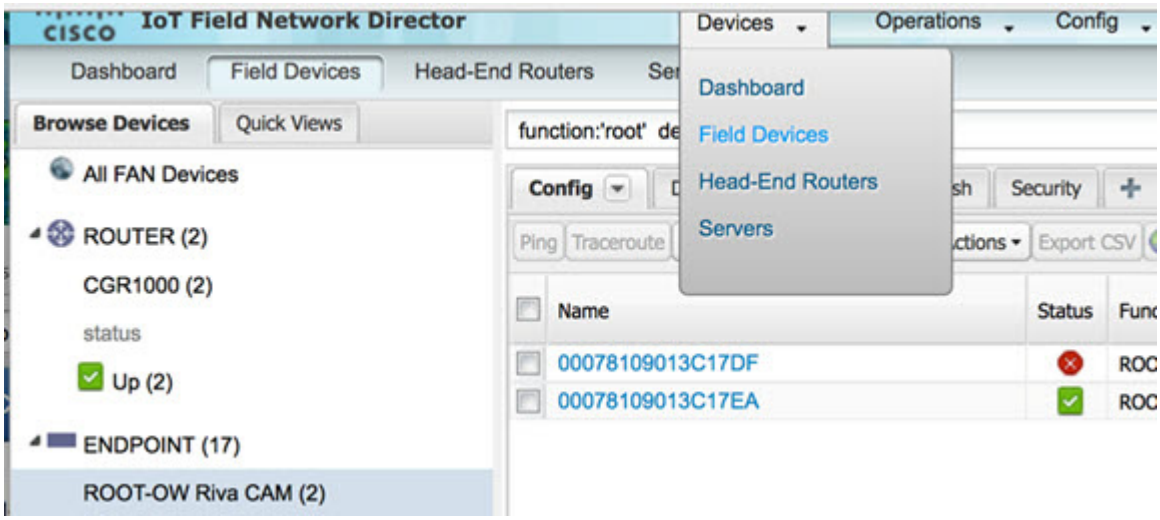
表 20 に、[Head-End Routers] > [Config Properties] ページの [Tunnel 2 Config] エリア内のフィールドを示します。

表 20　[Head-End Routers] > [Tunnel 2 Config Device] のフィールド

フィールド	Key	設定可能かどうか	説明
IPsec Tunnel Source 2	ipsecTunnelSrc2	Yes	IPsec トンネル 2 の送信元インターフェイスまたは IP アドレスを指定します。
IPsec Tunnel Dest Addr 2	ipsecTunnelDestAddr2	Yes	IPsec トンネル 2 の宛先インターフェイスまたは IP アドレスを指定します。
GRE Tunnel Source 2	greTunnelSrc2	Yes	GRE トンネル 2 の送信元インターフェイスまたは IP アドレスを指定します。
GRE Tunnel Dest Addr 2	greTunnelDestAddr2	Yes	GRE トンネル 2 の宛先インターフェイスまたは IP アドレスを指定します。

Inventory

表 21 に、[Device Info] ページの [Inventory] エリア内のフィールドを示します。



[Device Info] ページまでのパスの例:[Devices] > [Field Devices] > [ENDPOINT] > [ROOT-OW Riva CAM] > [Name](設定パネルの製品リンクを選択)。

表 21　[Inventory] のフィールド

フィールド	Key	設定可能かどうか	説明
Config Group	configGroup	Yes	デバイスが属している設定グループの名前。
Device Category	deviceCategory	不可	このフィールドは、デバイスのタイプをリスト表示します。
Device Type	deviceType	不可	このフィールドにより、他のすべてのフィールドが決定され、デバイスとの通信方法、および IoT FND でのデバイスの表示方法も決定されます。
Domain Name	domainName	Yes	このデバイスに設定されているドメイン名。
EID	eid	不可	デバイス クエリで一意のプライマリ キーとして使用されるデバイスのプライマリ要素 ID。
Firmware Group	firmwareGroup	Yes	デバイスが属しているファームウェア グループの名前。
Firmware Version	runningFirmwareVersion	不可	デバイスで実行されているファームウェア バージョン。
Hardware Version	vid	不可	デバイスのハードウェア バージョン。
Hypervisor Version	ハイパーバイザ	不可	(ゲスト OS が稼働している Cisco IOS CGR のみ) Hypervisor のバージョン。
Hostname	hostname	不可	デバイスのホスト名。
IP Address	ip	Yes	デバイスの IP アドレス。トンネル経由の IoT FND 接続にこのアドレスを使用します。
ラベル	label	Yes	デバイスに割り当てられたカスタム ラベル。1 つのデバイスに複数のラベルを割り当てることができます。ラベルは、XML ファイルや CSV ファイルでなく、UI または API により割り当てられます。
Last Heard	lastHeard	不可	デバイスが最後に IoT FND に接続した日時。
Last Metric Heard	該当なし	不可	最後のポーリング(定期的な通知)の時刻。

表 21　[Inventory] のフィールド（続き）

フィールド	Key	設定可能かどうか	説明
Last Property Heard	該当なし	不可	FAR の最後のプロパティ更新の時刻。
Last RPL Tree Update	該当なし	不可	RPL ツリーのポーリング（定期的な通知）の最後の更新の時刻。
Location	該当なし	不可	デバイスの緯度と経度。
メーカー	-	不可	エンドポイント デバイスの製造元。
Mesh Function	cgmesh	不可	メッシュのデバイスの機能。有効な値は、[Range Extender] および [Meter] です。
Meter Certificate	meterCert	不可	メータ別に報告されるグローバルまたは固有の証明書。
Meter ID	meterId	不可	ME のメータ ID。
モデル番号	pid	不可	デバイスの製品 ID。
名前	name	Yes	デバイスに割り当てられている固有の名前。
SD Card Password Lock	-	Yes	（CGR のみ）SD カードのパスワード ロックの状態（on/off）
Serial Number	sn	不可	デバイスのシリアル番号。
Status（ステータス）	status	不可	デバイスのステータス。
Tunnel Group	tunnelGroup	Yes	デバイスが属しているトンネル グループの名前。

メッシュ リンクの設定

表 22 に、[Routers] > [Config Properties] ページの [Mesh Link Config] エリアのフィールドを示します。

表 22　[Mesh Link Config] のフィールド

フィールド	Key	設定可能かどうか	説明
Mesh Prefix Config	meshPrefixConfig	Yes	サブネット プレフィックス のアドレス。
Mesh Prefix Length Config	meshPrefixLengthConfig	Yes	サブネット プレフィックスのアドレス長。
Mesh PAN ID Config	meshPanidConfig	Yes	サブネットの PAN ID。
Mesh Address Config	meshAddressConfig	Yes	メッシュ リンクの IP アドレス。
Master WPAN Interface	masterWpanInterface	Yes	（デュアル PHY CGR のみ）デバイスがマスターであるインターフェイス。
Slave WPAN Interface	slaveWpanInterface	Yes	（デュアル PHY CGR のみ）デバイスがスレーブであるインターフェイス。

メッシュ デバイスの状態

表 23 に、[Device Info] ビューの [Mesh Device Health] エリア内のフィールドを示します。

表 23　[Mesh Device Health] のフィールド

フィールド	Key	説明
Uptime	uptime	最後のブート以降に要素が稼働していた時間の合計（秒）。

メッシュ リンク キー

表 24 に、[Device Info] ビューの [Mesh Link Keys] エリア内のフィールドを示します。

表 24　[Mesh Link Keys] のフィールド

フィールド	Key	設定可能かどうか	説明
Key Refresh Time	meshKeyRefresh	不可	メッシュ リンク キーが最後にアップロードされた日。
Key Expiration Time	meshKeyExpire	Yes	メッシュ リンク キーの有効期限が切れる日。

メッシュ リンクの設定

表 25 に、[Device Info] ビューの [Mesh Link Settings] エリア内のフィールドを示します。

表 25　[Mesh Link Settings] のフィールド

フィールド	Key	説明
Firmware Version	meshFirmwareVersion	ME ファームウェアのバージョン。
Mesh Interface Active	meshActive	ME のステータス。
Mesh SSID	meshSsid	ME のネットワーク ID。
PANID	meshPanid	サブネットの PAN ID。
Transmit RF Power	meshTxPower	ME の送信電力（dBm）。
Security Mode	meshSecMode	ME のセキュリティ モード。
Transmit PLC TX Level	tx_level dBuV	Itron OpenWay RIVA CAM モジュールおよび Itron OpenWay RIVA 電気デバイス（dBuV）（この u = マイクロです）の PLC レベル
RPL DIO Min	meshRplDioMin	DODAG 情報オブジェクト（DIO）のトリクル タイマーの Imin を設定するのに使用される符号なし整数。
RPL DIO Double	meshRplDioDbl	DIO トリクル タイマーの Imax を設定するのに使用される符号なし整数。
RPL DODAG Lifetime	meshRplDodagLifetime	有向非循環グラフ（DAG）としてのすべての下りルートの表示で、デフォルトの有効期間（分）を設定するために使用される符号なし整数。
RPL Version Incr.時刻	meshRplVersionIncrementTime	RPL バージョンの増分期間（分）を指定するために使用される符号なし整数。

メッシュ リンク メトリック

表 26 に、[Device Info] ページの [Mesh Link Metrics] エリア内のフィールドを示します。

表 26　[Mesh Link Metrics] のフィールド

フィールド	Key	説明
Meter ID	meterId	ME のメータ ID。
PANID	meshPanid	ME の PANID。
Mesh Endpoints	meshEndpointCount	ME の数。
Mesh Link Transmit Speed	meshTxSpeed	短い要素固有期間（たとえば 1 時間）で平均した、アップリンク ネットワーク インターフェイスでのデータ送信の現在の速度（ビット/秒）。
Mesh Link Receive Speed	meshRxSpeed	短い要素固有期間（たとえば 1 時間）で平均した、アップリンク ネットワーク インターフェイスでのデータ受信の速度（ビット/秒）。
Mesh Link Transmit Packet Drops	-	アップリンクでドロップされるデータ パケットの数。
Mesh Route RPL Hops	meshHops	要素が RPL ルーティング ツリーのルートから開始されるホップ数。

表 26　[Mesh Link Metrics] のフィールド（続き）

フィールド	Key	説明
Mesh Route RPL Link Cost	linkCost	要素とそのアップリンク ネイバーとの間のリンクの RPL コスト値。
Mesh Route RPL Path Cost	pathCost	要素と、ルーティング ツリーのルートとの間の RPL パスのコスト値。
Transmit PLC Level	tx_level dBuV	PLC および Itron OpenWay RIVA 電気デバイスおよび Itron OpenWay RIVA G-W（ガス水道）デバイスのみでサポート（dBuV 内の u = マイクロです）

NAT44 メトリック

表 27 に、[Device Info] ページの [NAT44] エリア内のフィールドを示します。

表 27　[NAT44 Metrics] のフィールド

フィールド	Key	説明
NAT44 Internal Address	nat44InternalAddress0	NAT 44 で設定されたデバイスの内部アドレス。
NAT 44 Internal Port	nat44InternalPort0	NAT 44 で設定されたデバイスの内部ポート番号。
NAT 44 External Port	nat44ExternalPort0	NAT 44 で設定されたデバイスの外部ポート番号。

PLC メッシュ情報

表 28 に、[Device Info] ビューの [PLC Mesh Info] エリア内のフィールドを示します。

表 28　[PLC Mesh Info] のフィールド

フィールド	Key	説明
Mesh Tone Map Forward Modulation	toneMapForwardModulation	メッシュ トーン マップのフォワード変調は次のとおりです。 ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Tone Map Forward Map	toneMapForward	チャネル内の使用可能なサブキャリアの数を示し、2 進数のオクテット（たとえば、0011 1111）として表示されます。1 は固定チャネルを示します。1 の数が多いほど、チャネルの容量が大きくなります。
Mesh Tone Map Reverse Modulation	toneMapRevModulation	メッシュ トーン マップのリバース変調は次のとおりです。 ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK

表 28　[PLC Mesh Info] のフィールド（続き）

フィールド	Key	説明
Mesh Tone Map Reverse Map	toneMapReverse	チャネル内の使用可能なサブキャリアの数を示し、2 進数のオクテット（たとえば、0011 1111）として表示されます。1 は固定チャネルを示します。1 の数が多いほど、チャネルの容量が大きくなります。RSSI とともに使用されるリバース マップ情報と組み合わせて固定チャネルを決定します。
Mesh Absolute Phase of Power	-	電源のメッシュの絶対位相は、基本的に、PLC ノードの電流および電圧波形の相対的位置です。
LMAC Version	-	PLC モジュール DSP プロセッサにより使用される LMAC ファームウェアのバージョン。IEEE P1901.2 PHY 標準に準拠する PLC 通信に、下位のメディア アクセス機能を提供します。

raw ソケット メトリックおよびセッション

表 29 に、[Field Devices] > [Config Properties] ページの [TCP Raw Sockets] エリア内のフィールドを示します。

表 29　raw ソケット メトリックおよびセッションのビュー

フィールド	Key	説明
メトリック		
Tx Speed (bps)	rawSocketTxSpeedS[portNo]	シリアル データのパケット化ストリームの送信速度（ビット/秒）。
Rx Speed (bps)	rawSocketRxSpeedS[portNo]	シリアル データのパケット化ストリームの受信速度（ビット/秒）。
Tx Speed (fps)	rawSocketTxFramesS[portNo]	シリアル データのパケット化ストリームの送信速度（フレーム/秒）。
Rx Speed (fps)	rawSocketRxFramesS[portNo]	シリアル データのパケット化ストリームの受信速度（フレーム/秒）。
セッション		
Interface Name	-	raw ソケットのカプセル化用に設定されているシリアル インターフェイスの名前。
TTY	-	シリアル インターフェイスに関連付けられているルータ上の非同期シリアル回線。
VRF Name	-	仮想ルーティングおよびフォワーディング インスタンスの名前。
Socket	-	32 の接続のうちの 1 つを特定する番号。
Socket Mode	-	クライアントまたはサーバ。非同期回線インターフェイスが設定されているモード。
ローカル IP アドレス。	-	サーバが接続のために（サーバ ソケット モードで）そこでリッスンするか、またはクライアントがサーバへの接続を開始するために（クライアント ソケット モードで）バインドする IP アドレス。
Local Port	-	サーバが接続のために（サーバ ソケット モードで）リッスンするか、またはクライアントがサーバへの接続を開始するために（クライアント ソケット モードで）バインドするポート。
Dest.IP Address	-	リモート TCP raw ソケット サーバの宛先 IP アドレス。
Dest.Port	-	リモート サーバへの接続のために使用する宛先ポート番号。
Up Time	-	接続が確立していた期間。
Idle Time	-	パケットが送信されなかった期間。
タイムアウト	-	現在設定されているセッション アイドル タイムアウト（分）。

ルータ バッテリ

表 30 に、[Device Info] ページの [Router Battery] エリア内のフィールドを示します。

表 30　[Router Battery] デバイス ビュー

フィールド	Key	設定可能かどうか	説明
Battery 0 Charge	battery0Charge	不可	バッテリ 0 の充電の残量(パーセント)。
Battery 0 Level (%)	battery0Level	不可	バッテリ 0 の充電の残量(パーセント)。
Battery 0 Remaining Time	battery0Runtime	不可	バッテリ 0 がそのインストールまたは最後のリセット以降に動作している期間。
Battery 0 State	battery0State	不可	デバイスのバッテリ 0 の現在の状態。
Battery 1 Level (%)	battery1Level	不可	バッテリ 1 の充電の残量(パーセント)。
Battery 1 Remaining Time	battery1Runtime	不可	バッテリ 1 がそのインストールまたは最後のリセット以降に動作している期間。
Battery 1 State	battery1State	不可	デバイスのバッテリ 0 の現在の状態。
Battery 2 Level (%)	battery2Level	不可	バッテリ 2 の充電の残量(パーセント)。
Battery 2 Remaining Time	battery2Runtime	不可	バッテリ 2 がそのインストールまたは最後のリセット以降に動作している期間。
Battery 2 State	battery2State	不可	デバイスのバッテリ 0 の現在の状態。
Battery Total Remaining Time	batteryRuntime	不可	すべてのバッテリの残りの充電時間の合計。
Number of BBU	numBBU	不可	ルータにインストールされるバッテリ バックアップ ユニット(BBU)の数。ルータは、最大 3 つの BBU(バッテリ 0、バッテリ 1、バッテリ 2)を受け入れることができます。
電源	powerSource	不可	ルータの電源:AC または BBU。

ルータの設定

表 31 に、[Field Devices] > [Config Properties] ページの [Router Config] エリア内のフィールドを示します。

表 31　[Router Config] デバイス ビュー

フィールド	Key	設定可能かどうか	説明
Use GPS Location	useGPSLocationConfig	Yes	内部 GPS モジュールはルータの場所(経度と緯度)を示します。

ルータ クレデンシャル

表 32 に、[Field Devices] > [Config Properties] ページの [Router Credentials] エリア内のフィールドを示します。

表 32　[Router Credentials] のフィールド

フィールド	Key	設定可能かどうか	説明
Administrator Username	-	Yes	ルートの認証に使用されるユーザ名。
Administrator Password	-	Yes	ルートの認証に使用されるパスワード。
マスター キー	-	Yes	デバイスの認証に使用されるマスター キー。
SD Card Password	-	不可	SD カードのパスワード保護のステータス。

表 32 [Router Credentials] のフィールド(続き)

フィールド	Key	設定可能かどうか	説明
Token Encryption Key	-	Yes	トークン暗号キー。
CGR Username	-	Yes	CGR のユーザ名セット。
CGR Password	-	Yes	CGR で、関連付けられているユーザ名に対して設定されるパスワード。

ルータの DHCP 情報

表 33 に、[Device Info] ページの [DHCP Info] エリア内のフィールドを示します。

表 33 [Router DHCP] のフィールド

フィールド	Key	説明
DHCP Unique ID (DUID)	-	hex 文字列形式の DHCP DUID(0xHHHH など)。

ルータの DHCP プロキシの設定

表 34 に、[Field Devices] > [Config Properties] ページの [DHCP Proxy Config] エリア内のフィールドを示します。

表 34 [DHCP Proxy Config] のフィールド

フィールド	Key	設定可能かどうか	説明
DHCPv4 Link for Loopback Interfaces	dhcpV4LoopbackLink	Yes	ループバック インターフェイスでリースを要求するときに、DHCP DISCOVER メッセージ内で使用する IPv4 リンク アドレスを意味します。
DHCPv4 Link for Tunnel Interfaces	dhcpV4TunnelLink	Yes	トンネル インターフェイスでリースを要求するときに、DHCP DISCOVER メッセージ内で使用する IPv4 リンク アドレスを意味します。
DHCPv6 Link for Loopback Interfaces	dhcpV6LoopbackLink	Yes	ループバック インターフェイスでリースを要求するときに、DHCPv6 Relay-forward メッセージ内で使用する IPv6 リンク アドレスを意味します。
DHCPv6 Link for Tunnel Interfaces	dhcpV6TunnelLink	Yes	ルトンネル インターフェイスでリースを要求するときに、DHCPv6 Relay-forward メッセージ内で使用する IPv6 リンク アドレスを意味します。

Router Health

表 35 に、[Device Info] ビュー内の [Router Health] のフィールドを示します。

表 35 [Router Health] デバイス ビュー

フィールド	Key	設定可能かどうか	説明
Uptime	uptime	不可	ルータが、最後のリセット以降に起動して動作している期間(秒)を示します。
Door Status	doorStatus	不可	このフィールドのオプションは次のとおりです。 ■ Open:ルータのドアが開いているとき ■ Closed:ルータのドアが閉っているとき
Chassis Temperature	chassisTemp	不可	ルータの動作温度を表示します。動作温度が顧客が定義した温度範囲を超えたときにアラートを表示するよう設定できます。

ルータ トンネルの設定

表 36 に、[Field Devices] > [Config Properties] ページの [Router Tunnel Config] エリア内のフィールドを示します。

表 36　[Router Tunnel Config] デバイス ビュー

フィールド	Key	設定可能かどうか	説明
Tunnel Config	tunnelHerEid	Yes	FAR がセキュアなトンネル経由で接続している HER の EID 番号を表示します。
Common Name of Certificate Issuer		不可	証明書発行者の名前を表示します。
NMBA NHS IPv4 Address		Yes	非ブロードキャストマルチアクセス（NBMA）IPv4 アドレスを表示します。
NMBA NHS IPv6 Address		Yes	NBMA IPv6 アドレスを表示します。
Use FlexVPN Tunnels		Yes	FlexVPN トンネル設定を示します。

ルータ トンネル 1 の設定

表 37 に、[Field Devices] > [Config Properties] ページの [Router Tunnel 1 Config] エリア内のフィールドを示します。

表 37　[Router Tunnel 1 Config] デバイス ビュー

フィールド	Key	設定可能かどうか	説明
Tunnel Source Interface 1	tunnelSrcInterface1	Yes	WAN 冗長性を提供するために最初のトンネルを作成するインターフェイスを定義します。
OSPF Area 1	ospfArea1	Yes	（IPv4 を実行している）ルータがメンバーである OSPFv2 Area 1 を定義します。
OSPFv3 Area 1	ospfV3Area1	Yes	（IPv6 を実行している）ルータがメンバーである OSPFv3 Area 1 を定義します。
OSPF Area 2	ospfArea1	Yes	（IPv4 を実行している）ルータがメンバーである OSPFv2 Area 2 を定義します。
OSPFv3 Area 2	ospfV3Area1	Yes	（IPv6 を実行している）ルータがメンバーである OSPFv3 Area 2 を定義します。
IPsec Dest Addr 1	ipsecTunnelDestAddr1	Yes	IPsec tunnel 1 の宛先 IP アドレスを定義します。
GRE Dest Addr 1	greTunnelDestAddr1	Yes	GRE tunnel 1 の宛先 IP アドレスを定義します。

ルータ トンネル 2 の設定

表 38 に、[Field Devices] > [Config Properties] ページの [Router Tunnel 2 Config] エリア内のフィールドを示します。

表 38　[Router Tunnel 2 Config] デバイス ビュー

フィールド	Key	設定可能かどうか	説明
Tunnel Source Interface 2	tunne2SrcInterface1	Yes	WAN 冗長性を提供するために 2 番目のトンネルを作成するインターフェイスを定義します。
OSPF Area 2	ospfArea2	Yes	（IPv4 を実行している）ルータがメンバーである OSPFv2 Area 2 を定義します。

表 38　[Router Tunnel 2 Config] デバイス ビュー(続き)

フィールド	Key	設定可能かどうか	説明
OSPFv3 Area 2	ospfV3Area2	Yes	(IPv6 を実行している)ルータがメンバーである OSPFv3 Area 2 を定義します。
IPsec Dest Addr 2	ipsecTunnelDestAddr2	Yes	IPsec tunnel 2 の宛先 IP アドレスを定義します。
GRE Dest Addr 2	greTunnelDestAddr2	Yes	GRE tunnel 2 の宛先 IP アドレスを定義します。

SCADA メトリック

表 39 に、[Device Info] ページの [SCADA] タブのフィールドを示します。

表 39　[SCADA Metrics] のビュー

フィールド	Key	設定可能かどうか	説明
Channel Name	channel_name	不可	FAR のシリアル ポートと RTU とが通信するチャネルを示します。
Protocol Type	protocol	不可	プロトコル変換のタイプを示します。
Messages Sent	-	不可	FAR が送信したメッセージの数。
Messages Received	-	不可	FAR により受信されたメッセージの数。
Timeouts	-	不可	接続確立のタイムアウト値を表示します。
Aborts	-	不可	中心された接続試行の数を表示します。
Rejections	-	不可	IoT FND に拒否された接続試行の数を表示します。
Protocol Errors	-	不可	FAR によって生成されたプロトコル エラーの数を表示します。
Link Errors	-	不可	FAR によって生成されたリンク エラーの数を表示します。
Address Errors	-	不可	FAR によって生成されたアドレス エラーの数を表示します。
Local IP	-	不可	FAR のローカル IP アドレスを表示します。
Local Port	-	不可	FAR のローカル ポートを表示します。
Remote IP	-	不可	FAR のリモート IP アドレスを表示します。
Data Socket	-	不可	FAR により設定された raw ソケット サーバを表示します。

ユーザ定義のプロパティ

[Routers] > [Config Properties] ページの [User-defined Properties] エリアには、顧客が定義したプロパティが表示されます。

WiFi インターフェイスの設定

表 40 に、[Field Devices] > [Config Properties] ページの [WiFi Interface Config] エリア内のフィールドを示します。

表 40　[WiFi Interface Config] のフィールド

フィールド	Key	設定可能かどうか	説明
SSID	wifiSsid	不可	FAR の WiFi インターフェイスに割り当てられているサービス セット識別子(SSID)。
Pre-Shared Key	type6PasswordMasterKey	不可	FAR に保存されている他の事前共有キーを暗号化するために使用されるキー。

WiMAX の設定

表 41 に、[Device Info] ページの [WiMAX Config] エリア内のフィールドを示します。

表 41　[WiMAX Config] のフィールド

フィールド	Key	説明
PkmUsername	PkmUsername	
PkmPassword	PkmPassword	

WiMAX リンク メトリック

表 42 に、[Device Info] ページの [WiMAX Link Health] エリア内のフィールドを示します。

表 42　[WiMAX Link Health] のフィールド

フィールド	Key	説明
Transmit Speed	wimaxTxSpeed	短い要素固有期間（たとえば 1 時間）で平均した、WiMAX アップリンク ネットワーク インターフェイスでのデータ送信の現在の速度（ビット/秒）。
Receive Speed	wimaxRxSpeed	短い要素固有期間（たとえば 1 時間）で平均した、WiMAX アップリンク ネットワーク インターフェイスでのデータ受信の現在の速度（ビット/秒）。
RSSI	wimaxRssi	WiMAX RF アップリンクの測定 RSSI 値（dBm）。
CINR	wimaxCinr	WiMAX RF アップリンクの測定 CINR 値（dB）。

WiMAX リンクの設定

表 43 に、[Device Info] ページの [WiMAX Link Settings] エリア内のフィールドを示します。

表 43　W[WiMAX Link Settings] のフィールド

フィールド	Key	説明
BSID	wimaxBsid	WiMAX デバイスに接続されているベース ステーションの ID。
ハードウェア アドレス	wimaxHardwareAddress	WiMAX デバイスのハードウェア アドレス。
Hardware Version	wimaxHardwareVersion	WiMAX デバイスのハードウェア バージョン。
Microcode Version	wimaxMicrocodeVersion	WiMAX デバイスのマイクロコード バージョン。
Firmware Version	wimaxFirmwareVersion	WiMAX デバイスのファームウェア バージョン。
デバイス名（Device Name）	wimaxDeviceName	WiMAX デバイスの名前。
リンクの状態	wimaxLinkState	WiMAX デバイスのリンク状態。
Frequency	wimaxFrequency	WiMAX デバイスのの周波数。
帯域幅	wimaxBandwidth	WiMAX デバイスが使用する帯域幅。